

**UCISA Information Security Management Toolkit**

**Edition 1.0**

**Volume 1**



## **UCISA**

UCISA is the Universities and Colleges Information Systems Association. UCISA is a membership organisation representing almost all the higher education institutions in the UK. It exists to promote best practice and to act as a representative and lobbying body.

### **Copyright**

This publication is licensed under the Creative Commons Attribution-NonCommercial 4.0 International licence. Subject to the source being appropriately acknowledged and the licence terms preserved, it may be copied in whole or in part and incorporated into another document or shared as part of information given, except for use for commercial gain.

The publication also contains resources from institutions; where this material is copied or otherwise reused, both UCISA and the institution concerned should be acknowledged.

### **Disclaimer**

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas, such as internet addressing, and consequently URLs and email addresses should be used with caution. UCISA cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

### **Availability**

The UCISA Information Security Management Toolkit is freely available to download for non-commercial use from [www.ucisa.ac.uk/ismt](http://www.ucisa.ac.uk/ismt)

Further printed copies of this document may be obtained from UCISA.

I am very pleased to present the UCISA Information Security Management Toolkit, a new resource that has been created from within our community in order to offer guidance and advice on information security management (ISM); to enable colleagues from across the sector to demonstrate locally why ISM is important and to help universities and colleges implement their own information security management systems.

I consider this publication to be a significant addition to the suite of materials that UCISA provides to the sector, and I hope that you find it useful within your institution.

John Cartwright, Director of Computing Services, University of Liverpool  
UCISA Chair

Cyber security is an increasingly business critical issue for universities. Universities operate on the trust of students, staff and partners to manage information safely and securely. Furthermore, universities produce research of great value which can be a target for a variety of economic and political reasons. The UCISA Information Security Management Toolkit is an important guide for security practitioners working toward implementing proportionate risk based controls in complex institutions.

Paul Clark, Director of Policy, Universities UK



# Contents

|   |           |
|---|-----------|
| <b>Introduction</b>   | <b>11</b> |
| The structure of this document  | 12        |
| Definitions and standards   | 12        |
| Route map for using the UCISA Information Security Management Toolkit | 13        |
| Resources   | 14        |
| Reading list  | 14        |
| <b>1 What is information security</b>                                 | <b>15</b> |
| 1.1 The purpose of information security                               | 15        |
| 1.2 Context   | 15        |
| 1.3 Legal and contractual requirements                                | 16        |
| 1.4 What is information security management?                          | 16        |
| Summary   | 16        |
| Resources   | 17        |
| Reading list  | 17        |
| <b>2 Information security governance</b>                              | <b>19</b> |
| 2.1 What is information security governance?                          | 19        |
| 2.2 What does information security governance look like?              | 19        |
| 2.3 Identifying stakeholders and interested parties                   | 20        |
| 2.4 Oversight and audit   | 20        |
| 2.5 Identifying and securing adequate resources                       | 20        |
| 2.6 Example governance structure                                      | 21        |
| 2.7 Selling an ISMS to top management                                 | 21        |
| 2.7.1 For all organisations   | 21        |
| 2.7.2 For research intensive organisations                            | 22        |
| 2.7.3 Preparing a briefing  | 22        |
| 2.7.4 Preparing a business case                                       | 22        |
| Summary   | 23        |
| Resources   | 23        |
| Reading list  | 23        |
| <b>3 Drivers</b>  | <b>25</b> |
| 3.1 Overview  | 25        |
| 3.2 Identifying drivers   | 25        |
| 3.3 Identifying requirements  | 27        |
| 3.4 Continual monitoring of drivers                                   | 27        |
| Summary   | 27        |
| Resources   | 28        |
| Reading list  | 28        |
| <b>4 Scoping</b>  | <b>29</b> |
| 4.1 Introduction  | 29        |
| 4.2 Different scopes  | 29        |
| 4.3 How to define the scope of an ISMS                                | 30        |
| 4.3.1 Identify what needs to be protected                             | 30        |
| 4.3.2 Understand the organisation                                     | 30        |
| 4.3.3 Ensure endorsement of scope                                     | 30        |
| 4.3.4 Monitor and review  | 30        |
| 4.4 Outsourcing and third parties                                     | 31        |
| 4.4.1 Scoping considerations for cloud and outsourcing services       | 31        |
| 4.4.2 Scope and third party contracts                                 | 31        |
| 4.4.3 Questions when outsourcing IT or using a cloud provider         | 32        |
| 4.4.4 Example: third parties and PCI DSS                              | 32        |
| 4.4.5 Example: outsourced scope in an HE environment                  | 32        |

|   |           |
|---|-----------|
| Summary .....   | 33        |
| Resources.....  | 34        |
| Reading list.....   | 34        |
| <b>5 Risk assessment.....</b>                                       | <b>35</b> |
| 5.1 Information risk management.....                                | 35        |
| 5.2 Define information risk measurement criteria.....               | 36        |
| 5.3 Information asset identification and profiling.....             | 36        |
| 5.4 Threat identification and assessment.....                       | 37        |
| 5.5 Identify and assess vulnerabilities .....                       | 37        |
| 5.6 Scoring information risk impact assessment.....                 | 37        |
| 5.6.1 Quantitative vs. qualitative information risk assessment..... | 37        |
| 5.7 Process .....   | 38        |
| 5.8 Information risk treatment.....                                 | 38        |
| 5.9 Information risk register.....                                  | 39        |
| Summary .....   | 39        |
| Resources.....  | 40        |
| Reading list .....  | 40        |
| <b>6 Controls.....</b>  | <b>41</b> |
| 6.1 What is a control?.....   | 41        |
| 6.2 Types of controls.....  | 41        |
| 6.3 Control sets.....   | 42        |
| 6.3.1 A note on the ISO/IEC 27001 Statement of Applicability.....   | 42        |
| 6.4 Implementing controls.....                                      | 42        |
| 6.5 Assessing and managing change.....                              | 43        |
| 6.6 Documenting controls.....                                       | 43        |
| Summary.....  | 44        |
| Resources.....  | 44        |
| Reading list.....   | 44        |
| <b>7 Information management.....</b>                                | <b>45</b> |
| 7.1 What is an information management scheme?.....                  | 45        |
| 7.2 Classification.....   | 46        |
| 7.3 How many levels?.....   | 46        |
| 7.3.1 A note on special cases.....                                  | 46        |
| 7.3.2 Naming the classifications.....                               | 47        |
| 7.4 Labelling .....   | 47        |
| 7.5 Handling.....   | 47        |
| 7.6 Example handling scheme.....                                    | 48        |
| 7.7 Documenting the scheme.....                                     | 48        |
| 7.7.1 Asset inventories.....  | 49        |
| 7.7.2 The information management policy and process.....            | 49        |
| 7.8 Information management as part of an organisation's ISMS.....   | 49        |
| Summary .....   | 49        |
| Resources.....  | 50        |
| Reading list.....   | 50        |
| <b>8 Roles and competencies.....</b>                                | <b>51</b> |
| 8.1 Who does information security? .....                            | 51        |
| 8.2 Top management – decision makers.....                           | 52        |
| 8.2.1 Competencies of top management.....                           | 52        |
| 8.3 Asset owners.....   | 52        |
| 8.3.1 Competencies of asset owners.....                             | 53        |
| 8.4 Dedicated information security roles.....                       | 53        |
| 8.4.1 Competencies of information security professionals.....       | 54        |

|           |   |           |
|-----------|---|-----------|
| 8.4.2     | Competencies of legal and compliance professionals.....         | 54        |
| 8.5       | Other roles.....  | 54        |
| 8.5.1     | Competencies of research leads.....                             | 55        |
| 8.5.2     | Competencies of contractors and third party organisations.....  | 55        |
| 8.5.3     | Competencies of administrators.....                             | 55        |
| 8.5.4     | Competencies of all staff.....                                  | 55        |
| 8.6       | Students.....   | 56        |
| 8.6.1     | Competencies of students.....                                   | 56        |
|           | Summary.....  | 56        |
|           | Resources.....  | 56        |
|           | Reading list.....   | 56        |
| <b>9</b>  | <b>Awareness raising.....</b>                                   | <b>57</b> |
| 9.1       | Introduction.....   | 57        |
| 9.2       | Awareness, education and training.....                          | 57        |
| 9.3       | Triggers for awareness activities.....                          | 58        |
| 9.4       | Foundations of an awareness programme.....                      | 58        |
| 9.5       | Identifying channels for an awareness programme.....            | 59        |
| 9.6       | Identifying content for an awareness activity.....              | 59        |
| 9.7       | Arguments for different audiences.....                          | 60        |
| 9.8       | Challenges.....   | 60        |
| 9.9       | Evaluating the response.....                                    | 61        |
| 9.10      | Evaluating the awareness programme.....                         | 61        |
|           | Summary.....  | 62        |
|           | Resources.....  | 62        |
|           | Reading list.....   | 62        |
| <b>10</b> | <b>Measurement.....</b>   | <b>63</b> |
| 10.1      | Why measure?.....   | 63        |
| 10.2      | What is a useful measurement?.....                              | 63        |
| 10.3      | How to design a useful measurement.....                         | 64        |
| 10.3.1    | Designing measurements of ISMS processes and controls.....      | 64        |
| 10.3.2    | Designing measurements of threat.....                           | 64        |
| 10.4      | Evaluating a measurement.....                                   | 64        |
| 10.5      | How to use measurements.....                                    | 64        |
| 10.6      | Reporting and interpretation.....                               | 65        |
| 10.7      | Examples of effective measurements.....                         | 65        |
| 10.7.1    | Measurements of information risk.....                           | 65        |
| 10.7.2    | Measurements of ISMS effectiveness.....                         | 65        |
| 10.7.3    | Measurements of control effectiveness.....                      | 66        |
| 10.7.3.1  | Types of incidents.....   | 66        |
| 10.7.3.2  | Successful attacks vs attempted attacks.....                    | 66        |
| 10.7.3.3  | Measuring time to patch.....                                    | 66        |
| 10.7.4    | Measurements which are controls.....                            | 66        |
| 10.8      | Examples of measurements which may be less helpful.....         | 66        |
| 10.8.1    | Level of information security.....                              | 66        |
| 10.8.2    | Number of incidents handled.....                                | 67        |
|           | Summary.....  | 67        |
|           | Resources.....  | 68        |
|           | Reading list.....   | 68        |
| <b>11</b> | <b>When things go wrong: nonconformities and incidents.....</b> | <b>69</b> |
| 11.1      | Introduction.....   | 69        |
| 11.2      | Nonconformities.....  | 70        |
| 11.2.1    | Identifying nonconformities.....                                | 70        |

|           |   |            |
|-----------|---|------------|
| 11.2.2    | Dealing with nonconformities.....   | 70         |
| 11.3      | Information security incidents.....   | 70         |
| 11.3.1    | The incident response policy and plan.....  | 71         |
| 11.3.2    | Responsibilities and authorities.....   | 71         |
| 11.3.3    | Stages in incident response.....  | 71         |
| 11.3.4    | Review.....   | 72         |
|           | Summary.....  | 72         |
|           | Resources.....  | 72         |
|           | Reading list.....   | 72         |
| <b>12</b> | <b>Continual improvement.....</b>   | <b>73</b>  |
| 12.1      | What is continual improvement?.....   | 73         |
| 12.2      | Processes for improvement.....  | 73         |
| 12.3      | Types of improvement.....   | 74         |
| 12.4      | Steps in an improvement process.....  | 75         |
| 12.5      | Sources of information and opportunities for improvement.....                                       | 75         |
| 12.6      | Improvement as part of ISMS formalisation.....  | 77         |
| 12.6.1    | Vision for improvement.....   | 77         |
| 12.6.2    | Where are we now?.....  | 77         |
| 12.6.3    | Planning and implementing (where do you want to be and how to get there).....                       | 77         |
| 12.7      | Measurement.....  | 78         |
|           | Summary.....  | 78         |
|           | Resources.....  | 78         |
|           | Reading list.....   | 78         |
| <b>13</b> | <b>Policies.....</b>  | <b>79</b>  |
|           | Summary.....  | 79         |
|           | Resources.....  | 80         |
|           | Reading list.....   | 80         |
| <b>14</b> | <b>Conclusion.....</b>  | <b>81</b>  |
|           | Overall summary.....  | 81         |
|           | <b>Annex – Example resources to accompany the Toolkit.....</b>                                      | <b>85</b>  |
|           | <b>Resources for Introduction.....</b>  | <b>87</b>  |
|           | Different elements of an Information Security Management System – Cardiff University.....           | 88         |
|           | Stages for implementing an Information Security Framework (ISF) programme – Cardiff University..... | 89         |
|           | <b>Resources for Chapter 1 – What is information security?.....</b>                                 | <b>91</b>  |
|           | Template for an information security strategy proposal.....   | 92         |
|           | <b>Resources for Chapter 2 – Information security governance.....</b>                               | <b>95</b>  |
|           | Template for an information security policy.....  | 96         |
|           | Responsibilities overview: Information ownership and risk management – Cardiff University.....      | 97         |
|           | Developing an information security policy – University of York, case study.....                     | 98         |
|           | Bringing information security strategy to senior management – UCL, case study.....                  | 99         |
|           | Key questions for top management.....   | 101        |
|           | Example of a presentation to sell the concept of an ISMS to top management.....                     | 104        |
|           | <b>Resources for Chapter 3 – Drivers.....</b>   | <b>107</b> |
|           | Incidental security improvements from sustainability policies – UCL, case study.....                | 108        |
|           | Information security within the research arena – Loughborough University, case study.....           | 109        |
|           | <b>Resources for Chapter 4 – Scoping.....</b>   | <b>111</b> |
|           | Scope definition for a data safe haven – UCL, case study.....                                       | 112        |
|           | <b>Resources for Chapter 5 – Risk assessment.....</b>   | <b>115</b> |
|           | Template for information risk management principles.....  | 116        |
|           | Development and use of risk assessment templates – UCL, case study.....                             | 117        |

|  |            |
|--|------------|
| Project information risk assessment – Requirements and expectations - UCL.....   | 118        |
| Service information risk assessment – Requirements and expectations - UCL.....   | 120        |
| Project information risk assessment – Capability - UCL.....  | 122        |
| Service information risk assessment – Capability - UCL.....  | 124        |
| Risk treatment plan – UCL.....   | 126        |
| Risk assessment methodology – Cardiff University.....  | 128        |
| Information asset register tool – University of Oxford.....  | 141        |
| <b>Resources for Chapter 6 – Controls.....</b>   | <b>143</b> |
| Evaluating software security patches – Loughborough University, case study.....  | 144        |
| Hacking before and after: How Certified Ethical Hacking (CEH) training changed my<br>perspective on hacking – UCL, case study..... | 146        |
| Technical vulnerability management.....  | 148        |
| Penetration testing.....   | 151        |
| <b>Resources for Chapter 7 – Information management.....</b>   | <b>153</b> |
| Information Classification Scheme – University of York.....  | 154        |
| Development of an Information Classification and Handling Policy –<br>Cardiff University, case study.....                          | 158        |
| Information Classification and Handling Policy – Cardiff University.....   | 160        |
| University Guidance on Classification of Information – University of Oxford.....   | 170        |
| <b>Resources for Chapter 8 – Roles and competencies.....</b>   | <b>173</b> |
| Job description template - Information Security Manager.....   | 174        |
| Job description template - Senior Information Security Specialist.....   | 177        |
| Job description template - Information Security Specialist.....  | 181        |
| SFIA competencies.....   | 184        |
| Collaboration between security administrators and academic researchers – UCL, case study ..  | 185        |
| <b>Resources for Chapter 9 – Awareness raising.....</b>  | <b>187</b> |
| Raising user awareness of information security - Cardiff University, case study.....   | 188        |
| Development and use of a phishing exercise to raise awareness of phishing as an issue -<br>Cardiff University, case study.....     | 192        |
| <b>Resources for Chapter 10 – Measurement.....</b>   | <b>195</b> |
| Evaluating a measurement.....  | 196        |
| <b>Resources for Chapter 11 – When things go wrong: non-conformities and incidents.....</b>  | <b>197</b> |
| Developing an Information Security Incident Response Plan based on ISO/IEC 27035:2011 –<br>University of Oxford.....               | 198        |
| Example of an information security incident response scheme.....   | 200        |
| Information Security Service: Information Security Incident Management Process – UCL.....  | 211        |
| Investigations and Data Access Policies – University of York, case study .....   | 212        |
| Data breach – case study.....  | 213        |
| <b>Resources for Chapter 12 – Continual improvement.....</b>   | <b>215</b> |
| <b>Resources for Chapter 13 – Policies.....</b>  | <b>217</b> |
| Template for a generic policy.....   | 218        |
| <b>Acknowledgements.....</b>   | <b>221</b> |



*Information is the lifeblood of successful organisations. Without it, they cannot operate. Equally, if it is untrustworthy, every activity is suspect, and no-one can make a reliable decision. This is especially important in research, where data accuracy is vital. Finally, some information, such as commercial research findings, personnel records and medical data, is so sensitive that even knowledge of it by the wrong people is dangerous to the organisation.*

Because everyone in any organisation needs to create, access and use information, everyone is responsible for protecting it and using it appropriately. This protection requires a culture where information is seen as being valuable and worth protecting, where effective data management is established, and where student and staff privacy are respected.

In order to achieve and maintain a good approach to information risk management, or information security, organisations can benefit from the well-developed international standards in this area.

ISO/IEC 27001 is the international standard describing the creation and maintenance of an information security management system (ISMS). It can be used by any size of organisation, and is flexible enough to fit any sector. It has been in existence for over twenty years, and is used by many universities in the UK and abroad.

The UCISA Information Security Management Toolkit has been constructed for use by information security/governance professionals wishing to put in place an ISMS in their organisation. It also addresses how to convey the importance of information security to the organisation, since the need for an ISMS is based upon the acceptance that information security is worth investing in. This edition of the Toolkit outlines an approach to successfully implement an ISMS based on ISO/IEC 27001:2013 (Information technology — Security techniques — Information security management systems — Requirements). It is intended as a practical resource, providing an overview of the key aspects of a successful ISMS and guidance on how to implement them. It also includes case studies, as well as templates and example resources which organisations can tailor to suit their needs.

The Toolkit has evolved from edition three of the UCISA Information Security Toolkit, which was based upon the 2005 version of ISO/IEC 27002 (Information technology — Security techniques — Code of practice for information security management), and included sample policies for all the Standard's controls, grouped according to the internal functions of the organisation.

The different approach taken this time reflects the need of organisations for advice and guidance upon setting up and maintaining the organisational infrastructure (including top level policies, processes, and governance) which enables policies and other security measures (controls) to be appropriate, well maintained, and effectively implemented. Information on how to implement controls is not included.

The document has also been revised to reflect the changing trends in the workplace, such as: the growth of the use of personal devices to access organisational systems and services; the increase in off-site working; and the complexities of the research agenda (e.g. protecting intellectual property in an open environment).

Information is not the sole domain of the IT department — it is a cross-institutional concern.

Good information security requires a proportionate, risk-based response.

The UCISA Information Security Management Toolkit will:

- assist those who have responsibility for implementing information security across the organisation by providing advice and guidance to them;
- help them to provide senior university management with an understanding of why information security is an important, organisation-wide issue.

## The structure of this document

The Toolkit is arranged in chapters, each one covering a key aspect of an ISMS and providing advice, instructions and examples to aid implementation. At the end of each chapter is a summary of key points and references. At the end of the document, in the Conclusion, is a collection of all the chapters' summary points.

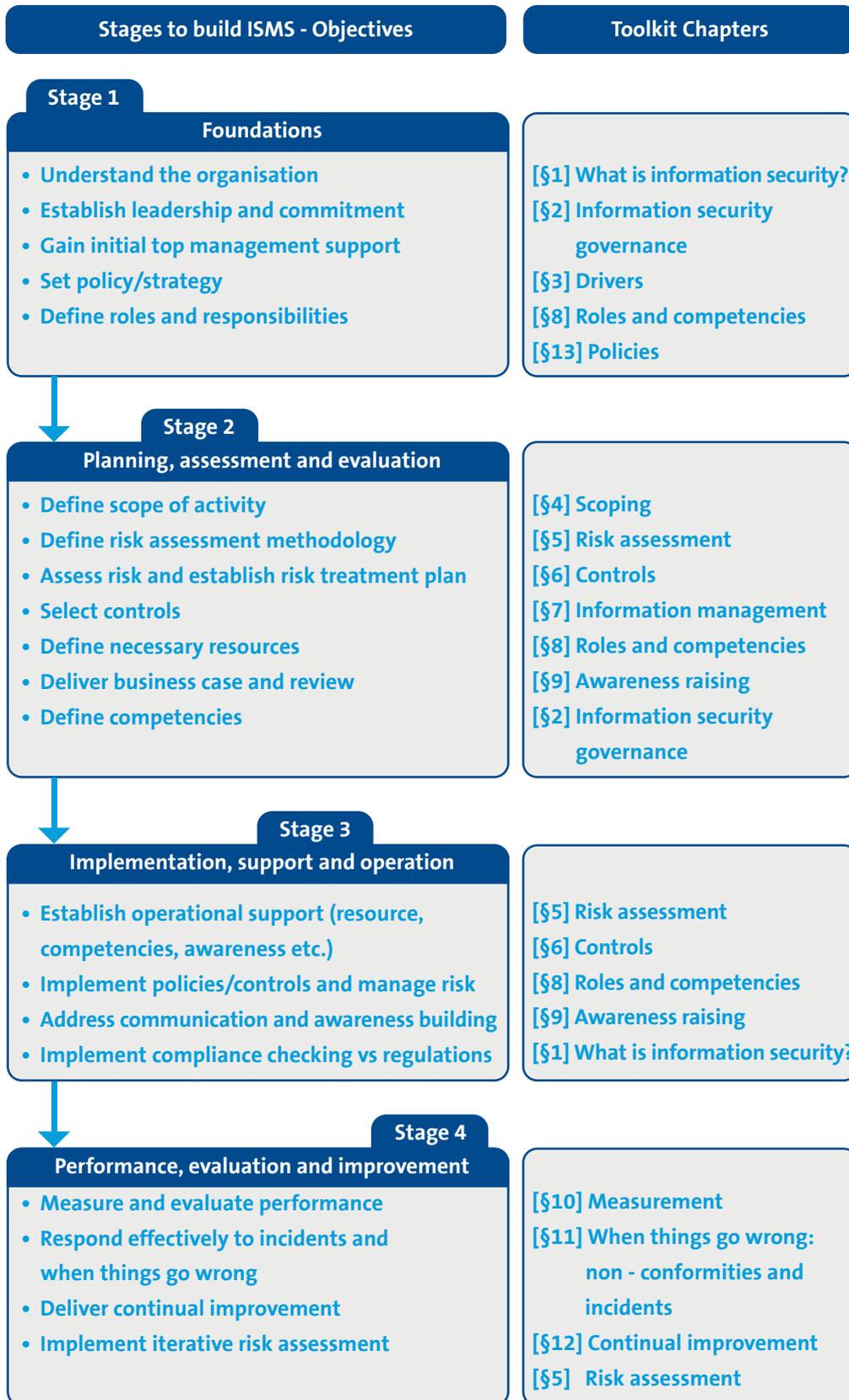
## Definitions and standards

Please note that this document uses the definitions in ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary. These definitions may differ from standard dictionary definitions.

It is also strongly recommended that readers read this document in conjunction with the standards ISO/IEC 27001 and ISO/IEC 27002.

# Route map for using the UCISA Information Security Management Toolkit

## Toolkit Route Map



## Resources

Different elements of an Information Security Management System - Cardiff University

Stages for implementing an Information Security Framework (ISF) programme - Cardiff University

## Reading list

ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary

[www.ucisa.ac.uk/ismt1](http://www.ucisa.ac.uk/ismt1)

<http://standards.iso.org/ittf/PubliclyAvailableStandards/>

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

[www.ucisa.ac.uk/ismt2](http://www.ucisa.ac.uk/ismt2)

[www.iso.org/iso/home/standards/management-standards/iso27001.htm](http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

[www.ucisa.ac.uk/ismt3](http://www.ucisa.ac.uk/ismt3)

[www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=54533](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533)

The Business Dictionary

[www.ucisa.ac.uk/ismt4](http://www.ucisa.ac.uk/ismt4)

[www.businessdictionary.com](http://www.businessdictionary.com)

*This chapter describes the basic concepts of information security, the context within which educational organisations operate, and introduces the topic of information security management. It forms part of Stage 1 – Foundations and Stage 3 – Implementation, support and operation in the Toolkit Route map.*

### Key topics

- The three aspects of information security
- How threats to information are changing
- The purpose of information security management

## 1.1 The purpose of information security

Information takes many forms. It can be stored on computers, transmitted across networks, printed out or written down on paper, and spoken in conversations. In an academic context, information is a crucial asset.

Regardless of its form and content, information has value. This value is maintained by its:

- confidentiality: it is accessible to the right people
- integrity: it has not been tampered with or damaged
- availability: it is there when needed.

Information security is intended to protect information to an appropriate extent by maintaining the level of risk to the organisation at an acceptable level. Effective information security management enables information to be used and shared while protecting its value. In this way, an organisation can maintain efficient operations, achieve legal compliance and maintain its reputation.

Each organisation will have its own attitude to information risk, and should take this into account when deciding what controls to implement.

All members of an organisation are responsible for contributing to its management of information security: their actions, or inaction, can protect or expose information to risk.

## 1.2 Context

All universities are facing increasing threats to their information from a wide range of sources, including organised crime, as noted in the Universities UK publications on Cyber Security. New sources of threat, such as nation states, and ideologically motivated organisations, continue to emerge. Such threats are becoming more widespread, more ambitious and increasingly sophisticated. Attacks can also be carried out without an attacker even having to leave their home.

According to the Ponemon Institute, the cost of a data breach in 2014 was \$145 (£90) per record, including recovery costs, fines/legal costs and impact to normal operations. Thus the overall cost of a breach affecting a database containing 2,000 student records would be expected to be £180,000.

Attackers motivated by money will attack anything from which they can make a profit: e.g. by reselling the

The UK National Security Strategy identifies attacks in cyber space and cyber-crime as a “Tier 1” threat on a par with terrorism.

use of IT resources, by selling personal data, financial data and industrial secrets, or by holding valuable information for ransom. Attackers motivated by the desire to further their country's interests will seek to gather information in bulk and to determine how to disable rival countries' capabilities. Attackers motivated by ideology will seek to spread fear and disorder, for example by destroying high-profile targets.

At the same time, due to organisations' evolving usage of IT, they are becoming more vulnerable to less obvious threats. The growth of cloud services, outsourced approaches to information management and external collaborations present new opportunities for misuse and error, and reduce the role of central, specialised control of IT facilities.

Furthermore, since research activities are increasingly intended to show real-world relevance and benefit, it is reasonable to expect that their work will become more appealing to attackers, as it will be more likely to have a value on the black market.

Educational institutions have other unique properties which make their information risks, and approaches to handle them, different from other organisations (see Chapter 2, Information security governance, for more information).

As their awareness of information risk increases, institutions are seeking to align their operational information security activities to business goals, and asking information security teams to provide assurance of information risk management.

### 1.3 Legal and contractual requirements

Legislation, including the Data Protection Act 1998, the Copyright, Designs and Patent Act 1988, the Regulation of Investigatory Powers Act (RIPA) 2000 and the Computer Misuse Act 1990, places requirements on businesses to protect personal privacy and to ensure the confidentiality and security of their information. For example, holders of personal data must not only be registered with the Information Commissioner's Office but must also take adequate steps to protect that data from unauthorised access. Fines for breaching the Data Protection Act can be up to £500,000. It is also worth mentioning the Privacy and Electronic Communications Act 2003.

Other contractual agreements bring with them further sources of requirements, such as the Health and Social Care Information Centre's Information Governance Toolkit (IG Toolkit) and the Payment Card Industry Data Security Standard (PCI DSS).

Finally, in order to be granted permission to use certain datasets for research purposes (medical records, for example), organisations are increasingly being required to provide evidence of mature information governance.

### 1.4 What is information security management?

If information security is concerned with protecting the confidentiality, integrity and availability of information to an appropriate extent, then information security management is the means by which this can be achieved. The international standard ISO/IEC 27001 describes a way to manage information security, by creating what it calls an information security management system, or ISMS. This is a combination of processes, policies, governance activities, and specific security measures which work together to enable an organisation to manage information risk effectively, and to demonstrate that it is doing so.

#### Summary

- Information security applies to all forms of information
- Threats are becoming more sophisticated and revenue-led
- Information security is the responsibility of all members of an organisation

Creating and maintaining an information security management system (ISMS) is an ongoing activity; as with gardening, there is no moment when it is possible to say that it is finished, and there is no more work to do.

## Resources

Template for an information security strategy proposal

## Reading list

**The UK National Security Strategy**

[www.ucisa.ac.uk/ismt5](http://www.ucisa.ac.uk/ismt5)

[www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/61936/national-security-strategy.pdf](http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf)

**Cyber security and universities: managing the risk**

[www.ucisa.ac.uk/ismt6](http://www.ucisa.ac.uk/ismt6)

[www.universitiesuk.ac.uk/highereducation/Documents/2013/CyberSecurityAndUniversities.pdf](http://www.universitiesuk.ac.uk/highereducation/Documents/2013/CyberSecurityAndUniversities.pdf)

**Ponemon Report: 2014 Cost of Data Breach Study**

[www.ucisa.ac.uk/ismt7](http://www.ucisa.ac.uk/ismt7)

<http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>

**Monetary Penalty Notices: Information Commissioner's Office**

[www.ucisa.ac.uk/ismt8](http://www.ucisa.ac.uk/ismt8)

<https://ico.org.uk/enforcement/fines>



*The first step in establishing adequate information security management within any organisation is the formulation and approval of an overall information risk governance strategy.*

*This chapter explains information security governance and gives an overview of the development, implementation and maintenance of a successful ISMS. Lead implementers need to be able to sell the concept of an ISMS to top management (e.g. the governing body of a university) and to the senior operational board in order to get them fully behind the initiative, and this chapter also describes how to do that effectively. It forms part of Stage 1 – Foundations and Stage 2 – Planning, assessment and evaluation in the Toolkit Route map.*

### Key topics

- **The most critical components in the development, implementation and maintenance of a successful ISMS**
- **How to use your organisational structure to give your ISMS the greatest possible chance of success**
- **How to align your ISMS with your organisation's business strategy**

## 2.1 What is information security governance?

Information security governance can be defined as:

“the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals.” - Gartner

Governance is the foundation of an ISMS, as it provides both strategic and operational frameworks. Information security governance is an integral part of the organisation's wider governance structures and mechanisms, such as business continuity, risk management, financial planning and research ethics.

Information security objectives must support organisational objectives, rather than be an end in themselves.

## 2.2 What does information security governance look like?

An ISMS should be part of the organisation's risk management activities, driven by the organisation's risk appetite and implemented to enable the organisation's strategic aims.

From ISO/IEC 27014, the principles of information security governance are to:

- establish an organisational wide information security policy
- adopt a risk based approach
- set the direction of investment
- ensure conformance with requirements
- foster a security-positive environment
- review performance in relation to business outcomes.

Information security governance should be approached holistically and cover people, processes and technology – it is not an IT issue. The security controls that form part of the ISMS must take account of human, environmental and physical factors and cover information in all its forms including paper records. The information security governance framework must encompass policies, processes, procedures, tools and training that are all joined up and designed in relation to each other in order to achieve the organisation's information security objectives.

**Policy and objectives** - There should be a top level policy which sets out the information security objectives, that in turn support the overall organisational strategy. The policy must be signed off by top management.

**Accountability and responsibility** - The organisation should define accountabilities and responsibilities at a high level, making top management explicitly accountable for information security but ensuring that personal roles and responsibilities are also defined (see Chapter 8, Roles and competencies).

## 2.3 Identifying stakeholders and interested parties

Identifying who requires what assurance is one of the critical success factors of implementing any ISMS. This will involve identifying the major stakeholders.

Stakeholders, in this context, may also be referred to as interested parties and could involve any of the following:

- top management
- business/process owners
- third parties setting requirements/standards (such as the NHS, UK Government, merchant banks)
- internal and/or external auditors
- relevant internal professional service departments (IT Services, Legal Services etc.)
- customers and end users (e.g. students and/or staff).

Identifying stakeholders and interested parties will help ascertain the applicable security requirements for the ISMS. The primary stakeholder(s) will be those who ultimately require assurance that any applicable requirements are being implemented appropriately. These stakeholders may also be the sponsor of the ISMS.

## 2.4 Oversight and audit

One of the most important things to ensure, when designing information security governance, is that there is the capability for oversight. The organisation needs to have confidence that it is investing time, effort and money wisely, and that its activities to manage risk are effective: or, if not, that there is a need for improvement, and in which areas. Accountability for areas and key information assets should be clearly defined (see Chapter 8, Roles and competencies).

In the financial industry, measures are taken to reduce the risk of cognitive bias: the same should exist in the realm of information security.

In order to achieve these two complementary goals, the organisation should ensure that it gives a group or body the formal responsibility for reviewing the effectiveness of the organisation's activities to manage risk. This can be a formal governance body, supported by an executive group made up of staff with responsibility for aspects of risk management. The body with such responsibilities should be independent of the areas upon which it is reporting.

However much we wish to believe in our ability to remain impartial, we cannot ignore the natural human tendency toward bias.

The Audit Committee in an organisation should review the risk register; similarly the internal audit function has a role in reviewing policies and procedures, recommending control systems and monitoring their implementation.

## 2.5 Identifying and securing adequate resources

Resources are required to establish, maintain and improve an ISMS. The level of investment should be based on risk management considerations (see Chapter 5, Risk assessment).

It is recommended that a project or programme be set up to manage any large scale work involved in creating (or significantly changing) any ISMS, with top level oversight. The programme or project should have a cross organisational focus, and should not be presented or perceived as a piece of work for the IT function alone. It can be quite helpful to have the lead for such a programme or project based, in, for example, a governance or risk management role. Significant input will be required from both the governance and IT departments. In addition, representatives for the Human Resources function and those responsible for physical security should be involved in the programme or project. Finally, requirements, products, outputs and outcomes should be quality checked with the wider stakeholders, including the academic community.

Once the initial work is complete, resources required for the continuing management and maintenance of the ISMS should be made available from the organisation's recurrent (or business as usual) budget. This will ensure that the ISMS can continue to be effective, and can adapt to take account of the needs of the organisation into the future.

## 2.6 Example governance structure

The organisation could establish an Information Security Governance Group at a senior level within the organisation hierarchy. This Group would include representation from those responsible for key administrative services (for example, HR, student records), representatives of those responsible for other information assets (for example, the Pro-Vice Chancellor for Research) and those responsible for implementing the information security policy, such as the CISO or members of the Information Security Service. The CISO and their team could:

- review the ISMS and play a role in its continual improvement (see Chapter 12, Continual improvement)
- act as the focal point for co-ordination of cross-organisational controls and conflict resolution
- provide regular performance reports (see Chapter 10, Measurement) to the Audit Committee or similar body
- provide advice and expert assistance, including carrying out risk assessments.

Note: This structure contains the risk of conflict of interest, as the CISO team is responsible for advising on controls as well as measuring and reporting on the effectiveness of the ISMS; care should be taken to ensure separation of duties to manage this risk.

## 2.7 Selling an ISMS to top management

Successful governance depends on buy-in from top management. All organisations operate differently, but one thing which they all have in common is their existence in law. Even the most devolved or federated organisation is still composed of one or more legal entities, each of which is liable to prosecution or criminal charges if found to be breaking the law. Top management are accountable in this respect.

When selling an ISMS to top management, and getting their buy-in, it is important to not use the legal argument as the only, or even the most important, reason for implementing a formal ISMS. For many members of top management, arguments relating to the protection of reputation, safeguarding of intellectual property and maintaining a competitive edge when competing for research grants and contracts are just as persuasive.

Information security should be sold as a business enabler as opposed to a cost. It is imperative to pitch this in terms of the key drivers which align to the organisation's strategic objectives (also see Chapter 3, Drivers). Some examples are given below.

### 2.7.1 For all organisations

- Protection of reputation – a security breach (and a badly handled aftermath) brings bad publicity, and potential litigation and/or fines, which all damage the corporate reputation and can result in the loss of funds from research and students. An effective ISMS supports the UK's National Security Strategy and its focus on cybercrime and thus can be promoted as a reputation enhancing activity.
- Ensuring continued revenue – most funding councils are now asking for assurances that the information which is to be used in research is to be properly protected.
- Risk management – top management is de facto responsible for information security risk. An ISMS provides them, and their governing body and funding body, with assurance that the risk is being appropriately managed throughout the organisation.
- Effective use of resources - an ISMS can lead to more efficient ways of working and best use of resources as controls are deployed (or relaxed) in a co-ordinated, cross-organisation manner to meet the corporate risk appetite. This can lead to higher staff satisfaction as policies are made clear, training is provided and resources are provided to allow application of controls.
- Customer satisfaction - staff and students can feel assured that their own personal data is held securely and that their identity is safe. In the absence of an ISMS, how confident is top management that their own personal data is safe in the organisation's hands? Are they happy for their own salary details or performance reviews to be held in insecure systems, or potentially accessible by untrained staff in a cyber café?

### 2.7.2 For research intensive organisations

- Protection of researchers' and the organisation's intellectual property.
- Compliance with research council requirements for data management and availability.
- Assurance to external stakeholders whose data is used for research —the ISMS gives a competitive advantage in winning research grants and framework bids.

### 2.7.3 Preparing a briefing

Top management will need a concise briefing on what information security is all about, stressing that it is as much about availability as it is about confidentiality and integrity, and outlining the concept of an ISMS to deliver information security assurance. The high level briefing should explain the holistic approach of an ISMS (people, processes and technology) and outline why the organisation should pursue an ISMS.

Key points to remember when preparing a briefing to top management include:

- Top management have very little time to spend on any topic: keep your presentations, documents and arguments very brief.
- Explicitly link information security to the organisation's business strategy.
- The main questions to address will be “What are you asking us to do?”, “Why?” and “What will this cost?”
- Present positive arguments such as cost savings, improvements in efficiency through process improvement, and the opportunity to really get benefit from information held by the organisation (now it will know what it actually holds).
- Use fear, uncertainty and doubt arguments with great care - only make cases based upon provable fact, e.g. recent and relevant incidents within the organisation.
- Be prepared to “show your working” on any particular statement you make in a document.

### 2.7.4 Preparing a business case

In order to secure resources for an ISMS, an initial or outline business case should be presented. It should include relevant drivers as described above and provide an outline of the costs involved in setting up and maintaining an ISMS.

The business case may, if appropriate, explain how the ISMS will provide a return on investment; this is more of a challenge, since an ISMS is largely insurance against loss. It helps to be able to compare the ISMS costs to

Visual representations of what you are trying to achieve, and how you plan to get there, can be more effective than lengthy narratives.

a published index of costs incurred by similar sized organisations as a result of a major information security breach, such as the annual Information Security Breaches Survey Report commissioned by the Department for Business, Innovation and Skills. An initial outline risk assessment may also be used to support the business case (see Chapter 5, Risk assessment).

Relevant metrics should be identified to show how the information security team will be able to measure and report on the effectiveness of the ISMS.

It is important to continually reinforce that the purpose of an ISMS is to achieve a level of security which is consistent with the organisation's risk appetite and which enables corporate objectives. Once a project or programme to establish an ISMS has been agreed and an initial risk assessment exercise undertaken, it is often the case that the originally agreed risk appetite is modified when the financial cost of the security controls required to meet that appetite is presented to the organisation's executives. It is important, however, to keep reflecting the costs back in terms of the risks mitigated and make it clear that a decision not to spend is in effect a decision to accept a specific risk - and that this is perfectly acceptable as long as it is explicitly understood by top management.

## Summary

- A suitable governance framework is a critical component in the development, implementation and maintenance of a successful ISMS
- Top management must endorse and be accountable for information security
- Good governance ensures ownership, scrutiny and accountability

## Resources

[Template for an information security policy](#)

[Responsibilities overview: Information ownership and risk management - Cardiff University](#)

[Developing an information security policy – University of York, case study](#)

[Bringing information security strategy to senior management – UCL, case study](#)

[Key questions for top management](#)

[Example of a presentation to sell the concept of an ISMS to top management](#)

## Reading list

[Gartner article on information governance](#)

[www.ucisa.ac.uk/ismt9](http://www.ucisa.ac.uk/ismt9)

[http://blogs.gartner.com/debra\\_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/](http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/)

[ISO/IEC 27014 Information technology – Security techniques – Governance of information security](#)

[www.ucisa.ac.uk/ismt10](http://www.ucisa.ac.uk/ismt10)

[www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=43754](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43754)

[Annual Information Security Breaches Survey Report commissioned by the Department for Business, Innovation and Skills](#)

[www.ucisa.ac.uk/ismt11](http://www.ucisa.ac.uk/ismt11)

<http://www.pwc.co.uk/audit-assurance/publications/2014-information-security-breaches-surveyjhtml>



*This chapter describes the external and internal factors which influence an organisation to adopt formal information security management, and which shape an information security management system. It also provides advice on how to balance conflicting drivers. It forms part of Stage 1 – Foundations in the Toolkit Route map.*

### Key topics

- The levels at which drivers operate
- Where drivers come from
- How to manage drivers

## 3.1 Overview

In any academic environment, there will be many different external pressures that may seek to influence how the organisation handles information. These may range from formal contractual and statutory requirements, through industry standards (both formal and informal) and funder expectations, to informal but nonetheless compelling desires to gain competitive advantage by enhancing or maintaining the organisation's reputation as a safe place to conduct research. These can all be seen as "drivers".

There are drivers which might influence an organisation to adopt formal information security management (e.g. ISO/IEC 27001); then there are drivers which might influence and shape an existing formal ISMS. The former include contracts, the need to be competitive, and the desire to use existing "known good" methods to secure information. The latter include those standards (including PCI DSS, the IG Toolkit and the Cyber Essentials scheme) which mandate the adoption of certain controls, or which require the use of detailed processes, such as a particular risk assessment methodology (see Chapter 6, Controls).

Failure to adequately recognise and address drivers can have consequences from adverse headlines to loss of future research contracts, financial loss (e.g. if PCI DSS requirements are not met), fines, or the loss of licences for sensitive areas of research or study.

Unfortunately drivers may conflict with internal requirements, or even with each other. For example there may be opposing requirements between open research and commercial exploitation of results, or between data protection and freedom of information, whose resolution will depend on the organisation's priorities and risk appetite.

A formal ISMS can provide a framework for addressing potential conflicts between drivers in a transparent and coherent way that supports the organisation's objectives. See Chapter 2, Information security governance, for more advice on how to encourage the implementation of an ISMS, and advice on stakeholders.

## 3.2 Identifying drivers

Once all of the stakeholders are known (see Chapter 2, Governance), the organisation should aim to identify the drivers for the ISMS. Organisations should aim to identify relevant drivers early on in the formalisation of their ISMS, so that it is fit for purpose from the beginning.

In any organisation, it is likely that the work of managing the impact of external drivers will be spread across multiple departments. For example, DPA and FOIA compliance may be managed by the Legal department, while Finance handles PCI DSS, the Medical School addresses the IG Toolkit, and the IT department, along with Estates, manages the business continuity plan. See Chapter 8, Roles and competencies, for more on this subject.

The table below provides a sample of different types of drivers, and indicates how specific and granular they are.

**Table 1: Types of Driver**

| Driver  | Internal or external? | Issues addressed by driver   | Type of driver  |
|---|-----------------------|--|---|
| Data Protection Act 1998 (DPA)                                  | External              | Publication of, or damage to: personal data; inaccurate personal data; personal data used for unapproved purposes; personal data retained for too long | Legislation<br>High-level principles  |
| Research contracts  | External              | Loss, publication, or damage to sensitive research data.   | Contractual obligation varies: mostly high level, referencing other standards |
| Business advantage  | Internal              | Loss of contracts, staff and students to competitors   | Business policy<br>High level direction from top management                   |
| Risk management   | Internal              | Inconsistent, inappropriate and ineffective controls which waste money and do not protect the organisation   | Business policy<br>High level direction from top management                   |
| Cyber Essentials Standard, Top 20 Cyber-security controls, etc. | External              | Compromise of insecure computers through malware or “hacking”, focussing on likely routes and commonly neglected technical measures                    | Good practice guidance<br>Granular specifications                             |
| The organisation’s Business Continuity Plan                     | Internal              | Damage to operations during a natural disaster or systems failure  | Business policy<br>Granular specifications                                    |
| Information Governance Toolkit (IGT)                            | External              | Insecure storage and use of medical data   | Contractual obligation<br>Granular specifications and high level content      |
| Anti-terrorism legislation                                      | External              | Access by terrorists to certain research areas and equipment   | Legislation<br>High level principles  |
| Payment Card Industries Data Security Standard (PCI DSS)        | External              | Fraud through theft of credit and debit card data  | Contractual obligation<br>Granular and prescriptive                           |
| ISO/IEC 27001   | External              | Inconsistent approach to security; ineffective measures; recurring incidents; inability to demonstrate due diligence                                   | Good practice standard<br>High level guidance and principles                  |
| IT Infrastructure Library (ITIL) and ISO/IEC 20000-1            | External              | Inconsistent and expensive IT support  | Good practice guidance<br>High level guidance and principles                  |

### 3.3 Identifying requirements

Drivers may determine requirements directly or indirectly. Wherever the requirements come from, it is unlikely that all requirements will apply to all systems. Decisions as to which requirements apply to which systems should be justifiable, and should be based on an assessment of risk against the overall objectives of the organisation and the ISMS (see Chapter 5, Risk assessment). This should be appropriately documented and available for inspection if challenged, e.g. during an audit.

Different stakeholders may have different (possibly conflicting) requirements, in which case the primary stakeholders need to agree which requirements are considered to be in scope.

### 3.4 Continual monitoring of drivers

A common mistake which can be made at the point of setting up an ISMS is to assume that it will be possible to identify all drivers and sources of requirements at an early stage. The organisation may make a huge master list of drivers and requirements, use this to identify controls, implement controls, and then believe that all will be well thereafter. Leaving out the issue that not all of the relevant drivers may be known when the ISMS is set up, it is inevitable that not only will new drivers arise, but that existing drivers may change, or cease to be of relevance (also see Chapter 6, Controls, for more information).

A full lifecycle approach to external drivers is therefore required (see Chapter 12, Continual improvement). This should be linked to organisational change processes (e.g. the project management process, strategic planning process, and research funding process) so that changes to drivers can be identified and assessed in good time i.e. before any formal commitments are made by the organisation. It may be possible to extend existing change management processes to cover the activities described in this chapter.

The organisation should develop a standard process for assessment of requirements provided by a new, changed, or retired driver.

A new driver should be assessed to determine whether it is indeed relevant and appropriate; the correct role in the organisation should provide this verification. This step reduces the risk of inappropriate drivers being included, and of inconsistency within organisations where multiple areas are running semi-independent information security management systems. Equally, changed and retired drivers should be ratified.

## Summary

- Drivers can operate at a very high level (e.g. organisational reputation), or be very granular in their level of detail (e.g. researcher reputation)
- Drivers can be internal (e.g. responsibility to students and staff), but are often external (e.g. the Information Governance Toolkit)
- Managing the impact of drivers is an iterative process

## Resources

Incidental security improvements from sustainability policies – UCL, case study

Information security within the research arena – Loughborough University, case study

## Reading list

**Criminal Justice Secure Email**

[www.ucisa.ac.uk/ismt12](http://www.ucisa.ac.uk/ismt12)

<http://cjsm.justice.gov.uk/>

**Business Impact Levels**

[www.ucisa.ac.uk/ismt13](http://www.ucisa.ac.uk/ismt13)

[http://www.cesg.gov.uk/publications/Documents/business\\_impact\\_tables.pdf](http://www.cesg.gov.uk/publications/Documents/business_impact_tables.pdf)

**Risk Management and Accreditation Documentation Set (RMADS)**

[www.ucisa.ac.uk/ismt14](http://www.ucisa.ac.uk/ismt14)

[www.gov.uk/service-manual/making-software/information-security.html](http://www.gov.uk/service-manual/making-software/information-security.html)

**CERT Top 10 List for Winning the Battle Against Insider Threats**

[www.ucisa.ac.uk/ismt15](http://www.ucisa.ac.uk/ismt15)

[www.rsaconference.com/writable/presentations/file\\_upload/star-203.pdf](http://www.rsaconference.com/writable/presentations/file_upload/star-203.pdf)

**Guide to developing a Data Management Plan**

[www.ucisa.ac.uk/ismt16](http://www.ucisa.ac.uk/ismt16)

[www.dcc.ac.uk/resources/how-guides/develop-data-plan](http://www.dcc.ac.uk/resources/how-guides/develop-data-plan)

**PCI DSS and related standards**

[www.ucisa.ac.uk/ismt17](http://www.ucisa.ac.uk/ismt17)

<https://www.pcisecuritystandards.org/>

*This chapter outlines what is meant by scope and how to decide the scope for an ISMS. It forms part of Stage 2 – Planning, assessment and evaluation in the Toolkit Route map.*

### Key topics

- How scope can mean something different depending on the context
- How to successfully define the scope of an ISMS
- What to consider when scoping outsourced/third-party services

## 4.1 Introduction

Scoping is a critical part of planning the roll-out and implementation of an information security management system (ISMS). An organisation is often sub-divided into smaller ISMS scopes (e.g. an ISMS relating to a particular project, service, audit or policy etc). In either case, the scope determines the boundaries and applicability of information security management and controls. Scope will be shaped by:

- the business of an organisation
- the needs and expectations of relevant interested parties
- the organisational structures that are currently in place.

It is important to correctly define and agree scope with the relevant senior stakeholders at the outset, so as to manage expectations, agree in advance what is (and is not) to be achieved, and ensure that applicable security requirements for relevant systems are identified and implemented.

## 4.2 Different scopes

An organisation will typically have multiple scopes relating to information security. For example, the overall scope for information security is likely to be considered as the entire organisation. However, in most Higher Education environments it would be difficult to tackle the whole organisation in one go. Similarly, it would be an almost impossible task to certify the entire organisation against a standard such as ISO/IEC 27001 or PCI DSS. Thus the organisation should consider having multiple, smaller, scopes, each of which is tailored to the protections required for the information it encompasses. For example, the scope of a PCI DSS audit is determined by protecting only payment cardholder data.

Starting with a reduced scope (as opposed to trying to tackle too much too quickly) may also increase the chances of success, and of achieving the objectives of the ISMS in a reasonable time.

Examples of scopes include:

- scope of an ISMS for the purposes of ISO/IEC 27001 certification
- scope to which a policy applies
- system components potentially affecting the security of cardholder data for PCI DSS compliance
- scope of an audit
- scope of specific information security projects and services
- scope of responsibility in contractual agreements.

The scope of an ISMS should take account of the organisational objectives, structure, location, assets, technology and/or people involved in the delivery of those objectives.

## 4.3 How to define the scope of an ISMS

### 4.3.1 Identify what needs to be protected

One of the first questions to ask is “what needs to be protected”? It is likely that there will be many information assets that need to be protected in order to support the organisation in achieving its business objectives. It is important to understand which of these the organisation considers to be most important, and so a risk-based, prioritised approach should be taken to scoping. In order to establish that assets are actually worth protecting, the organisation should justify why each asset requires protecting.

The scope of an ISMS may initially be defined to include only specific processes, services, systems or particular departments. Success stories can then be presented as a business case for expanding the scope of the ISMS, or creating another, separate scope with different requirements and protections.

In order to make the scope entirely clear, especially to third parties, it is a useful exercise to identify what is not in scope (e.g. the activities of the HR department).

Either way, the scope should clearly define what is being included, based on the business objectives and information assets to be protected, and it should be clear that anything else is out of scope.

### 4.3.2 Understand the organisation

The scope of an ISMS should take advantage of the organisational, management and governance structures that currently exist. The person(s) tasked with managing information security across an organisation should therefore begin by identifying relevant structures, and any constraints set by the structures that currently exist. If there is no governance currently in place then progress will be limited when trying to identify requirements and risk, and implementing security controls across the entire organisation. The scope of any initial work may therefore be to implement an appropriate management and governance framework (see Chapter 2, Information security governance).

Where the scope of an ISMS is defined by the need to protect a particular asset (e.g. cardholder data) or delivery of an objective (e.g. certification against ISO/IEC 27001) then it is important to first understand system components and structure involved in the delivery of relevant services. This may include, for example, obtaining system diagrams showing data stores and flows and relevant IT systems. Personnel involved in managing and delivering all system components will then likely be considered “in scope”.

### 4.3.3 Ensure endorsement of scope

The scope of an ISMS, policy, project or audit etc. should be endorsed and formally agreed by the relevant senior stakeholders (top management), to manage expectations and clearly define the objectives that will be delivered. Failure to correctly identify and formally agree the scope in this way is likely to lead to unclear objectives, difficulties in measuring progress and ultimately decrease the chances of success.

For those managing information security, it is important to consider the boundaries of control and authority. If, for example, the security of services or systems in a particular department are beyond the control or authority of the owners of the ISMS, they should not be included in the scope.

In the context of an audit, agreeing which systems are in scope may be particularly important so as to ensure that it is clear which systems the auditor is authorised to access and under what circumstances. Failure to obtain such authorisation in advance could even lead to a breach of law (such as the Computer Misuse Act 1990).

### 4.3.4 Monitor and review

The scope of an ISMS, policy, audit or project is not static and may evolve over time as circumstances, threats, technologies and requirements develop. Therefore scoping is not something that should be done once at the beginning of a project and then forgotten about. Rather, scope should be monitored and reviewed at regular intervals and/or in the light of significant changes. In the event of an audit (be it for internal control or certification purposes) one of the first things an auditor should do is to review and assess the appropriateness of the scope. Factors that might affect/change the scope of an ISMS include:

- time dependencies: e.g. the scope of a particular ISMS and/or security project may only be applicable for a particular time period
- change in regulatory environment
- changes/updates to standards and/or third party requirements

- change in organisation (e.g. organisation structure changes)
- identification of non-conformities and/or incidents indicating incorrect scope
- overall maturity of ISMS (scope may increase over time)
- change in processes and practices (e.g. ceasing certain activities)
- outsourcing services.

## 4.4 Outsourcing and third parties

Outsourced: Any element that is not wholly controlled, managed, built, implemented and maintained by staff employed by the organisation.

Cloud services: A shared computer-based storage solution for data that is based in a virtualised computer environment. Cloud services can describe any shared environment, which can be provided both locally or outsourced.

All organisations will outsource some activities to third parties. Some third parties are taken so much for granted that, when questioned, staff do not remember them – e.g. the cleaning teams, waste removal contractors, and potentially accountants or auditors. Their activities may not be under scrutiny, yet they may have the highest levels of access.

There are many reasons why an organisation may want or need to outsource some (or all) of its IT provision. As information technology changes and evolves extremely quickly, it can be more cost-effective to outsource some of an organisation's IT solution, or to use cloud storage or services. Economies of scale means that large data warehouse-style storage facilities can offer cheap storage and extremely good availability. Externally hosted services may also provide specialist IT knowledge and support that is not available within the organisation.

If managed properly, outsourced IT or cloud technology carries no greater risk, and arguably less risk, than managing an in-house IT environment. However, poorly sourced or managed outsourcing, or inappropriate cloud provision, can be extremely risky.

### 4.4.1 Scoping considerations for cloud and outsourcing services

When cloud services are used, there can be multiple parties involved in the production of the overall service. For example, infrastructure and software services can be provided by different organisations.

Scoping in this context will involve having a clear understanding of the system components involved and the security responsibilities of each service provider. These security requirements should be included in any contractual agreements.

Responsibility for implementing security may be outsourced, but the accountability cannot be, and so it is therefore important to understand the scope of an ISMS in this context. Put simply, when it comes to meeting certain security requirements, outsourced functions or processes will be in scope for an ISMS, but the suppliers are unlikely to be. It is up to the organisation to decide how it may be assured that services provided are of an appropriate standard.

For further information, the ICO has produced a guide on the use of cloud computing, and UCISA has a briefing paper on cloud computing.

When outsourcing, it is vital to define the boundaries of applicability, responsibility and accountability.

### 4.4.2 Scope and third party contracts

Understanding an organisation's relationship with third parties is extremely important to ensure security for the business and the information that it holds, especially where information security may be put at risk by third party activities, even though their activities are not obviously related to information (e.g. cleaners).

When working with any third party, it is important for information security that the following are defined:

- Legal responsibility, accountability and insurance: all the parties' responsibilities must be detailed and understood. Running through a risk assessment process will uncover many areas where accountability needs to be defined. Disaster planning and incident response is also a good way of verifying that ownership and insurance responsibilities are correctly scoped.
- Access and authorisation: it is essential to make sure the rules and regulations for who can access what are clearly defined. If the organisation is allowing contractors into buildings, it should understand who has the keys or access codes; and who ensures the staff are trained and things are secure. Out of hours

office cleaning staff often have more physical access to an organisation than even the most trusted day staff. Access to IT systems and data should also be considered.

- Disclosure and privacy: the organisation should define and categorise the information that is being used and shared, and specify the applicable rules and regulations.
- Contract terms: The terms of contracts with third parties should be clearly defined to make sure that all parties are clear on the expectations of the work to be conducted, and sanctions or liabilities in the event of default are assigned.

#### **4.4.3 Questions when outsourcing IT or using a cloud provider**

When selecting a third party, questions such as the following should be considered:

- What data are going to be on the outsourced system? Do the data include any sensitive information, or have special requirements?
- What laws or regulations apply to the service provider who is supplying the IT provision? If it is a company outside of the EU, how will that interact with the requirements of the data which it will handle? Where will the data itself be stored?
- Who needs access to the IT solution? Is it something that needs a lot of physical involvement or does it not need any attention for many months?
- Are there restrictions on who administers the system? Who will the administrators be and who controls the access rights?
- Where is the system physically housed? Is the facility secured, who is it shared by, and who controls the access?
- Does the outsourced service provider themselves outsource any of their provision (e.g. off-site back-ups)? How do they manage the security controls which their third parties are handling?
- What service level is expected or provided? What levels of assurance for confidentiality, availability and integrity of data are there? Check the policies in place within your organisation.
- At the end of the business relationship, how will it be possible for the organisation's information to be extracted from the third party environment in a usable form?
- What provisions (if any) are in place for compensating the organisation for the impact of a business continuity incident or disaster (e.g. loss or exposure of information)?

#### **4.4.4 Example: third parties and PCI DSS**

A service provider may supply remote firewall management, or paper shredding, services to the organisation. The service provider themselves would not need to be PCI DSS compliant, but the service provided to the organisation should be compliant and would fall in scope for the PCI DSS assessment of the organisation.

Service providers can demonstrate PCI DSS “compliance” either by having their service included in the organisation's assessment, or by undergoing an assessment themselves. In either case, the services provided that may affect the security of cardholder data must be considered to be in scope. It is the responsibility of the organisation to demonstrate compliance – rather than the service provider.

#### **4.4.5 Example: outsourced scope in an HE environment**

A large organisation is divided into distinct units that use different types of data and have different requirements for that data. The organisation is federated into many different smaller units that each require basic IT. The basic IT provision consists of desktop and file services for general information.

In one area of the organisation, IT is provided by an external company employed by the organisation. The units using this “group IT provision” treat it as outsourced provision and have service level agreements in place. The reason it is considered outsourced is that, when the scope was defined, the control of the system administration, access control, physical security and changes to the systems were out of the control of the individual units.

One of the units using the “group IT provision” requires a fully validated and highly secure database for one project. This is a very specialised system that neither the unit IT nor the “group IT provision” can provide on its own. The unit employs a third party software provider to build, maintain and support the database, but, because of the sensitivity of the data, it has been built on the servers and storage provided by the group IT provider, and is managed by the IT support personnel employed by the unit.

Every element of this outsourcing must be clearly understood to manage the scope:

- Where was the database physically housed?
- Who has access to each part of the system from software to hardware?
- What provides the integrity checking?
- What and who ensures availability?
- Who provides the assurance of confidentiality?
- What laws and regulations are involved in each part of the system?
- What countries are involved?
- What service level provision is required by each of the parties?
- What security controls need to be considered?

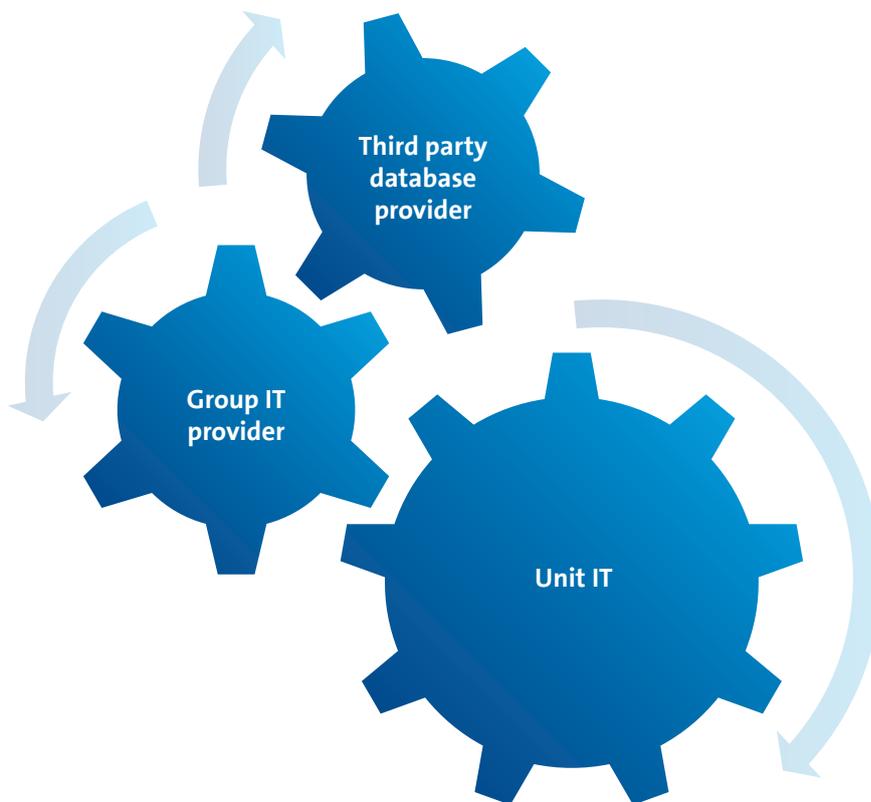


Figure 1: Illustrates the relationships detailed above.

## Summary

- Successfully defining and agreeing the scope of an ISMS from the beginning is a critical success factor in the implementation of any ISMS – if the scope is wrong you will not know where you are going or when you got there!
- There are different scopes involved in implementing information security in an organisation, from high-level scopes covering the entire organisation, to the scope of a particular project or service
- Start small with one limited scope, demonstrate success and build from there
- Monitor and review, and if your scope is wrong then change it accordingly

## Resources

Scope definition for a data safe haven – UCL, case study

## Reading list

The Common Vulnerabilities and Exposures database:

[www.ucisa.ac.uk/ismt18](http://www.ucisa.ac.uk/ismt18)

<https://cve.mitre.org/>

UCISA briefing paper on cloud computing:

[www.ucisa.ac.uk/ismt19](http://www.ucisa.ac.uk/ismt19)

[www.ucisa.ac.uk/publications/cloud.aspx](http://www.ucisa.ac.uk/publications/cloud.aspx)

The Information Commissioner's Office's advice on choosing a cloud service provider:

[www.ucisa.ac.uk/ismt20](http://www.ucisa.ac.uk/ismt20)

[https://ico.org.uk/media/for-organisations/documents/1540/cloud\\_computing\\_guidance\\_for\\_organisations.pdf](https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf)

*This chapter of the Toolkit is devoted to the subject of information security risk assessment and management. Information risk management is important as organisations cannot avoid being exposed to information risk. It forms part of Stage 2 – Planning, assessment and evaluation, Stage 3 – Implementation, support and operation and Stage 4 – Performance, evaluation and improvement in the Toolkit Route map.*

*Within this chapter, a methodology for information risk assessment is described, as well as some of the key considerations involved when carrying out information security risk assessment.*

### Key topics

- **Why information security risk assessment is important**
- **The key steps in carrying out an information security risk assessment**
- **How to decide the appropriate cost of mitigating an information risk**

Organisations wishing to achieve certification to ISO/IEC 27001 should note that (as per clauses 8.2 and 8.2 of ISO/IEC 27001) they should carry out information security risk assessments, keep records of those information risk assessments and use the information risk treatment plan derived from the information risk assessments to treat the documented information risks.

The exact risk assessment methodology to be used is not specified by the Standard. Organisations can choose to follow the approach described here, or another approach which suits them better.

## 5.1 Information risk management

Information risk management is the systematic identification and assessment of information risk, coupled with the consideration, planning and application of risk responses, in order to ensure that the exposure to a given risk is at an acceptable level. It is an iterative process which, due to the ever changing internal and external environments and the emergence of new threats and identification of new vulnerabilities, is never complete.

All organisations have information assets. These information assets are often critical in supporting business operations. Equally, all organisations are exposed to threats and vulnerabilities which constitute risks to those information assets and if left unchecked have the potential to damage the organisation's ability to meet its stated objectives.

As such it is prudent to consider the risks which may have a negative impact on their information assets and, through the consistent application of information risk assessments, determine the controls they wish to apply to treat the risks to those assets.

It is important to ensure that any corporate risk management strategy, risk management method and assessment methods are borne in mind when carrying out information security risk assessments.

Carrying out and documenting information risk assessments provides for an auditable process, demonstrating and providing justification for decisions made in relation to information security.

The extent to which an organisation invests resource in protecting its information assets should be directly related to the potential impact of the risks on those assets.

Each organisation should determine the specific threats which affect the confidentiality, integrity and availability of their information assets.

Only by carrying out information security risk assessments to identify and assess all the risks facing its information assets can an organisation hope to identify how to best utilise its resources to treat those risks. Additionally carrying out and documenting information risk assessments provides for an auditable process demonstrating and providing justification for decisions made in relation to information security.

Whilst this toolkit is written from the perspective of risk assessing information assets, it is important to note this is not the only approach. For those pursuing certification against ISO/IEC 27001:2013, the latest version of the standard does not require an information asset-based approach. However, certainly in the short term this is what auditors will be used to seeing, and it will not invalidate an ISMS from their perspective. Regardless of the risk assessment methodology chosen, the essential steps of information risk identification followed by assessment of impact and likelihood still apply.

The reading list for this chapter contains links to examples of established best practice.

## 5.2 Define information risk measurement criteria

Whilst information security risk assessment is a distinct activity, it is important to ensure that any corporate information risk management strategy, information risk management method and assessment methods are borne in mind when carrying out information security risk assessments. This is in order that the assessment of, and products from, information security risk assessments make sense in the context of the wider organisational risk management framework and fit into wider organisational and strategic risk registers.

It is also important to note that information risks can be mapped to the type of organisational objective concerned, that is to say strategic (long-term), programme/project (medium-term) and operational (short-term) objectives. The type of objective which an information risk affects will have some bearing on the level of audience who should be reviewing and managing the risk. However there may be interplay between the different levels. For example a project risk could quite easily be relevant in terms of the programme to which it belongs and potentially could affect a strategic objective. As such, risks identified at one level will often feature on the risk register at another.

Information risk assessments should consider impact in terms of the effect on the organisation's stated purpose and objectives.

The OCTAVE Allegro guidebook V1.0 on information security risk assessment suggests that as a minimum the following impact areas are considered: reputation/customer confidence, financial, productivity, safety and health, fines/legal penalties, plus one or more user-defined impact areas.

## 5.3 Information asset identification and profiling

An information asset is essentially a distinct set of information which has some value to the organisation. Every organisation will have thousands, or even millions, of information assets, and it is infeasible to expect to identify and profile each one individually. However, many assets will be sufficiently similar that they can be addressed in aggregate, while a few (e.g. certain research data sets) will be unique and valuable/critical enough to warrant individual attention.

When evaluating risk against an information asset, it is important to have a sufficient understanding of the information asset (or class of assets).

The organisation should develop a profile which covers:

- exactly what the asset is
- its requirements for confidentiality, integrity and availability
- the lifecycle of the asset (some assets, such as research findings, experience a change in their requirements for confidentiality after publication)
- the business processes which affect it
- ownership
- the value of the asset to the organisation, and why the asset is important to the organisation
- the expected value of the asset to an attacker
- its classification (see Chapter 7, Information management)
- its expected lifespan.

It is also important to understand where the information asset is located in terms of information asset

“containers” i.e. the information asset may be more or less vulnerable to a specific threat depending on the systems or storage locations in which it is held through the information lifecycle. Information may be more vulnerable to disclosure during transmission as opposed to processing or storage.

A clear understanding of the asset enables better understanding of the threats and vulnerabilities and thus enables more effective information risk assessment.

## 5.4 Threat identification and assessment

Having identified and profiled the information asset, the next stage is to identify the threats to that information asset. This can be done by brainstorming or by reviewing a list of common threats and identifying which threats are relevant. Some typical threat categories include: natural disaster, human, competitors, criminals, political. However each organisation should determine the specific threats which affect the confidentiality, integrity and availability of their information assets. Threat identification can be carried out in a hierarchical fashion, starting with the business and strategic threats and then working down to technical threats and relating them to strategic and business threats.

When carrying out a threat assessment, each identified threat should be classified and ranked according to potential impact. There are a range of models which can be used to rank threats. Typically they will include some or all of the following:

- the potential damage
- how repeatable the attack/event is
- how easy it is to carry out the threat e.g. what skills might be required
- how easy it would be for a malicious party to discover the vulnerability
- motivation.

## 5.5 Identify and assess vulnerabilities

A vulnerability is a weakness that exposes an organisation to information risk by providing an attack surface for a threat. For example, a hacker can be seen as a threat, and a vulnerability that the hacker may exploit could be a poorly patched web server. The information risk is a combination of the threat of the hacker and the opportunity provided by the availability of the web server vulnerable to attack. The information risk can then be calculated by assessing the likelihood of the hacker attacking the webserver and multiplying it by the impact on the organisation of the attack. As with threat assessment, the likelihood and impact relating to each vulnerability should be assessed. As with threats, there are different aspects such as motivation, repeatability and how easy it is to exploit the vulnerability.

With regard to types of vulnerabilities, it is possible to find lists of typical vulnerabilities online. For example, the Common Vulnerabilities and Exposures database is a freely available dictionary of publicly known information security vulnerabilities and exposures. However, information security vulnerabilities come in human, physical and process form as well as software and hardware. Identification of vulnerabilities can also be treated hierarchically, as for threats (see previous subsection).

The potential impact of each vulnerability should then be assessed and quantified in order to allow the highest priority vulnerabilities to be addressed first.

## 5.6 Scoring information risk impact assessment

Having identified the threats and vulnerabilities, the resultant information risks must be quantified. Since no organisation has unlimited resources to employ in the mitigation of risk and since different mitigation actions are more or less effective than each other, it is essential to understand which risks need to be addressed first, and what mitigation actions offer the most protection, for the least investment in time and effort.

### 5.6.1 Quantitative vs. qualitative information risk assessment

Qualitative information risk assessment is the most commonly used approach to information security risk assessment and uses subjective estimates (e.g. high, medium, low) for likelihood and loss/consequence. When performing information risk assessments, it is recommended that information risks are assessed by more than one person to reduce the subjective element of this approach. A workshop format is often a useful way of bringing those individuals who are most familiar with the information asset and the associated threats and

When performing risk assessments, because of the subjective nature of this approach, it is recommended that risks are assessed by more than one person.

An information asset may be more or less vulnerable to a specific threat, depending on the way in which it is handled and stored.

vulnerabilities together to discuss and agree the likelihood and impact of each risk. Examples of this type of information risk assessment can be seen in the resources section for this chapter.

Quantitative information risk assessment, unlike qualitative information risk assessment, uses numerical values (normally monetary) rather than subjective values (high, medium, low) for risk assessment. Figures are derived for the Single Loss Expectancy (how much the occurrence of a given information risk costs) and Annual Rate of Occurrence (how often a risk will occur per year). From these it is possible to calculate the Annual Loss Expectancy (how much the organisation can expect to lose each year for a given risk).

By defining a monetary value for risks and having the historic data to determine the expected frequency, it is not only possible to prioritise information risks in order of the financial impact on the organisation, but in combination with an understanding of the costs of your controls and their effectiveness at mitigating risk, it is possible to make some statements about the Return On Security Investment.

Unfortunately, quantitative information risk assessment requires a significant amount of data about information risk impacts and probabilities, which may not be readily available and which are resource intensive to collect. Calculations can be complex and resource intensive and, as a result, professional risk management software is often required for effective analysis. In addition, technology changes so fast that historical data may not be a good source of information about current and future impacts and probabilities.

It is often the case, particularly with information security risk, that the impact of a risk cannot be defined solely as a numerical value or monetary sum. For example, the reputational impacts of a data breach cannot easily be measured by quantitative methods. Quantitative information risk assessment is a process which requires experience and competence to use and is not as straightforward to involve colleagues in as qualitative information risk assessment.

One possible approach is to use qualitative information risk management by default, and quantitative information risk assessment where it is felt that the benefits provided by the technique outweigh the costs.

## 5.7 Process

The information risk assessment case study provides a practical example of how information risk measurement criteria can be used to help achieve consensus when using qualitative information risk assessment.

Since qualitative information risk assessment is largely subjective, agreement may not be reached if a simple high, medium, low rating is used to rate impact and likelihood. Using information risk measurement criteria provides a consistent basis on which to assess the impact and likelihood of a risk and provides a descriptor for each impact level and likelihood rating so that individual perceptions of what is high or low are excluded and consensus is reached on which impact statement best described the perceived risk.

The steps involved are:

1. Considering the threats and vulnerabilities, generate information risk scenarios (e.g. through brainstorming). These scenarios should, in real world terms, outline something which could go wrong and the mechanism by which it could occur. You can also use a standard list of risk scenarios.
2. Assess and score each information risk for impact.
3. Assess and score each information risk for likelihood.
4. Plot impact and likelihood of each information risk on a risk acceptance matrix (examples of which appear in the case studies supporting this chapter).

It is important to retain some sense of proportion when attempting to estimate impacts and effects; the organisation should bear in mind that some of the most devastating impacts actually rely on a chain of specific circumstances, which reduces the likelihood of an event with that very high impact occurring.

## 5.8 Information risk treatment

Having plotted the identified information risks on the information risk acceptance matrix, decisions (based on the organisation's information risk appetite) can be made as to the responses to be taken for each information risk. Typical risk treatment options include:

- terminate (cease the activity giving rise to the risk)
- transfer<sup>1</sup> (typically by passing some aspect of the risk onto another body such as an insurance company)
- reduce or increase (through applying, modifying or removing controls)

When describing risks, it is good practice to break the description down into a statement clarifying the cause, event and effect.

- accept (accept the risk).

When treating an information risk by implementing a control, an estimation should be made as to the effect of that control on the overall risk score (also see Chapter 6, Controls, for an overview of controls). In doing this, the residual risk score (amount of risk remaining) can be calculated and a decision made as to whether the residual score is still too high and further mitigation is required.

The organisation should ensure that the effort and expense involved in treating an information risk does not significantly exceed the loss (whether measured in financial, reputational, legal, ethical, etc. terms) which would be suffered should the risk materialise.

It is essential that, as part of the process, information risk owners and action owners are assigned. The information risk owner is the person or body which has the authority and accountability for managing an information risk. The action owner is the individual responsible for carrying out the activities to control the information risk. It is possible that the information risk owner and action owner may be the same person.

At a higher level, whether part of the organisation's pre-existing risk management framework or a specific information security governance body, there should be a review body which on a regular basis scrutinises the management of information security risk. See Chapter 2, Information security governance.

It is essential to understand which risks need to be addressed first, and what mitigation actions offer the most protection for the least investment in time and effort.

## 5.9 Information risk register

Identified information risks should be added to an information risk register outlining all the information risks faced by the organisation, what controls are being applied, and the initial, current and residual information risk scores. In this way, it is possible to see at a glance how exposure to an information risk has changed over time. Information risk management is a cyclical process, and risks should be reassessed on a regular basis (the degree of regularity depending on the significance of the risk) but also as part of managing changes to the operating environment. Changes in the threat landscape may allow the relaxation of certain controls or, equally, require extra controls.

A further reason for maintaining an information risk register is to provide an auditable account of decisions made. This will allow the organisation to manage identified information risks as well as to determine the overall information risk exposure. The register will also act as an historical record of the assessed value of each information risk over time.

It should be noted that information security risk assessment cannot be carried out and managed in isolation. Risks identified as part of the information security process should be integrated into the appropriate organisational risk registers. For example, information security risks which have the potential to impact on organisation strategies should be referenced from the organisation's overall strategic risk register.

## Summary

- Information risk management is a systematic, consistent, iterative process where risks are identified and assessed before being treated and monitored
- Information risk treatment options should not cost more to deploy and manage than the cost of the risk itself
- Information risk management should not be done in a vacuum, but as part of the overall organisational risk management process

<sup>3</sup>NB: Risk transference cannot entirely mitigate a risk, as reputational risk tends to remain with the organisation (e.g. TKMaxx's incident was due to activities of a third party, yet it was TKMaxx which experienced the reputational damage).

## Resources

Template for information risk management principles  
Development and use of risk assessment templates - UCL, case study  
Project information risk assessment – Requirements and expectations - UCL  
Service information risk assessment – Requirements and expectations - UCL  
Project information risk assessment – Capability - UCL  
Service information risk assessment – Capability - UCL  
Risk treatment plan – UCL  
Risk assessment methodology – Cardiff University  
Information asset register tool – University of Oxford

## Reading list

A complete set of resources necessary to perform an information security assessment based on the OCTAVE Allegro method  
[www.ucisa.ac.uk/ismt21](http://www.ucisa.ac.uk/ismt21)  
[www.cert.org/resilience/products-services/octave/octave-allegro-method.cfm](http://www.cert.org/resilience/products-services/octave/octave-allegro-method.cfm)

European Union Agency for Network and Information Security (ENISA) Risk Management Hub  
[www.ucisa.ac.uk/ismt22](http://www.ucisa.ac.uk/ismt22)  
[www.enisa.europa.eu/activities/risk-management](http://www.enisa.europa.eu/activities/risk-management)

ISO 31000:2009 Risk Management Principles and Guidelines  
[www.ucisa.ac.uk/ismt23](http://www.ucisa.ac.uk/ismt23)  
[www.iso.org/iso/home/standards/iso31000.htm](http://www.iso.org/iso/home/standards/iso31000.htm)

University of Oxford Risk Assessment of Information Assets  
[www.ucisa.ac.uk/ismt24](http://www.ucisa.ac.uk/ismt24)  
<http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/risk-assessment>

Risk management in higher education - A guide to good practice, prepared for HEFCE by PricewaterhouseCoopers  
[www.ucisa.ac.uk/ismt25](http://www.ucisa.ac.uk/ismt25)  
<http://dera.ioe.ac.uk/5600/>

Higher Education Funding Council for England (HEFCE) strategic risk register in which 11 key risk areas are identified  
[www.ucisa.ac.uk/ismt26](http://www.ucisa.ac.uk/ismt26)  
<http://webarchive.nationalarchives.gov.uk/20100202100434/http://www.hefce.ac.uk/about/standards/howweareaccountable/riskman/>

*This chapter describes how to approach security measures, or controls, and how to make them work in practice. It forms part of Stage 2 – Planning, assessment and evaluation and Stage 3 – Implementation, support and operation in the Toolkit Route map.*

### Key topics

- Definition of a control
- How to pick and assess controls
- What to do about “ready-made” sets of security controls

## 6.1 What is a control?

A control is a tool for treating risk. Controls can reduce the impact or likelihood of a risk, thus decreasing its overall rating. Many controls can be applied to treat a single risk, and, equally, one control can treat multiple risks. Controls can be selected by the organisation’s risk assessment (see Chapter 5, Risk assessment) or imposed by internal or external requirements (e.g. PCI DSS).

Some controls can be applied to the whole organisation (e.g. the authentication scheme, or retention schedules), while some can be specific to a particular scope (e.g. password lifespans, or patching policies).

The organisation should first consolidate its business and compliance requirements, and only then design and consolidate controls. This minimises duplication and redundancy.

## 6.2 Types of controls

Controls can be roughly grouped into three categories, as follows.

Table 2 - Types of Controls

| Category                | Examples                     | Reduces likelihood? | Reduces impact? |
|-------------------------|------------------------------|---------------------|-----------------|
| Preventative/ Deterrent | Training                     | Y                   | N               |
|                         | Pre-employment screening     | Y                   | N               |
|                         | Segregation of duties        | Y                   | Y               |
|                         | Secure media disposal        | Y                   | Y               |
| Detective               | Intrusion Detection System   | N                   | Y               |
|                         | Review of user access rights | Y                   | Y               |
| Reactive                | Burglar alarm                | Y                   | Y               |
|                         | Back-ups                     | Y                   | Y               |

Controls can fall into more than one category. For example, anti-malware software both prevents infection and acts to remove existing malware.

Controls can also be technical (such as anti-malware) or non-technical (such as keeping documents in a drawer overnight, rather than on a desk). Non-technical controls often involve changes to business processes, which

may require more involvement from different parts of the organisation to implement, but which are more cost-effective. When selecting technical controls, the organisation must always ask itself the question, “Why is this control the best or only option? Is there a non-technical approach which is more effective?”.

Different cultures may have very different attitudes to acceptable behaviour, which should be taken into account when designing controls (see Chapter 5, Risk assessment). For example, in some cultures, it is considered unacceptable to let a door close in the face of someone walking behind you – in this case, the organisation should consider alternative controls to pass-opened doors, such as turnstiles.

## 6.3 Control sets

There is no “perfect control set”, any more than there is a “perfect diet”.

There are many sets of controls available, some backed by government, others produced by professional bodies, and still more developed by community organisations (see the reading list for this chapter for a few examples).

Control sets are like diets – everyone is looking for a “quick fix”. Some approaches are faddish and incomplete and require huge lifestyle changes. Others require you to pay a third party to make all of the difficult decisions for you. Others start with good advice based upon fact, and expect you to interpret it to suit your situation. Unfortunately, just as there is no one menu which will suit us all, there is no one control set which will sufficiently protect every organisation.

Using governmental advice can be a good start, if there is a clear message.

The crucial point of difference between a control set and a diet, where the analogy breaks down, and which explains the fluidity in the information security sector (which far exceeds the confusion even in the nutrition sector) is the rapidly changing and volatile state of technology. Human biology is relatively static. Imagine if a person born thirty years ago was unrecognisable to anyone born twenty years ago, and could not eat the same food or even talk to them.

The more specific and technology-focused a control set is, the more effort it will take to keep it up to date – which is why managing people and business processes can be a better way to manage a risk.

Any organisation seeking to identify a control set to implement should assess it for stability (given the changing nature of technology), suitability for their needs, and other side benefits (e.g. will it make it easy to get government funding?). The control set chosen will almost certainly need to be augmented to fill in the areas where organisational risk tolerance differs from the tolerance of the authors of the control set.

Governmental control sets can be used to improve top level buy-in, as top management may have been contacted by governmental bodies asking for feedback on compliance with the currently popular control set. An example of an initial risk assessment which helped an organisation to raise awareness, gain support from governance and executive bodies and make the case for increased investment in information security controls was to take the CPNI 20 controls and assess: current organisational compliance (rated as red, amber or green), priority for action, actions recommended with cost, timescales and responsibilities.

### 6.3.1 A note on the ISO/IEC 27001 Statement of Applicability

The Statement of Applicability is one of the documents required to certify to ISO/IEC 27001. It consists of a mapping of the organisation’s list of selected controls to the list of controls in Annex A of ISO/IEC 27001 (which is the same as the controls in ISO/IEC 27002). Every information security control which is used by the organisation (in the environment being certified) should be in this list, even if they do not appear in Annex A of 27001. Justification should be given (briefly) for the inclusion of all implemented controls; and where a control listed in 27001 is not implemented, justification for its omission should also be given.

The purpose of the SOA is mainly to ensure that an organisation has not missed anything. The Annex is not intended to be a control set, or a means of bypassing a risk assessment. A good way to think of it is as a supermarket containing all the foods you can imagine – your list of controls is your shopping list. Going to this supermarket without a list and buying everything on the shelves will bankrupt you, and leave you with many foods you don’t need or want. Equally, implementing all controls in Annex A of ISO/IEC 27001 will be too expensive for the organisation, and will not meet its needs. That is why the list of controls in Annex A is best ignored until after the organisation has sorted out its list of required controls.

## 6.4 Implementing controls

Controls are only effective when completely defined, and implemented in the correct context.

For example, a policy developed by a small group, published on a website and left to the ravages of chance will

be unlikely to have its desired effect. Log files, as another example, in and of themselves have no protective or preventative capability. They need to be part of a detective control, and linked to incident response, in order to reduce the impact of incidents.

An effective control should be:

- developed through consultation with affected parties, transcending any internal “silos”
- designed to address a risk
- proportionate
- supported by top management
- tested
- implemented with appropriate awareness work to ensure that all impacted users understand what to do and have support in any transitional period
- managed, with non-compliance detected, followed up, reported on, and persistent issues handled effectively.

To put this another way, controls are a component of an ISMS; they do not replace it.

Implementation of a control should be managed as any other business change, using the techniques which the organisation finds most effective, and the management channels which are in place already.

## 6.5 Assessing and managing change

Business changes may change risk levels, introduce new sources of risk or new external requirements, which then cause controls to be revised. The impact of any new/changed/retired driver (see Chapter 3, Drivers) on existing controls should also be assessed (i.e. change or removal).

The impact on the organisation of each control introduction/change/retirement should then be assessed, so that any changes which are not feasible can be identified. As previously noted, this assessment should be done as early as possible, ideally before the organisation commits to a project or new service which brings with it changes which are not feasible to implement. For example, taking payment card data may result in specialist security software being required (file integrity monitoring), and hence a much higher cost for software licenses.

Using this information, the appropriate level in the organisation should then make a decision on the business change: should it go ahead?

Assuming that the business change will go ahead, once the changes to controls are clear, a plan should be agreed which leads to their implementation/alteration/removal (as relevant) in a suitable time frame.

## 6.6 Documenting controls

Controls deriving from requirements, either via risk assessment (see Chapter 5, Risk assessment) or via other drivers (see Chapter 3, Drivers), should be compiled into a single list, along with internally defined controls, to reduce the chances of unnecessary duplication and accidental omission. The source(s) of each given control should be recorded, so that changes in a driver can easily be propagated into policies, technical measures etc. Equally, should a question arise as to the necessity of a control, it will be easy to understand why it exists and the consequences of removing it.

In many cases, especially where legislation is concerned, an external requirement will not specify exact controls. In this situation, the organisation should use the driver to inform its risk assessment and control selection processes, with reference to its own risk appetite and legal counsel as appropriate. This ensures that legislation is not over- or under-interpreted.

In order to relate controls derived from external drivers to controls derived from risk assessment, the organisation should decide how to treat externally derived controls. They may be seen in one of two ways:

- as a way to address the risk of non-compliance (e.g. with the DPA)
- as a way to treat a specific information security risk (e.g. the risk of a user deliberately or accidentally leaking information).

Of these two options, the first is the easiest to do initially, but leaves externally derived requirements in a separate group, and does not, perhaps, encourage all controls to be treated equally. The second approach requires each control to be “deconstructed” to identify what risk (or risks) it is actually going to be addressing. This takes more time, but is a much more effective (and satisfying) approach.

## Summary

- Controls reduce the impact and/or likelihood of incidents
- Ready-made control sets should be considered carefully
- Controls form part of an ISMS – they do not replace it
- Controls should be traceable to the requirements/risks which they are intended to address

## Resources

Evaluating software security patches – Loughborough University, case study

Hacking before and after: How Certified Ethical Hacking (CEH) training changed my perspective on hacking – UCL, case study

Technical vulnerability management

Penetration testing

## Reading list

CPNI 20 Controls

[www.ucisa.ac.uk/ismt27](http://www.ucisa.ac.uk/ismt27)

[www.cpni.gov.uk/advice/cyber/critical-controls/](http://www.cpni.gov.uk/advice/cyber/critical-controls/)

10 steps to cyber security

[www.ucisa.ac.uk/ismt28](http://www.ucisa.ac.uk/ismt28)

[www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets](http://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets)

Educause IT Governance, Risk and Compliance Programme

[www.ucisa.ac.uk/ismt29](http://www.ucisa.ac.uk/ismt29)

[www.educause.edu/library/resources/it-governance-risk-and-compliance-higher-education](http://www.educause.edu/library/resources/it-governance-risk-and-compliance-higher-education)

Cyber Security Essentials scheme

[www.ucisa.ac.uk/ismt30](http://www.ucisa.ac.uk/ismt30)

[www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/317481/Cyber\\_Essentials\\_Requirements.pdf](http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf)

*This chapter addresses some of the considerations involved in designing an information management scheme and making it operate in practice. It forms part of Stage 2 – Planning, assessment and evaluation in the Toolkit Route map.*

### Key topics

- The benefits of having an information management scheme
- The components of an information management scheme
- Tips for creating and using a workable and appropriate scheme

## 7.1 What is an information management scheme?

An information management scheme provides a framework within which information can be identified, its security requirements determined and instructions given to those who may handle it. Although it may be tempting to have the information management scheme echo the full complexity of an educational organisation, this is not desirable and should not be necessary. A complex scheme is too easy to misunderstand and mistakes could expose the organisation to significant risks. The aim should be to have the simplest scheme that will satisfy the organisation's requirements: identifying this is likely to involve a series of iterations between theoretical and practical considerations. The most effective schemes take a pragmatic approach that can be understood by all their users.

An information management scheme, in a simple form, can be made up as follows:

- A classification scheme: a list of classifications with definitions to allow people to consistently classify information.
- A labelling scheme: a way for documents and other information to be visibly associated with a classification.
- Handling rules: information on how to use and protect information with each of the defined classifications.
- A process which explains how to use the above three documents (e.g. how to decide who is responsible for classifying a given item of information).

As usual, these documents should be supported by a policy statement, and endorsed by top management. The statement specifies the scope of the information management scheme; who is responsible for maintaining and controlling it; and what sanctions should apply in the case of non-compliance (sanctions can often be handled via normal disciplinary processes).

The organisation should appoint a suitable role(s) to develop this scheme (see Chapter 8, Roles and competencies), and ensure that the scheme is tested and approved (see Chapter 2, Information security governance).

## 7.2 Classification

In our daily lives we tend to see a huge number of attempts to mark information with a classification – “confidential”, “personal”, “commercial in confidence”, “private”, “off-the-record”, and even “classified”. In addition, there are formal schemes such as the Information Sharing Traffic Light Protocol<sup>2</sup> and the UK Government’s Security Classification scheme.

When designing an information management scheme for an organisation, it may seem prudent to implement all of the above classifications, if not more. However, a scheme that is too complicated will produce confusion, non-compliance and other unintended consequences – e.g. either information being seen when it shouldn’t be, or not disclosed when it needs to be. A scheme that is too simple carries the same risks, as it forces people to either over- or under-classify. It should be noted that the UK Government’s new scheme only has three classifications above the base level of unclassified – “Official”, “Secret” and “Top Secret”, of which the top level may never be encountered in most branches of the Government.

Classifications must apply to information, not to the particular form it is in: it makes little sense to say that a printed copy of a document must not be left on a desk, if computers with access to the same information are left logged in when unattended. As information changes format, it must experience a consistent level of protection.

## 7.3 How many levels?

To develop a classification scheme, the organisation should decide how few different sets of information handling rules it needs to use. In many situations, particularly given the need for consistency in handling across different formats of information, that turns out to be surprisingly small. Many organisations in the educational sector have settled on classification schemes with three or four levels, despite initially expecting that they would need more.

If the initial attempt at designing a scheme does produce a large number of classifications, the organisation should check for mixed or inconsistent treatments for different formats of information. This is likely to undermine both the actual effectiveness and the credibility of the scheme.

The classification levels chosen should be compatible with the classification structure implied by the Freedom of Information Act 2000 (FoIA). The Act effectively groups information into three classes with regard to confidentiality:

- information that is routinely published
- information that is disclosed subject to a public interest test
- information that is not disclosed.

There is no advantage in sub-dividing the first of these classifications, since anyone can obtain the information merely by asking for it. There may be some point in sub-dividing the third (and possibly the second) if there are clear divisions within the FoIA categories. For example “does not leave the building” and “viewable from outside” might be different sub-classes of “not disclosed”. A classification scheme whose breakpoints do not match those of FoIA may be both confusing and liable to error. Note: this also applies to the Data Protection Act 1998.

Business Impact Levels (BILs), as used by the UK Government, are a way to formalise the assessment of risk. However the seven columns and significant detail in their Impact Level tables are likely to be too complex for practical information classification schemes. Noting the Business Impact Levels that are likely to match the organisation’s own information classifications may, however, be a useful check, especially if the organisation will be expected to engage with BILs in its interactions with other organisations, e.g. funding bodies.

Classifications should take account the information’s requirements for integrity and availability, as well as confidentiality.

### 7.3.1 A note on special cases

Encryption keys must be handled with extra care, as they constitute security controls in themselves, not just information. Equally, information on security controls, such as plans for a security system, lists of roles with privileged access, maps of sensitive areas, results from penetration testing, and risk treatment plans, are special cases where the risk may be intrinsically higher.

### 7.3.2 Naming the classifications

Once the organisation has agreed the number and definition of its classifications, they need to be given easy-to-recognise names. Classification schemes are harder to use if names don't form an obvious sequence – is “confidential” more or less restricting than “personal”, for example? If a classification scheme does have a sequence, then its names should make that sequence obvious: something like “non-sensitive”, “sensitive” and “highly sensitive”, or “low integrity”, “medium integrity” and “high integrity” (e.g. research data) works well.

Classification instructions/definitions should be clear and easy to follow, so that information owners can quickly classify their information, and have appropriate cues during information creation (or at receipt) to remind them to classify information. Guidance for information owners may also include policy and regulatory requirements that apply to particular kinds of information, and which require them to be given a particular classification. For example, personal information is likely to have an elevated classification.

## 7.4 Labelling

It is good practice, and may be a requirement, to label information with its classification. Different formats of information will need to be labelled in different ways: for digital documents or e-mails the label should be in a standard place in the digital content; for paper it should be on the file or envelope (double envelopes may be required if the actual classification needs to be protected); for on-line systems the label may need to be on a login page if it's not possible to put it on every screen.

The important thing is that the label is understandable (this is why the classifications are created first), and visible to all readers, even those who only skim the start of a message. Everyone who sees information must know how to handle it.

It may be necessary to consider information as being of two types: structured (e.g. files in a database or CMS) and unstructured files (anything ad hoc, e.g. in a private file system, email, or in a notebook). Structured information will be much easier to label than unstructured information, so it may be necessary to consider how information of value is being managed in general, in order to make labelling and handling it more feasible.

One method for labelling information, which is simple but very effective, is to specify that everything in a particular system, or environment, is automatically of a particular classification. This approach requires there to be a verification process at the point where information is introduced into the system, to make sure that information with a higher classification is not entered into the system, and at the point of data extraction, to ensure that it is labelled and handled effectively outside the system.

While the classification label, along with a handling scheme, defines how information should be handled, labelling related to confidentiality can also be used to indicate who should handle the information. Here the most important thing may well be that those who are not entitled to see the information should be able to immediately recognise that fact, return the information and report a security breach. Labels also need to make clear to those who are entitled to see the information who they may share it with. Provided that labels meet these twin requirements of being immediately clear to both authorised and unauthorised recipients, they can be relatively flexible. For example, information might be labelled with the department(s) where it should be used, or with the name of a project, event or function.

The “how” and “who” labels may appear together, for example as “SENSITIVE:Finance”. “SENSITIVE:Finance” and “SENSITIVE:Physics”. They must require the same handling rules in all departments, otherwise the security of the department's information may be breached by accident.

## 7.5 Handling

Each classification of information should have its own set of rules for how that information should be handled. Although many information management schemes concentrate on the confidentiality of information, rules should also address the organisation's requirements for integrity and availability. These too, must be consistent across different formats of information: making a written note of information from a conversation or phone call, and ensuring that work is not left on a single laptop or memory stick, both protect the availability of information. Ensuring that only authorised individuals can alter information, whether it is on paper or digital form, protects its integrity.

Information handling rules will probably have emerged during the development of the classification levels (especially if the advice above has been followed), but it is recommended that they be revisited after the initial decision on classifications, to ensure that they are appropriate, clear, and provide consistent risk management.

Be careful if borrowing terms from classification schemes in other sectors. If the organisation decides to use a classification entitled “Secret”, for example, then that will mean something very specific to anyone who has worked with Government documents, and that meaning, and related handling rules, probably are not consistent with those defined by the organisation.

Each classification should relate to unique rules for how information with that classification is handled: if two different classification levels impose the same rules, information owners are likely to be confused about which classification they should apply, and users are less likely to understand how they should handle the information. A useful test for consistency is to consider which format of information a determined attacker would find it easiest to gain unauthorised access to: do they need to hack central servers or can they just hang around in the coffee room? With consistent handling rules, the difficulty (or ease) of unauthorised access should be about the same for all formats.

Once the organisation has established and agreed a consistent set of handling rules, it should look at how current processes require information to be used, to identify any inconsistencies. For example, if tender documents have been given the highest classification, but have to be sent to external assessors for review, then a “does not leave the building” rule will not work and the classification, and the handling rules, should be reviewed and revised as necessary.

Organisations should therefore expect to make a series of adjustment to classifications and rules as inconsistencies with either the organisation’s risk or operational requirements are discovered. The goal should be a classification and rules that satisfy both.

## 7.6 Example handling scheme

Here is an example of a three-tier approach, which focuses exclusively on protecting the confidentiality of information. If integrity and availability are of particular interest (e.g. if the information in question is likely to be viewed on a website), then the handling rules should be extended to protect these attributes, in addition to confidentiality.

**Table 3 - Three tier information handling scheme**

|                                     | <b>Classification 1<br/>(no concern)</b> | <b>Classification 2<br/>(slightly unsettled)</b>  | <b>Classification 4<br/>(genuinely scared)</b>  |
|-------------------------------------|--|---|---|
| Store, process and transmit - where | Anywhere                                 | Premises of organisation or trusted third party (can take work home with minor precautions) | High security location (can't take work home unless you live in a bunker)   |
| Store, process and transmit - how   | Any method allowed                       | Only approved methods (e.g. encrypted, or via registered post)                              | Storage only in bunker. Processing with formal approval on high security systems. Hand transport by security personnel only. Face to face discussions only. |

## 7.7 Documenting the scheme

Once an information management scheme has been designed, it must be documented, for the benefit of both information owners (who will be marking information with the relevant classification), and information users (who need to understand how to handle material with each classification).

One way to document handling rules, and to highlight the need for consistency across formats, is to start with the high-level risk the information needs to be protected against, then list the measures to be taken for each classification level and each format of information. For example:

**Table 4 - Example documentation for handling rules**

| <b>Risk</b>      | <b>Information should not be seen/heard by unauthorised people</b>   |  |
|------------------|--|--|
| Sensitive        | Don't leave papers lying around; lock your screen when you leave it; don't have conversations or phone calls in public places. |  |
| Highly sensitive | Keep paper under lock and key; password-protect individual files; have conversations only in private offices.                  |  |

### 7.7.1 Asset inventories

It is no longer required by ISO/IEC 27001 that an asset inventory be created or maintained. If the organisation, as a result of a risk assessment, decides that one would be appropriate, perhaps in certain areas, then this should be managed just as any other control, providing additional focus to the information management system.

### 7.7.2 The information management policy and process

An information handling policy and process are required that describe when and how the information management scheme should be applied. They should not only explain the classifications and labelling rules, but provide a process for classification- who should do it, how, and when? How should it be audited and verified to ensure that it is being applied consistently? The process should also address how to deal with situations where there are differences of opinion, and where information is found to have been incorrectly classified /labelled /handled (e.g. what steps should be taken to identify potential incidents).

A particular characteristic of educational organisations is that information may have different classifications and different points in its lifecycle. Both research data and exam results change their requirements for confidentiality and availability after publication, for example. The information management process therefore needs to be able to handle these time-related aspects. Lifecycles, like classifications, are best identified when the collection or creation of information is planned, whether the information is destined for publication, archiving or destruction. The Jisc model Records Retention Schedules may be a useful starting point.

## 7.8 Information management as part of an organisation's ISMS

An Information Management Scheme is actually a set of controls. In order to ensure that information classifications are applied appropriately, and that information is handled suitably, it is important to handle the controls in the context of the wider ISMS (also see Chapter 6, Controls). Here is an example of how this could work.

1. Roles are chosen to take responsibility for classifying, labelling and handling information (see Chapter 8, Roles and competencies) – this may include the information owner.
2. Decisions are made as to how the information management scheme is maintained and how compliance with it is measured (see Chapter 10, Measurement).
3. Top management are regularly informed of how the scheme is working, and whether there is anything they need to be aware of, or make decisions on (see Chapter 2, Information security governance).
4. Staff are trained in the content and use of the scheme (see Chapter 9, Awareness raising).
5. Problems with the implementation and running of the scheme are identified and addressed (see Chapter 11, When things go wrong: nonconformities and incidents).
6. Opportunities to make the scheme work better are identified, assessed and implemented if appropriate (see Chapter 12, Continual improvement).

## Summary

- An Information Management scheme should comprise: a classification scheme, a labelling scheme, handling rules and processes to define how these all interact
- A classification scheme describes how information should be classified
- A handling scheme describes how information given a particular classification should be treated
- Don't have more classification levels than necessary, or practical
- Labelling can indicate both the classification and who should (and should not) see the information
- Handling rules must provide consistent protection across different media

<sup>2</sup><http://www.terena.org/activities/tf-csirt/publications/ISTLP-v1.1.pdf>

## Resources

Information Classification Scheme – University of York

Development of an Information Classification and Handling Policy – Cardiff University, case study

Information Classification and Handling Policy – Cardiff University

University Guidance on Classification of Information - University of Oxford

## Reading list

UK Government information classification scheme

[www.ucisa.ac.uk/ismt31](http://www.ucisa.ac.uk/ismt31)

[www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/251480/Government-Security-Classifications-April-2014.pdf](http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf)

CESG, Business Impact Level Tables

[www.ucisa.ac.uk/ismt32](http://www.ucisa.ac.uk/ismt32)

[www.cesg.gov.uk/publications/Documents/business\\_impact\\_tables.pdf](http://www.cesg.gov.uk/publications/Documents/business_impact_tables.pdf)

JISC records retention schedule

[www.ucisa.ac.uk/ismt33](http://www.ucisa.ac.uk/ismt33)

<http://bcs.jiscinfonet.ac.uk/>

*This chapter outlines the roles and responsibilities, and supporting competencies, required of staff within an organisation in order to implement and sustain a successful information security management system. It forms part of Stage 1 – Foundations and Stage 2 – Planning, assessment and evaluation, and Stage 3 – Implementation, support and operation in the Toolkit Route map.*

### Key topics

- The roles required to deliver effective information security in an organisation
- The responsibilities that may be assigned to individuals' roles or functions
- The core competencies required of key groups of staff

## 8.1 Who does information security?

Information security is the responsibility of all members of an organisation.

There are few roles which do not involve interaction with information or information management systems (either paper or IT based). Staff present the greatest risk to information security; although malicious action by individuals cannot be ruled out, there is a greater risk of breaches occurring as a result of ignorance, inconsistent risk tolerances, or carelessness. Roles within the organisation share responsibility for achieving and maintaining appropriate information security.

At the top of the organisation, governance and oversight must be the priority; the creation of goals and objectives and the balancing of information risk (see Chapter 2, Information security governance). Top management roles have top-level responsibility for implementation of objectives. Senior information security specialists provide specialist advice and support to executives, along with legal roles and other information management roles (e.g. records managers). Asset owners and technical specialists supply the decisions and expertise to make goals and objectives a reality, while operational staff, students and contractors need to be aware of, and comply with, information security requirements which apply to their roles.

An individual's role in the organisation should dictate their level of responsibility for information security processes and controls. The organisation should ensure that responsibilities are appropriate and fit-for-purpose. These responsibilities should subsequently be reflected formally in the agreements between the organisation and its members – whether these are employment contracts, or any other legal document defining the relationship of a member and the organisation.

Implementing a policy and technical measures goes some way to achieving a good level of information security in an organisation, but should be supplemented by individuals having an understanding of the value of information security and how it relates to their jobs (also see Chapter 9, Awareness raising). Different roles and job functions require different levels of competence, ranging from fairly elementary to a deep understanding of a wide range of topics, and may therefore require different levels of training and awareness.

Who is responsible for information security in your organisation's top level body?

It is important to distinguish between personal and organisational risk tolerance.

## 8.2 Top management – decision makers

Information security decision-makers, or “top management”, manage information security strategy (including Chapter 12, Continual improvement) and governance (see Chapter 2, Information security governance), as these relate to the organisation, its values and its goals. They will have responsibility for determining strategy, policy and, critically, budget. Decisions which they will take include:

- investment in new technologies
- approving a training programme
- authorising a data classification scheme (see Chapter 7, Information management)
- authorising audits to ensure processes and policies remain fit for purpose.

Decision-makers exist at both the organisational and departmental levels within higher and further educational institutions. This leadership should be visible within the organisation.

The risks associated with information need to be owned by a member of top management. In many organisations, this role is known as the Senior Information Risk Owner (SIRO). The role of the SIRO focuses upon ownership of information risk, which is necessary for good information security governance (see Chapter 2, Information security governance).

It is likely that the SIRO will be part of the portfolio of responsibilities of a top level operational manager within the organisation (e.g. the Director of Governance, Risk and Compliance). It is a key decision making role which, in order to be effective, must fit in with any existing risk management hierarchy. The role of the SIRO is an established part of most public sector ISMSs, notably in the NHS.

The SIRO acts as lead and champion for information risk management initiatives and ensures that top management are adequately briefed on strategic level information risk management issues. The SIRO can also authorise acceptance or mitigation of major information security risks that deviate from agreed standards, and determine when (and by whom) breaches of information security will be reported to relevant external authorities.

### 8.2.1 Competencies of top management

The need to implement an organisation-wide information security management system will be competing with many other initiatives; top management must understand why information security is important to the organisation to ensure that it is adequately funded. Specifically, they need to understand:

- the principles of risk management and the part that information security management plays in mitigating risks
- the potential risk and impact of an information security breach
- that information assets vary in their sensitivity and importance and hence may require different approaches to information security.
- In addition to the above, the Senior Information Risk Owner (SIRO) for the organisation needs to have:
  - the communications skills to ‘sell’ why information security is important to the other members of top management
  - the ability to link information security issues to the overall organisational strategy.

## 8.3 Asset owners

A number of senior staff will have de facto responsibility for the information assets under their control. For example, the HR Director will have responsibility for all the personnel information held within the organisation and will, in part, be responsible for determining how it is used, accessed and stored.

The responsibility may be implicit, for example the post holder will be the senior business owner of processes relating to the given asset. Alternatively, it may be explicitly outlined, for example in the terms and conditions associated with research grant awards for principal investigators.

The responsibility will cover being aware of, and authorising, the uses to which asset(s) are put. It may also extend to ensuring that those that have access to assets are trained and are operating appropriately.

Asset owners must have sufficient seniority to take decisions about the protection of their asset from a strategic perspective. Issues may arise here, as information asset owners may have no direct management control over dispersed instances of those assets. In this case, the focus of the role may be on setting security policy/standards for handling of the asset.

Do you have a mechanism to establish asset owners in your organisation? Does, for example, the HR Director understand that s/he has this responsibility?

### 8.3.1 Competencies of asset owners

Organisational asset owners, such as the HR Director, will be members of the organisation's information security group and so should have sufficient understanding in order to be able to inform the decisions made by the group and to understand the impact on their aspect of the organisation's business. Specifically they need to understand:

- the principles of risk management and the part that information security management plays in mitigating risks
- information security principles
- how to classify information assets
- the risk and impact of an information security breach affecting their assets
- the implication of organisational information security policy on the aspect of the business they are responsible for
- the contribution which policies and processes in their business areas make to organisational information security
- the processes relating to the maintenance and use of their information assets.

Understanding the interaction between business functions and information security is particularly critical for those responsible for information relating to people in the organisation.

Maintenance of the information asset may be devolved to departments across the organisation. Consequently some of the responsibility for ensuring that information security policy and principles are applied appropriately to assets may also be devolved to individuals at a departmental level (for example, a departmental administrator). Individuals fulfilling these roles will need the same competencies as the organisational asset owner, albeit applied in a departmental context. Overall responsibility, however, remains with the organisational asset owner.

## 8.4 Dedicated information security roles

The role of a Chief Information Security Officer (CISO) is a necessary part of information security management. The CISO is the head of the information security function within an organisation, and is usually responsible for establishing and maintaining the enterprise vision, strategy and programme to ensure information assets and technologies are adequately protected.

There will be a number of roles required to support the CISO that are focused on advice, implementation and monitoring. These are often hybrid roles requiring an understanding of legislative requirements and organisational policy and, in IT focused teams, may also require technical knowledge.

Responsibilities may include activities such as conducting risk assessments, monitoring and reporting breaches and monitoring for potentially malicious activity (see Chapter 10, Measurement), and developing processes to ensure that access to systems is removed in a timely fashion from those leaving the organisation. These responsibilities may be vested in an individual or in a team; sample job descriptions are given in the Annex: Example resources to accompany the Toolkit.

The individuals fulfilling the implementation and monitoring roles will often form the core of the team to manage security incidents in the organisation. The team will have responsibility for the monitoring, detection and reporting of security breaches (see Chapter 11, When things go wrong: nonconformities and incidents), for the implementation of centrally mediated measures, and for providing advice and guidance to local areas. The team will also be a focal point for notifications of potential breaches of security and will lead internal investigations. In some instances, there may also be a sub-team with specific responsibility for IT-based information security.

The overall information security team may adopt a collaborative approach to inform decisions and guidance; a case study from UCL included in the Annex illustrates this approach.

Where possible, areas which handle subjects strongly related to information security should be integrated, or work closely together. Relationships should be maintained with areas which influence information security, but which have their own identity (the physical security department may be a good example of this).

Legal professionals will also exist within the specialist information security space, to handle situations relating to Data Protection, Freedom of Information, Information Rights management, Information Governance Toolkit compliance, payment card security, intellectual property and other related areas. Some roles also audit and review activities as part of organisational processes which do not directly or explicitly involve information security or information technology - this can include paper-based information or physical access to organisation facilities.

### 8.4.1 Competencies of information security professionals

Information security roles within an organisation must have a variety of skills and expertise in order to fulfil their roles. They will need people skills in order to communicate to a wide range of the organisation's staff, process skills to understand how information/data is used and the risks those processes may present, technical skills (knowledge of law, IT skills for those in IT focussed positions), and a high level appreciation of what IT protection can be delivered for those at a CISO level). They will need to:

- understand the nature of threats and risks to the organisation's information
- understand information security legislation and its application within the organisation
- understand organisational policy and its relationship to the organisation's information assets
- be able to communicate at all levels within an organisation to promote the need for information security
- understand the processing of information assets.

There are a wide variety of skills frameworks which can be used to measure and develop information security competence, including:

- The C ESG Information Assurance Programme
- IISP Skills Framework
- ISACA qualifications (e.g. CISM)
- ISC2 Common Body of Knowledge and qualifications (e.g. CISSP)
- SANS programmes.

There is no "best" scheme – an organisation should evaluate their requirements and decide which scheme, or schemes (if any) is/are most suited to their needs.

### 8.4.2 Competencies of legal and compliance professionals

Roles with responsibility for legal advice will require a good appreciation of how their specific field fits into the wider organisation's approach to information risk management. They also have to be able to enable the organisation to be aware of and comply with legal requirements – some of which may vary depending upon the country in which information is being handled. They will need:

- to understand the relevant laws and contracts which relate to the information being handled by the organisation
- to maintain cordial relations with external bodies which impose requirements upon the organisation
- to liaise closely with information security professionals to ensure that policies and advice are legally acceptable
- to be able to negotiate with internal and external parties and achieve a common understanding of ambiguous or conflicting requirements, or agree approaches to handling risk which do not exactly match external requirements
- to be able to liaise with areas across the organisation to advise on and provide approval (as appropriate) for proposed activities.

## 8.5 Other roles

Almost all individuals in any organisation interact with information in the course of their activities and can therefore impact information security. This can include staff who handle personal information, faculty administrators managing student data, researchers developing intellectual property and managing sensitive data, and students using the organisation's infrastructure to conduct their studies.

Principal investigators, as the lead individuals on research projects, will create information assets during the course of their research. There is, for publicly funded research, growing emphasis on the curation of research data and open access to both research outcomes and the data that informed it.

A significant volume of research is funded by commercial organisations. Such research may be carried out to meet the specific needs of the funder, who may need to protect the commercial value of the research and related data. Research contracts with commercial organisations may well stipulate that the data and outcomes from the research are commercially sensitive and so need to be held securely, and require a data management plan in advance as supporting evidence. In addition, if medical data is being received, additional requirements such as the Information Governance Toolkit may need to be satisfied prior to the provision of data.

Roles which are engaged in the delivery of administrative services will have a greater level of responsibility for security of the information their service holds, by virtue of the fact that they will have higher levels of access than those that merely access the information on a read-only basis.

### 8.5.1 Competencies of research leads

Responsibility for the security of the assets generated by a research project lies with the grant holder – often the Principal Investigator (PI). This implies that the grant holder also has responsibility for the conduct of any members of the research team involved in their project. PIs (and their teams) will need to understand:

- information security principles
- the sensitivity of the information assets that will be used and/or generated by their research (whether they are commercially confidential, personal, or ethically sensitive)
- how to apply appropriate security measures to sensitive data
- the likely impact of an information security breach (relating to the information they are handling) on their organisation and on their own professional standing.

### 8.5.2 Competencies of contractors and third party organisations

Third party contractors coming into the organisation are usually specialists or professionals, and it is easy to assume that their expertise also extends to information security. In fact, the converse is true; they are less likely to appreciate local organisational information security arrangements. Those responsible for managing the appointment of contractors should be aware of the risks they pose. Contractors should be required to sign agreements that recognise information security requirements or complete appropriate training before beginning work.

Similarly, whilst adequate security constraints may be in force for employees and contractors, those same levels of safeguard may be overlooked when dealing with third parties, such as hardware and software suppliers, consultants and other service providers. See Chapter 4, Scoping for advice on managing third parties.

### 8.5.3 Competencies of administrators

Administrative staff need to be able to:

- understand the need to protect information (much of this may be tied to the need to adhere to data protection principles) and the risks of not protecting information
- apply information security principles when dealing with information such as staff and student records
- understand how the information is being used.

### 8.5.4 Competencies of all staff

The majority of staff will have access to a limited range of systems and will require a clear understanding of relevant information security principles. The relevant competencies are:

- to understand why protecting information is important
- to understand the relationship between the information they maintain and information security and hence their responsibility to maintain data accurately and in a timely fashion
- to be able to distinguish between types of information (and hence, what is important to protect)
- to understand why it is good practice to back up data, change passwords, etc.

The final point is important to ensuring accurate data – whilst it may be clear that there is a statutory requirement to record staff sickness absences, it may not be apparent to the person entering the data why some details may be required. For example, HR staff may not be aware that entering an end date against an employee's record will trigger the termination of access to IT systems and buildings. Consequently timely entry of that data may mitigate an information security risk. Understanding the use of data and its importance to the organisation assists in ensuring its accuracy; central administrative staff may have a role in educating those maintaining data within departments on how the information is used.

How well is responsibility for information security embedded in individual job descriptions in your organisation?

## 8.6 Students

Although much of the focus of information security policies is on staff responsibilities, students also share responsibility for ensuring the security of information and the systems they use. As with staff, levels of responsibility vary. The majority of taught students will only have read access to data and perhaps the ability to update their own records, but they will still need to adhere to regulations and not place the organisation at risk by introducing malware or other similar activity. However, postgraduate research students may have direct or delegated responsibility for critical information and as such, should be made aware of their responsibilities and good information security practices.

### 8.6.1 Competencies of students

Students have access to an organisation's systems and may inadvertently present a risk to the organisation. They may also have access to (and the ability to update) their own data. Students like staff, will have consented to the organisation's regulations for the use of IT facilities and these will be linked to student terms and conditions and hence disciplinary measures. However, there is also a need (particularly for new entry undergraduates) to raise awareness of information security and for them to understand the need to protect their own personal data. In short, the majority of taught students will need a basic awareness of sound practice, supplemented by reinforcement of key points from the regulations.

Postgraduate research students may require an additional level of awareness and competency, particularly if they are making use of personal data for their research, or are part of a wider research project (for example, as a research assistant).

## Summary

- The organisation's information security policy should define the roles and responsibilities required of staff
- All staff have responsibility for information security; this responsibility will be included in general terms and conditions of employment as well as individual job descriptions
- An information security group should be established at a high level, chaired by a member of top management with specific responsibility for championing information security and including owners (and representatives of owners) of key information assets
- A team to monitor and implement information security measures should be established and should be represented on the information security group
- The information security policy needs to be supported by effective personnel procedures

## Resources

[Job description template - Information Security Manager](#)  
[Job description template - Senior Information Security Specialist](#)  
[Job description template - Information Security Specialist](#)  
[SFIA competencies](#)  
[Collaboration between security administrators and academic researchers – UCL, case study](#)

## Reading list

No items.

*This chapter covers the various justifications for, and approaches to, improving awareness of information security, as well as mistakes to avoid. It forms part of Stage 2 – Planning, assessment and evaluation and Stage 3 – Implementation, support and operation in the Toolkit Route map.*

### Key topics

- The different ways to target awareness communications to members of an organisation and to specific groups, as well as related challenges
- The qualities that awareness material should have in order to get attention and support individuals in developing the necessary security skills
- How to align awareness activities with the rest of the organisation, in terms of managing risk and measuring effectiveness

## 9.1 Introduction

Information security is a collective responsibility for all members of an organisation. Members of the organisation must be appropriately aware of the risks to information within their role, and how they should use processes and technologies – as provided or sanctioned by the organisation – to manage those risks. Skills must be developed through engagement with individuals and teams working with information, coupled with delivery of targeted knowledge to those who can apply the expertise in practice. Evidence should be available to external parties to show due diligence in making staff aware of their responsibilities, for example after a data protection incident.

## 9.2 Awareness, education and training

Awareness activities help individuals in an organisation to recognise information security concerns that relate to their role, preparing them for education and training. Here we refer to security awareness, security education and security training, three distinct stages in changing a person's behaviour. The following is a user-focused view demonstrating where each may be applied:

**Table 5 - Choosing awareness approaches**

| Reason for not doing the “right thing” | Targeted intervention |
|--|-----------------------|
| Don't know what it is                  | Training              |
| Don't know how to do it                |                       |
| Don't think it makes sense             | Education             |
| Never think of doing it                | Awareness             |
| Have no reason to do it                | Motivation            |

For further information see Security Awareness, Education and Training in the reading list.

Security awareness encourages people to be interested in security, by attracting attention and conveying the effect security has within their roles.

With increased awareness, people respond better to security education – materials or courses that provide information about threats and vulnerabilities, and the actions individuals should take to protect themselves and the organisation. This can effect a change in perceptions and attitudes towards security.

Realising change in behaviour – the breaking of old habits and establishing of new habits – requires security training. Through a programme of training new behaviours are presented, but also tested and corrected to develop competencies and skills. Security training must be based in the work context and address specific security needs, and needs to be repeated enough to form the right habits. Monitoring capabilities and user feedback channels should be provided to determine the effectiveness of the programme. In the remainder of this chapter awareness, education, and training will be collectively referred to as awareness activities.

### 9.3 Triggers for awareness activities

There are various triggers for awareness, education and training activities within an organisation. Numerous external and internal factors can require awareness activities, beyond response to breach events and ongoing management of risks. These can include new laws or government initiatives which directly affect the organisation, updated or new technologies, or changes to organisation strategy or management. Trigger events, such as a revision to the Data Protection Act for example, should be identified and responses formulated at a strategic level through dialogue with decision-makers across the organisation (see Who does information security? within Chapter 8).

Communication channels should be maintained to support response to trigger events (rather than being developed in response to an event). A coordinated response also limits awareness content to that which is necessary for members of the organisation - this is important, as security is an enabling task supporting people in doing their job. Referring to the previous section, members may require awareness, education or training, depending on how the trigger event affects their work.

Members may also look to the organisation to provide guidance to address concerns or a desire to work more securely. Factors can include the vicarious experience of information security threats and visible enforcement of policies, but also social elements such as wishing to avoid embarrassment, demonstrating allegiance to the organisation and respect for others, and maintaining the reputation of the organisation. Factors should be identified through user engagement activities such as targeted surveys, regular involvement in team talks, or dedicated feedback channels within the organisation. (see Who does information security? within Chapter 8).

### 9.4 Foundations of an awareness programme

The training that individuals receive should align with the information risks that they need to manage as part of their role. The management of risks should then drive decisions within an awareness programme, including how to prioritise messaging to both address top risks for specific groups and limit the draw on members' attention.

Whilst general awareness raising is extremely important, the organisation should start with the clear message that compliance is required, both to encourage appropriate behaviour and to demonstrate to third parties, such as the ICO, that it takes information security seriously.

See Chapter 5, Risk assessment, for a discussion of risk management – a risk-driven awareness programme tempers the amount and relevance of training, through regular review of risks as the operating environment and threat landscape change. Messaging should also align with the values of the organisation, and the shared sense of professional responsibility for upholding those values.

An awareness programme cannot necessarily achieve its goals through fixed-period computer-based training alone; embedded training develops skills to address risks as they arise within the production task i.e. the person's job.

Good training requires appropriate resources and expertise. Trainers must be prepared to help individuals repeat awareness activities sufficiently often to form secure habits. Monitoring of the internalisation of awareness material, and the effects of awareness campaigns upon the operating environment, should be implemented, as well as a capacity for corrective feedback while skills are being developed (rather than as an isolated, static, one-off exercise). The organisation (specifically those managing the application of the awareness programme) should be prepared to dedicate extra resources to those who may fail to develop skills despite training and feedback – these individuals or groups may benefit from alternative solutions such as supporting processes or technologies rather than the application of more training.

## 9.5 Identifying channels for an awareness programme

There are many ways to communicate an information security message to target audiences. There is a right place for every format, with advantages and disadvantages to each approach. Approaches include:

- physical hand-outs such as leaflets, fact sheets, and comics
- on the job person-to-person guided work
- electronic communications (email, enewsletter)
- fixed-place messaging (posters and banners, fairs and seminars)
- persistent messaging such as screensavers
- videos/podcasts/webinars
- dedicated websites
- online intranet tools (wikis, forums, blogs) and training materials.

The US National Institute of Standards and Technology (see the NIST handbook in the reading list) separates activities by teaching method:

- media may act to improve recognition;
- practical instruction improves skills;
- theoretical instruction e.g. seminars improves understanding.

When designing awareness materials and approaches, the organisation should consider how long these will be valid for. For example, posters will “fade into the background” after a while, and people will forget what they learned in a course.

The ENISA publication *The new users guide: how to raise information security awareness* notes the advantages and disadvantages of various approaches. Note that there should be a recognition of general communications intended for all members of the organisation (supporting the values and intended image of the organisation); targeted communications for specific groups requiring particular competencies based on the risks they must manage (see Chapter 8, Roles and competencies), and targeted behaviour change activities that address specific scenarios (which especially can involve interactive or embedded training). Note that individuals learn mostly from doing, then less so from others around them, with formal training having the smallest impact.

The *Raising user awareness of information security - Cardiff University case study* demonstrates an awareness programme which uses a range of approaches together - doing so can serve to reach a wider audience within the organisation.

## 9.6 Identifying content for an awareness activity

Organisations can target behaviour change further by developing content around key risks or assets (see Chapter 5, Risk assessment). Engagement with individuals and local decision-makers may take time and resources, but can identify how vulnerable assets factor in the working day – awareness activities must support individuals to manage risks themselves. Awareness activities must be targeted so as to identify the right content for the right task, for the right audience. This may not necessarily be targeted at a departmental level, but otherwise scoped by profession or role (see Chapter 8, Roles and competencies). Regulate the scalability of the awareness programme with the level of targeted training for specific groups, applying a best-effort approach. Ideally education materials will empower users, avoiding “don’t” mandates wherever possible.

Carefully-designed survey exercises or user quizzes can identify the needs of technology users and those handling information. This includes capturing how groups use IT facilities and sensitive information. The ENISA publication *The new users guide: how to raise information security awareness* includes template user questionnaires. Surveys and questionnaires provide the user perspective, and engagement with decision-makers and implementers identifies the system-level and strategic measures for monitoring the effectiveness of awareness activities.

The organisation should also consider how messaging around security relates to promoted values. Content should be able to change the way people think about security and make it fun and interesting (through cartoons or games). Role models – ideally organisational leadership – must be seen to follow the rules. Training should then be supported with strategic buy-in and tailored to those with authority and influence. Materials should be of appropriate technical level, as technology-related information can fall on deaf ears. Certain buzz-phrases can also cause a negative reaction (e.g. “information security”, ironically).

For the design of security messaging, the organisation should be realistic in the demands made on user time and attention. Some principles from advertising may be useful: try to make material informative, brief, visual, attractive, unexpected, or funny. The posters appended to Cardiff University's case study on raising user awareness of information security, in the resources section at the end of this document, demonstrate some of these qualities in practice.

## 9.7 Arguments for different audiences

Distinct roles within organisations should be considered when planning for effective awareness activities (see Chapter 8, Roles and competencies). Awareness activities are generally concerned with the enabling task of security that supports a person in their job. For different groups there will be different risks to manage, and in turn different situations where individuals need to make the right decisions or know who to contact (where the security outcome can depend on actions taken in the moment). There will also be routine tasks, and novel problems where existing skills must be adapted based on the individual's reasoning of the situation.

Every member of the organisation should have the skills to use the organisation's facilities securely in their role. In using basic organisation facilities such as provisioned email accounts, all members likely need some basic comprehension of the threats posed by phishing, spam, and social engineering. There is also a need to manage regular access to system accounts (through passwords or other authentication technologies), as well as the management of data according to the organisation's policy (see Chapter 7, Information management, for reasons why an information management scheme must be easily understood). Information security extends to all forms of information/records, not just electronic copies (for example exam scripts, paper-based records, etc.). Mobility activities may require instruction on how to work remotely, use teleconferencing facilities, and work at conferences/events in a secure manner (not just with technology, but also in respect to information that is shared during those activities).

Staff and management should appreciate the impact of their actions on organisational reputation, as should students (potentially including recent or not-so-recent alumni). For those involved in securing funding, professional reputation is important, and security events can impact upon this - they will want to know how to protect their standing in the community. Those involved in research must manage intellectual property (unpublished work, research data, sensitive data, personal data), and those managing sensitive data must have the skills to appropriately adhere to data protection regulations. Staff with administrative duties must, amongst other things, consider protection of student coursework records, management of staff payroll details, and on- and off-boarding of staff or students to managed systems. Temporary or irregular visitors and collaborators may need a highly-targeted crib sheet that outlines their responsibilities even when they may only be working with organisation representatives for a brief time in limited ways. Hosts must know where to find this information and where it fits in the on-boarding process (whether shared upon arrival or made available beforehand).

There may also be third parties such as cleaning staff and contractors to consider, as they will at the very least have physical access to campus facilities – departmental representatives may have to understand procedure for overseeing access, and the third parties themselves should be aware of practices that relate to their activities on-campus.

Internet2 describes further considerations for various user groups in their Information Security Guide (see the reading list for this chapter).

## 9.8 Challenges

An individual's perception of security may make changing habits difficult. This may be seen as a failure to appreciate or understand threats – “I know how to do my job”, “Nobody would target me”); frequently-made excuses (such as futility in the face of a determined attacker); or that security-conscious behaviour is not seen as an attractive or socially-accepted trait (e.g. challenging people when they try to follow an employee through a secure door without authenticating). Issues such as these should be identified in user engagement activities, such as surveys and team talks, and may require dedicated effort to change, or alternative solutions to manage related risks. Different cultures may have very different attitudes to acceptable behaviour, and this should be taken into account when designing awareness materials.

Individual capacity to engage with awareness material is limited, and competition for user attention is fierce. Individuals grow used to messaging that is targeted at them – even the most well-designed security posters can blend into the environment. Awareness techniques should then be creative and frequently changed. Care should also be taken not to overburden individuals with unneeded details, especially as they will be the target

of multiple (other) training programmes within the organisation.

Pitching material can be difficult. Awareness activities should act to improve basic security practices, not to make individuals security experts in their own right – security-specific terminology may further confuse non-experts in security. At the other end of the scale, awareness activities can fail if they provide no explanation as to why a behaviour should be adopted. User engagement activities can help to find a balance.

## 9.9 Evaluating the response

Monitoring capabilities and user feedback channels should be provided to determine the effectiveness of the programme, particularly to identify any individuals who are not responding to training and may require dedicated attention. There may be persistent behaviours which cannot be changed, and these may not necessarily indicate a negative result but nonetheless inform awareness of security behaviours within the organisation.

In addition, records should be kept to verify that training is actually taking place as planned, and to record employees' performance in training courses, if relevant.

Referring to Chapter 11, When things go wrong: nonconformities and incidents, it may be that policies are not being followed, or that training to support policies is not effective. If training is not effective - and not relevant to the role - by drawing time away from the productive task it can also frustrate individuals. Feedback on the quality of training then contributes to the management of risks.

Embedded exercises such as self-phishing (as in Raising user awareness of information security - Cardiff University, case study) can serve as a leading indicator that something is happening or likely to happen, where incidents (see Chapter 11, When things go wrong: nonconformities and incidents) are a lagging indicator that something has happened. In line with organisation values and the management of risks, be careful in considering ways to reward good behaviour and punish bad behaviour beyond the awareness campaign.

The organisation should be in a position to identify security champions – there may be individuals who represent good security habits and are able to discuss security well with others in their team or the larger organisation. These role models should be supported in being seen in the organisation, and ideally would include top executives in their number.

## 9.10 Evaluating the awareness programme

The quality of the awareness programme should itself be monitored. Obstacles to an effective awareness programme can include lack of resources, the adaptive nature of social engineering attacks, and cost considerations – these include preparation and refreshing of materials (including the time of the preparer), the costs of providing instruction, and the employee time dedicated to attending courses and watching videos. Oversight is necessary when obtaining support for adjustments or additions to training material.

When deciding which training is mandatory, the suggestion of punishment for not following instructions should not be promoted if it is known that the instructions will be disobeyed (“we tell them not to, but we know they do it anyway”) – this would impact the visibility of policy enforcement. It should be determined upfront whether there are the monitoring capabilities to detect an infringement, and the resources and buy-in to take action.

On a related note, training records are a valuable source of evidence that people have at least undergone training. This is helpful when attempting to demonstrate that due diligence has been followed, especially when working with an external body (such as the ICO) to determine the cause(s) of an incident, and possibly assign liability. Records should include the names of people trained, dates, and any scores or training measurements (see Chapter 10, Measurement).

If technologies or processes are consistently not working or being ignored, no amount of training may persuade users to use them; consider alternative solutions beyond awareness.

There are a number of indirect indicators that training is not working or will not work: security education is static, one-way and saturates attention (such as one-way “briefings”, lectures, and posters); efforts are fragmented; the programme is the same for everyone regardless of responsibilities or where the message is best targeted; and education activities remain the same across consecutive years (regardless of any new technologies or feedback gathered in that time). These points should be addressed in the dialogue with decision-makers (see Who does information security? within Chapter 8, Roles and competencies). It is necessary to set a realistic timeline for achieving change in security habits.

## Summary

- For greatest impact, target content to match identified risks and roles within the organisation, in response to changes in the organisation environment and threat landscape
- Target learning through media, practical instruction, or theoretical instruction, using physical handouts such as flyers, electronic communications, fixed-place messaging like posters, and persistent messaging (such as screensavers and online training)
- Consider that security is supporting the individual to do their job well, and that there is competition for their attention – security needs to be there to help develop skills that will be applied in targeted roles

## Resources

Raising user awareness of information security - Cardiff University, case study

Development and use of a phishing exercise to raise awareness of phishing as an issue - Cardiff University, case study

## Reading list

ENISA, The new user's guide: how to raise information security awareness, 2010

[www.ucisa.ac.uk/ismt34](http://www.ucisa.ac.uk/ismt34)

[www.enisa.europa.eu/publications/archive/copy\\_of\\_new-users-guide/at\\_download/fullReport](http://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport)

C. Herley, More is not the Answer, Security and Privacy, Volume 12, Issue 1, Pg.14-19, IEEE, 2014

[www.ucisa.ac.uk/ismt35](http://www.ucisa.ac.uk/ismt35)

<http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6756734>

Information Security Guide: Effective Practices and Solutions for Higher Education, Internet2,

[www.ucisa.ac.uk/ismt36](http://www.ucisa.ac.uk/ismt36)

<https://spaces.internet2.edu/display/2014infosecurityguide/Home>

Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook: Chapter 13 - Awareness, Training, and Education

[www.ucisa.ac.uk/ismt37](http://www.ucisa.ac.uk/ismt37)

<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

Training materials from the Information Commissioner's Office:

[www.ucisa.ac.uk/ismt38](http://www.ucisa.ac.uk/ismt38)

<https://ico.org.uk/for-organisations/training-materials/>

Roper, Grau and Fischer, Security Awareness, Education and Training, 2006

Sasse et al, Human Factors Working Group White Paper: Human Vulnerabilities in Security Systems, Cyber Security KTN, 2007

Information Security Forum, From Promoting Awareness to Embedding Behaviours, Version 2, 2014

*This chapter covers designing and interpreting measurements for information security management, both generated within the organisation and drawn from external sources. It forms part of Stage 4 – Performance, evaluation and improvement in the Toolkit Route map.*

*Information security is a particularly challenging field for designing and interpreting measurements, as it deals with unknown circumstances and unexpected events, both of which are hard to measure. This chapter uses the term measurement throughout, except where quoting other documents.*

### Key topics

- Why measurements are worth using
- How to identify useful measurements, and evaluate the usefulness of the ones you are already using
- How to use measurements

## 10.1 Why measure?

To manage anything you need to be able to measure it. As an ISMS is the tool for managing information risk, it must include the making and use of measurements (see clause 9 in ISO/IEC 27001).

Measurements' purposes may include:

- Judging the performance of the ISMS (and its controls) over time: which actions are taking the organisation closer to/further from its objectives?
- Checking that controls are operating as expected.
- Identification of opportunities for continual improvement (see Chapter 12, Continual improvement).
- Benchmarking/comparison against peer organisations.
- Some measurements (e.g. "success of ISMS"/"ROI") may be used for selling to top management (see Chapter 2, Information security governance).

## 10.2 What is a useful measurement?

Measurements are most useful to the management of information security if they measure practical aspects of information security, such as the organisation's level of preparedness, or the level of external threat.

As with many other aspects of an ISMS, measurements have a lifecycle – they are selected and implemented, they are used, and they are retired when they are no longer useful. Measurements should therefore be reviewed by management on a periodic basis.

Many terms are used in the field of measurement, such as statistic, metric, and KPI. Find out what the rest of your organisation calls them, and use the same terms with the same meaning in your ISMS.

All measurements must have an effect: either to support decision making, or to spark action.

## 10.3 How to design a useful measurement

In simple terms, an organisation can measure:

- its ISMS processes
- the controls managed by its ISMS
- external threats.

In addition to the above, some controls are based upon measurements (e.g. alerting following multiple failed attempts to access a secure room). These controls are sometimes known as detective controls (see Chapter 6, Controls).

It is important that measurements consider people and processes, as well as technology.

Risk cannot be measured directly, but can be determined indirectly. Measurements of threat and of control effectiveness, as well as information from detective controls, are used to inform risk assessment, one of the ISMS processes (see Chapter 5, Risk assessment). This produces information on actual and acceptable risk.

Measurements should include, in their definition, the following:

- what is to be measured
- how the measurement will be made
- the purpose for which the measurement is taken
- when and/or how often a measurement should take place
- which role is responsible for ensuring that the measurement takes place
- how a measurement is to be used (including reporting format)
- the intended audience for a measurement (e.g. top management, or technical specialists)
- the classification of the information obtained (see Chapter 7, Information management).

See SANS guidelines and ISO/IEC 27004 for more information on measurement definition.

### 10.3.1 Designing measurements of ISMS processes and controls

The organisation should identify the key processes of its existing ISMS and, for each process and each control, determine:

- how to demonstrate that it is in place
- how to demonstrate that it is operating as intended.

This approach will naturally lead to the definition of useful and relevant measurements.

### 10.3.2 Designing measurements of threat

The organisation should identify what threats it is currently concerned with. For each threat or threat source, the organisation should determine:

- whether the threat is capable of being meaningfully measured
- if so, what measurement will be useful.

## 10.4 Evaluating a measurement

Existing and proposed measurements should be evaluated to identify if they are suitable and effective. The organisation can assess the effectiveness of measurements using the table in the resources section for this chapter.

## 10.5 How to use measurements

Measurements should be used as defined in the organisation's ISMS to monitor its effectiveness, and to track threat levels.

Every measurement, if it has a purpose for being taken, must also have actions and/or decisions which it affects. The organisation should, when defining each measurement, in every case define how to use the information it will provide. Likely actions should be documented and agreed with top management as appropriate in advance, to prevent misunderstandings.

Some measurements can be used to monitor the progress of the organisation towards a mature information security management system. Examples of these include the speed and completeness of responses to notifications, for example of the availability of patches; the number of known vulnerabilities that are detected

by routine scanning; or the number of the organisation's passwords that can be successfully cracked in a given time. On the non-technical front, the proportion of users who have received relevant training, and their scores on tests, are also very useful.

## 10.6 Reporting and interpretation

The results from monitoring and measurement should be evaluated and analysed (see ISO/IEC 27001 9.1 and 9.3), reported to a responsible management role or group, and appropriate actions taken to address any issues uncovered (see Chapter 11, Incidents and nonconformities).

The role of internal audit is key in ensuring that the organisation has, and maintains, an effective ISMS. Even if an organisation is not aiming for compliance with ISO/IEC 27001, its internal audit function can still undertake periodic reviews of different aspects of information security, especially to determine whether effective monitoring and controls are in place.

The presentation of measurements is critical to their usefulness, as appropriate presentation allows audiences to interpret the information easily. Reporting should be tailored to the audience. See Chapter 2, Information security governance, for suggestions on developing material for top management.

Reporting can also be used to highlight features of the information which the audience would otherwise not have noticed, or to explain subtleties in the measurement which can easily be misinterpreted.

An example of subtlety in measurement is where an organisation experiences an increase in reported incidents. While this increase might indicate that more security incidents are happening, industry surveys suggest that only a small percentage of incidents are noticed, so an increase is more likely to indicate improved detection. Users may also have become more confident that they can report them without being blamed.

The context of a measurement is also important; for example, if an organisation carries out an awareness campaign and subsequently sees an increase in reporting, this should normally be seen as a sign of increased awareness, rather than of decreased security.

Measurements gathered from other environments may not be directly comparable and may have been collected in different ways.

## 10.7 Examples of effective measurements

There are a number of sources of lists of measurements, including SANS, the US Office of Energy Delivery, and the Centre of Internet Security (see reading list for this chapter). In this chapter, a sample of metrics are given, divided into four categories:

- measurements of information risk
- measurements which aim to determine whether the ISMS is performing as expected
- measurements which aim to determine whether controls are performing as expected
- measurements which themselves are controls.

### 10.7.1 Measurements of information risk

These measurements can, by themselves, be monitored to identify whether information risk is increasing or decreasing. However, in order to tell whether there is a problem (see Chapter 11: Incidents and nonconformities), they should be evaluated to determine whether the actual risk related to them is acceptable to the organisation (see Chapter 5, Risk assessment). Examples of this type of measurement are:

- “opportunity window” between vulnerabilities being known and patches being installed
- number of unpatched systems at any given time
- percentage of sensitive data being handled in secure environments
- number of copyright complaints (which are correlated to the possibility of legal action, but not strongly correlated to the number of actual copyright violations)
- notifications to the Information Commissioner's Office (as for copyright complaints).

### 10.7.2 Measurements of ISMS effectiveness

The following measurements are examples of the types of measurement which can be used to determine if the organisation's ISMS is still performing as required.

- percentage attendance at management review meetings
- percentage of policies reviewed on or before their review dates
- percentage of controls whose effectiveness is being measured
- number of minor and major non-conformities found at last internal audit
- time to resolve non-conformities
- shortfall in resources.

### 10.7.3 Measurements of control effectiveness

The following examples are designed to show whether a control which the organisation has decided to implement is performing as required.

#### 10.7.3.1 Types of incidents

It may be useful to measure the numbers of incidents of different types they handle, according to a standard categorisation. Changes in these numbers can indicate areas where more resources or skills are required, for example if the number of internal investigations increases or where current controls need to be reviewed, for example if there is an increase in malicious code incidents.

Normalising these values to incidents per 100 users creates statistics that can be compared between organisations: differences in the rates of occurrence, the proportions of different categories or the trends in their prevalence have prompted useful discussions of the impact of different security approaches.

#### 10.7.3.2 Successful attacks vs attempted attacks

Where successful attacks can be measured using technical means – for example a phishing attack that directs victims to a unique website – a measurement looking at the proportion of recipients who became victims may be a useful guide to areas of the organisation where additional measures (e.g. awareness raising) are required. Through an employee phishing campaign, Caputo et al (see reading list for this chapter) demonstrate human factor considerations around the measurement of behaviour in organisations.

#### 10.7.3.3 Measuring time to patch

Where patching is considered to be a suitable control, the obvious associated measurement would appear to be how long it takes to patch after an update is available. In fact, the correct measurement is the difference between the agreed appropriate time to patch and the actual time to patch. Where the two are identical, then the control “patching our servers” is operating as expected. Where patching takes a longer or shorter time than required, then the organisation is not managing its risk as it has decided to, and there is a problem.

### 10.7.4 Measurements which are controls

The following measurements are direct measurements of components of the organisation’s environment and activities; their results can be used to determine if an incident is occurring, for example. They are also called “detective controls” (see Chapter 6, Controls).

- number of virus alerts
- unexpected changes in key database files
- loss of a heartbeat signal from a logging system
- alerts from an intrusion detection system.

## 10.8 Examples of measurements which may be less helpful

### 10.8.1 Level of information security

A simple measure of organisational information security is unlikely to be achievable and would, in any case, provide little clues regarding how information security can be improved.

### 10.8.2 Number of incidents handled

An often cited measurement is the number of incidents handled by an organisation's security team – for example, the number of copyright infringement notices. Typically this combines individual measures with many of the problems discussed above: some incidents will be triggered by user reports, others by technical detection of attacks. And as noted earlier in the chapter, the interpretation of this statistic is very ambiguous.

As a result it is unlikely to be a useful measure of the organisation's security, threat or preparedness. It is best seen simply as a measure of how busy the incident responders are – a measurement which can be used to manage service delivery, but which has a very indirect bearing on the actual level of risk or threat to the organisation. A better measurement may be the historical trend in incidents.

### Summary

- Measurements may be used to measure the performance of an ISMS, the effectiveness of controls, to track threat levels, and as part of controls themselves
- Every measurement must have a purpose: to direct action, and/or to support decision making
- Suitable presentation of measures is critical to their effectiveness

## Resources

How to evaluate a measurement

## Reading list

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

[www.ucisa.ac.uk/ismt39](http://www.ucisa.ac.uk/ismt39)

<http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity>

CIS Consensus Information Security Metrics

[www.ucisa.ac.uk/ismt40](http://www.ucisa.ac.uk/ismt40)

<http://benchmarks.cisecurity.org/downloads/metrics/>

SANS Guide to Security Metrics

[www.ucisa.ac.uk/ismt41](http://www.ucisa.ac.uk/ismt41)

<http://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55>

Jaquith, *Security Metrics*, 2007

Vaughn, Henning, Siraj, *Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy, HICSS'03*, 2002

Villarubia, Fernandez-Medina, Piattini, *Towards a Classification of Security Metrics, WOSIS '04*, 2004

Jansen, *Research Directions in Security Metrics, Discourses in Security Assurance and Privacy*, 2009

Hecker, *On System Security Metrics and the Definition Approaches, SECUREWARE '08*, 2008

Ouedraogo, Mouratidis, Khadraoui, Dubois, *Security Assurance Metrics and Aggregation Techniques for IT Systems, ICIMP '09*, 2009

Savola, *On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems, IJCSNS*, 2010

Wang, Wulf, *Towards A Framework For Security Measurement, NISSC '97*, 1997

Debra S. Herrmann, *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*, Auerbach Publications, 2007.

IATAC Cyber Security Report, *Measuring Cyber Security and Information Assurance State-of-the-Art Report (SOAR)*", IATAC, 2009

Atzeni and Leoy, *Why to adopt a security metric?*, 1st Workshop on Quality of Protection, 2005

Julisch, *A Unifying Theory of Security Metrics with Applications, IBM RZ3758*, 2009

Jonsson and Pirzadeh, *A Framework for Security Metrics Based on Operational System Attributes, International workshop on Security Measurements and Metrics - MetriSec2011*

Chapin and Akridge, *How Can Security Be Measured?*, ISACA, 2005

D. Caputo et al, *Going Spear Phishing: Exploring Embedded Training and Awareness, IEEE Security and Privacy*, 2014

*This chapter covers how to plan to deal effectively with failures in information security and how to use these experiences to improve your information security management system. It forms part of Stage 4 – Performance, Evaluation and Improvement in the Toolkit Route map.*

### Key topics

- How to detect and recover when things go wrong
- How to reduce the impact of adverse events
- How learning from adverse events can improve information security

## 11.1 Introduction

It is dangerous to assume that nothing will ever go wrong: information security is about managing the risk from adverse events, not eliminating them. Planning how to recover from failures is an important aspect of managing information security.

The ISO standards define two distinct types of failure:

- nonconformity: the nonfulfillment of a [known] requirement (ISO 19011)
- incident: an unexpected or unwanted event likely to compromise business operations (ISO/IEC 27000).

Organisations should take action to control and correct non-conformities, and respond to incidents to prevent recurrence.

Nonconformities may increase the likelihood of incidents, and incidents are one way in which that nonconformities are discovered. However not all incidents indicate the presence of nonconformities. A realistic ISMS will accept, and manage, a certain frequency and level of incidents (see Chapter 5, Risk assessment).

Both incidents and nonconformities require a prepared and timely response that remedies the immediate problem and learns lessons to reduce the likelihood of recurrence. Both involve identification, corrective action and analysis of root causes, which may follow similar processes. Both may (nonconformities must) lead to improvements in the ISMS.

A key difference is that, subject to audit requirements, the organisation will normally control the timescale on which it responds to a nonconformity, typically weeks or months. Incidents arise and evolve outside the organisation's control and require a technical response in minutes or hours. Incident response should link to the organisation's crisis communications plan (for example, see the final case study), and to business continuity and disaster recovery plans.

This chapter first considers how to address nonconformities, then incidents.

## 11.2 Nonconformities

### 11.2.1 Identifying nonconformities

Within an ISO/IEC 27001-aligned ISMS, there are two types of nonconformities:

- the documented management system deviates from the requirements of ISO/IEC 27001
- the implemented management system deviates from its documented state.

Nonconformities may result from not doing enough, or from doing too much (overkill). For example, blocking the use of USB sticks where a block has not been justified is a nonconformity; but so is identifying a need for such a block, documenting that it is in place, and then not implementing it.

Nonconformities are often found during an audit. A Stage 1 audit (“document review”) may identify that the ISMS documentation does not contain what is required by the ISO standard; a Stage 2 (“conformance”) audit may identify that the organisation’s practice does not match its documentation. For example a required firewall might not have been installed or a password policy be being ignored.

Nonconformities may also be discovered outside the audit process, including through information security incidents or if staff have difficulty implementing or working within a prescribed control (see Chapter 6, Controls, for more advice). Organisations should ensure their processes can capture these nonconformities and that staff feel comfortable pointing them out.

### 11.2.2 Dealing with nonconformities

ISO/IEC 27001 requires organisations to deal with every nonconformity. A common, clearly-defined, process should be used, though different nonconformities may require different resources. Minor nonconformities may be resolved between the ISMS manager and the owner of the related business activity, while major ones require top management attention.

If an existing process, such as those which are part of ITIL service management or COBIT IT governance, is available and suitable to handle corrective actions, this should be used to simplify matters.

The process must ensure that each nonconformity is reviewed and appropriate corrective actions taken to deal with it and any consequences. Corrective actions may involve any part of the system, from a more accurate implementation of a required technical security control, better training for users in implementing it, to a change in the risk management process itself. Records of nonconformities and corrective actions must be kept.

The causes of nonconformities must also be reviewed, investigated and corrected. This may reveal wider issues across the ISMS, where a nonconformity may recur at different times or in different parts of the system. Wider corrective actions may be required if, for example, the ISMS has failed to identify a significant risk or selected an unsuitable control. Again, these conclusions must be documented and the required actions managed to completion.

Nonconformities should be used as a tool for the continual improvement of the organisation’s information security (see Chapter 12, Continual improvement). It is important to remember that it is the organisation, not the individual, that is being assessed. Using nonconformities to assign blame will discourage correct behaviour among those involved in the ISMS.

## 11.3 Information security incidents

Any unwanted or unexpected event with a significant probability of threatening business operations or information security may constitute an incident. Incidents can affect information and its processing in any form: the compromise of a networked computer, the loss of a paper file or the inclusion of the wrong person in an information handling process may all be information security incidents.

Managing incidents effectively can significantly reduce their impact and so is a valuable way to enhance information security. For research and education organisations this reactive approach is particularly important since the wide range of legitimate users and activities makes strong preventive controls less appropriate (also see Chapter 6, Controls).

Information security incidents may also highlight areas needing improvement: for example identifying policies that are not followed, policies that are not effective, risks that have changed, or systems lacking necessary resources or skills. Reviewing incidents may also, of course, reveal the need for improvements to the incident management processes themselves.

Both outcomes require incident management to be planned, documented, resourced and recorded. The organisation must first define what it classes as an incident and plan its response.

### 11.3.1 The incident response policy and plan

The incident response policy is the basis for incident response activities. The policy defines what the organisation considers to be an incident, what incident response should achieve and how it is escalated, and the responsibilities and authorities of people within the organisation to make that happen.

Different events may qualify as incidents (“business-affecting events”) in different parts of the organisation; the desired response to an incident may also vary. In general the accidental destruction of a user’s file is unlikely to constitute an incident, but the accidental destruction of a business-critical database almost certainly will. If the organisation’s web server is compromised, the priority is likely to be to re-establish a secure web presence: if a server storing sensitive research data is compromised, the priority will be to find out what data may have been affected and how. The incident response policy may comprise a standard set of incident definitions and desired outcomes with variations covering areas with different requirements, consistent with the classification of information processed.

Once policy is set, an incident response plan should be developed to implement it. The plan will comprise processes, procedures and the systems and resources needed to implement them. These will themselves require preparation. The CERT Coordination Center’s Mission Risk Diagnostic for Incident Management Capabilities provides a useful health check. Exercises are a good way to identify problems and to train incident responders to work together.

Case studies in this chapter include how one organisation developed its incident response policy and plan and two examples of incident response plans.

### 11.3.2 Responsibilities and authorities

Successful incident response requires coordination. Most incidents will involve working with others, both inside and outside the organisation, from technical staff, HR, legal and communications advisors, to network providers, regulators and law enforcement. Preparation must ensure that the required people, systems and services will be available when needed, even if this takes them away from normal duties. Defining specific roles and responsibilities in the incident response plan will considerably strengthen an organisation’s capability to handle incidents.

Incident coordinators must be granted, or be able to quickly obtain, the authority to modify or suspend any of the organisation’s activities until they are restored to a secure state. For example a compromised computer may need to be disconnected from the network, a suspect account have its access rights withdrawn, or a research activity suspended while the integrity of its data is checked.

### 11.3.3 Stages in incident response

Responding to an incident normally involves three stages: detection, analysis and response. Each is driven by the definitions and requirements of the incident response policy. After an incident, a review should take place to identify lessons that can be learned, including any changes to the ISMS that may be required.

Incidents may be detected directly, by someone noticing a security failure, or indirectly, by human or computer monitoring of computer logs or other records. The organisation should ensure it has the reporting and monitoring systems needed to detect the types of incident defined in the policy, and that these are known to and trusted by all those who may detect signs of an incident. Information gathered during security events and incidents is likely to be sensitive: a case study shows one organisation’s policy for handling this material.

Successful incident management depends upon a critical resource – availability of the right people/roles to receive alerts, do the analysis, coordinate work, and carry out response activities. The organisation must have communication routes previously agreed, and tested – and contingency plans for those (frequent) cases where someone is unavailable.

Not all reported events will indicate incidents. An initial triage process determines whether a report, or group of reports, should be treated as an incident or whether another process, for example for faults or helpdesk enquiries, is appropriate. Those reports that are classed as incidents are likely to require further analysis to determine how best to restore the organisation to its desired operational state.

In complex incidents, the response stage may begin with containment to prevent the impact getting worse. This gives more time for the steps required to remove the incident’s cause and, to the extent possible, investigate and mitigate its consequences. Both containment and response are likely to involve working with those having relevant expertise both inside and outside the organisation (see Chapter 8, Roles and competencies), as well as official communications channels to ensure that the right messages are getting out. All actions taken to respond to incidents should be recorded, to ensure the response is effective and to inform the subsequent review.

Trust must be established before an incident, not during it.

### 11.3.4 Review

Completed incidents are a major source of information about the organisation's information security, so should be reviewed to identify lessons that can be learned. Incident coordinators should review whether the response was successful and whether changes are needed to the incident response plan or its implementation.

They should also generate a report for the organisation's ISMS review process (see Chapter 12, Continual improvement). The detail in this report may vary. For routine incidents resolved successfully it may just summarise the number of incidents and the systems or units affected; but for serious or novel incidents, the report should include the root cause of the incident (to the extent that this can be determined), the impact on the organisation, and the controls that were, and were not, effective in managing it.

The final case study describes one organisation's response to a security incident affecting personal data.

## Summary

- The ISMS should aim to manage the level and severity of adverse events, not to eliminate them
- The ISMS should contain plans to respond to, and learn from, these events
- Incident response requires trusted cooperation both within and outside the organisation; trust must be established in advance

## Resources

Developing an information security incident response plan based on ISO/IEC 27035:2011 – University of Oxford

Example of an information security incident response scheme

Information security service: information security incident management process – UCL

Investigations and data access policies – University of York, case study

Data breach – case study

## Reading list

ITIL

[www.ucisa.ac.uk/ismt42](http://www.ucisa.ac.uk/ismt42)

[www.axelos.com/itil](http://www.axelos.com/itil)

COBIT

[www.ucisa.ac.uk/ismt43](http://www.ucisa.ac.uk/ismt43)

[www.isaca.org/cobit](http://www.isaca.org/cobit)

CERT-CC, Mission Risk Diagnostic for Incident Response Capabilities

[www.ucisa.ac.uk/ismt44](http://www.ucisa.ac.uk/ismt44)

<http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=91452>

ENISA, CSIRT Exercises

[www.ucisa.ac.uk/ismt45](http://www.ucisa.ac.uk/ismt45)

[www.enisa.europa.eu/activities/cert/support/exercise](http://www.enisa.europa.eu/activities/cert/support/exercise)

NIST, Incident Response Exercises

[www.ucisa.ac.uk/ismt46](http://www.ucisa.ac.uk/ismt46)

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>, Appendix A

Information Commissioner, Notification of Data Security Breaches to the Information Commissioner's Office

[www.ucisa.ac.uk/ismt47](http://www.ucisa.ac.uk/ismt47)

[https://ico.org.uk/media/for-organisations/documents/1536/breach\\_reporting.pdf](https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf)

ENISA, Support for CSIRTs

[www.ucisa.ac.uk/ismt48](http://www.ucisa.ac.uk/ismt48)

[www.enisa.europa.eu/activities/cert/support](http://www.enisa.europa.eu/activities/cert/support)

Association of Chief Police Officers, Good Practice Guide for Digital Evidence

[www.ucisa.ac.uk/ismt49](http://www.ucisa.ac.uk/ismt49)

[www.digital-detective.net/digital-forensics-documents/ACPO\\_Good\\_Practice\\_Guide\\_for\\_Digital\\_Evidence\\_v5.pdf](http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf)

*This chapter outlines what is meant by continual improvement and looks at how to initiate processes and activities to achieve it. It forms part of Stage 4 – Performance, evaluation and improvement in the Toolkit Route map.*

### Key topics

- What is continual improvement?
- How to identify opportunities for improvement
- How to create an improvement plan for your organisation

## 12.1 What is continual improvement?

Organisations should aim to continually improve the suitability, adequacy and effectiveness of their established ISMS. This does not mean simply fixing problems as they occur, or even that risk must be continually reduced (which may not be possible). Instead, continual improvement requires measuring the effectiveness and efficiency of technology, people and processes and adapting to inevitable changes in the environment – technical, organisational or otherwise. It can be seen as “closing the loop” between risk management and actual incidents.

Continual improvement may therefore be achieved by a number of means, including:

- maintaining suitability of controls to maintain an appropriate level of residual risk in a changing environment (i.e. evolving as technology, threats, assets and vulnerabilities change)
- improving efficiency of the ISMS and controls in meeting security objectives; and/or
- improving the effectiveness of the ISMS and controls in meeting security objectives.

Continual improvement needs to be promoted by leadership and commitment of management and should be included in policy, planning and resources. Implementing a continual improvement process will help an organisation create prioritised and cost-effective improvements that are aligned to business requirements and available resources. Resulting monitoring and reporting capabilities will then increase the potential to identify further opportunities for improvement.

The process for continual improvement should be defined and overseen by the information security function within the organisation. The process should be integrated into existing procedures and processes where possible, so that existing process managers will be responsible for implementing the continual improvement process within their respective area.

## 12.2 Processes for improvement

Continual improvement involves long-term thinking, implementation of controls or fixes and regular review, monitoring and measurement of people, processes and technology.

Among the many frameworks for continual improvement are COBIT, the Deming cycle and ITIL:

- The Deming cycle is a method for continual improvement, characterised by the Plan-Do-Check-Act iterative steps
- The ITIL set of practices for IT service management defines a seven-step improvement process.

Making improvement an objective from the outset will improve both efficiency and security.

One example of how these processes might relate to continual improvement of an ISMS is given below:

**Table 6 - Sample mapping of Deming cycle to ITIL 7 step process**

| Deming Cycle | ITIL Seven Step Process  | Example activities  |
|--------------|--|---|
| Plan         | 1. Define what you should measure<br>2. Define what you can measure  | Identify technical, operational and strategic goals<br>Scoping<br>Risk assessment and risk treatment plans<br>Identify the strategy for improvement<br>Define what you will measure |
| Do           | 3. Gather the data<br>4. Process the data                            | Implement improvement plans<br>Implement controls, services monitoring etc.   |
| Check        | 5. Analyse the data  | Analyse gathered data (e.g. from monitoring)<br>Carry out gap analysis<br>Internal and external audits  |
| Act          | 6. Present and use the information<br>7. Implement corrective action | Implement corrective actions and fixes;<br>Record lessons learned<br>Feed back and report   |

### 12.3 Types of improvement

Improvements can be short or long term, and may arise as a result of planned or unplanned events. For example, improvements in the organisation’s ISMS may be planned over a period of months or years as part of an overall maturity improvement plan. Alternatively, improvements can be implemented as vulnerabilities and incidents are discovered.

Improvements can be broadly divided into three categories:

- improvements in strategy (i.e. why things are done)
- improvements in practice (i.e. what is done)
- improvements in process (i.e. how things are done).

Improving strategy improves or maintains the suitability of an ISMS in an evolving world and therefore requires improving knowledge and understanding of the environment and threat landscape.

Improving practice (i.e. what the organisation chooses to do, rather than what its members do) can increase the effectiveness of the ISMS and resulting security controls.

Improving processes can increase the efficiency of controls and surrounding processes.

In reality, there is considerable overlap since, for example, improving strategy may result in an increase of both effectiveness and efficiency. Examples of these types of improvement and their effect(s) are given in the table below:

**Table 7 - Types of improvement**

| Type of improvement | Primary improvement | Examples   |
|---------------------|---------------------|--|
| Strategy            | Suitability         | <ul style="list-style-type: none"> <li>• Adjusting strategy and/or security requirements</li> <li>• Creating risk treatment plans</li> <li>• Designing maturity improvement plans</li> <li>• Improving sources of information (e.g. implementing monitoring and detection)</li> <li>• Training and information gathering</li> </ul>  |
| Practice            | Effectiveness       | <ul style="list-style-type: none"> <li>• Implementing vulnerability fixes</li> <li>• Implementing new controls</li> <li>• Implementing new services</li> <li>• Implementing new processes and organisational structures</li> <li>• Reacting to new opportunistic for bonus improvements</li> <li>• Ceasing unnecessary actions</li> <li>• Implementing an awareness programme</li> </ul> |
| Process             | Efficiency          | <ul style="list-style-type: none"> <li>• Refining processes</li> <li>• Renewing technology (e.g. hardware replacement cycles, software updates)</li> <li>• Organisational changes</li> </ul>   |

## 12.4 Steps in an improvement process

Improvements can be made in the short or long term. However most improvements will follow the process below:

- Identify opportunity for improvement.
- Identify root cause (as applicable).
- Allocate responsibility for implementing change.
- Identify, analyse and evaluate (based on cost vs benefit) possible solutions.
- Plan implementation of changes.
- Implement changes.
- Measure effectiveness of actions (Chapter 10, Measurement for more information on measuring effectiveness).

## 12.5 Sources of information and opportunities for improvement

Continual improvement therefore involves identifying and reacting to opportunities for improvement. The following table lists a number of potential opportunities for improvement along with potential sources of information associated with these improvements.

**Table 8 - Sources of improvement opportunities**

| Opportunity for improvement   | Sources of information  |
|---|---|
| Organisational changes  | <ul style="list-style-type: none"> <li>• Meetings with top management</li> <li>• Departmental/organisational announcements, news bulletins etc.</li> </ul>  |
| Changes in business requirements/circumstances  | <ul style="list-style-type: none"> <li>• Third party requirements</li> <li>• Public media and news</li> <li>• Security/business conferences</li> <li>• Team meetings</li> <li>• Management reviews</li> <li>• Service reviews</li> </ul>  |
| Change in security requirements   | <ul style="list-style-type: none"> <li>• Policy reviews</li> <li>• Information security incidents</li> <li>• Service requests</li> <li>• Change requests</li> <li>• Bulletins and announcements</li> </ul>  |
| Changes in regulatory environment   | <ul style="list-style-type: none"> <li>• Notifications from suppliers</li> <li>• Notifications from third parties</li> <li>• Notification from statutory bodies e.g. the Information Commissioner's Office</li> <li>• Internal security forums</li> <li>• Security mailing lists</li> </ul>       |
| Contact with Special Interest Groups  | <ul style="list-style-type: none"> <li>• Security conferences and community meetings</li> <li>• Security mailing lists</li> </ul>   |
| Changes in skillsets  | <ul style="list-style-type: none"> <li>• Recruitment of new staff</li> <li>• Knowledge gained from training</li> </ul>  |
| User/customer engagement  | <ul style="list-style-type: none"> <li>• Service requests</li> <li>• User satisfaction surveys</li> <li>• Knowledge bases</li> </ul>  |
| Service requests  | <ul style="list-style-type: none"> <li>• Service desk management tools</li> <li>• Knowledge bases</li> </ul>  |
| Risk assessments  | <ul style="list-style-type: none"> <li>• Risk assessment outputs</li> <li>• Gap analysis reports</li> </ul>   |
| Vulnerabilities   | <ul style="list-style-type: none"> <li>• Vendor vulnerability announcements</li> <li>• Security community mailing lists</li> <li>• Results from penetration testing and vulnerability scanning</li> <li>• Log files</li> <li>• Service requests and notifications from users/customers</li> </ul> |
| Information security incidents (see also Chapter 11, When things go wrong: nonconformities and incidents) | <ul style="list-style-type: none"> <li>• Intrusion detection/prevention system alerts</li> <li>• Log files and network flows</li> <li>• Knowledge gained from analysing and resolving incidents</li> </ul>  |
| Internal audit and review (see also Chapter 11, When things go wrong: nonconformities and incidents)      | <ul style="list-style-type: none"> <li>• Review meetings</li> <li>• Policy reviews</li> <li>• Audit reports</li> <li>• Vulnerability scanning and penetration testing reports</li> <li>• Security reviews</li> </ul>  |
| External audits   | <ul style="list-style-type: none"> <li>• Review meetings</li> <li>• Audit reports</li> <li>• Vulnerability scanning and penetration testing reports</li> <li>• Security reviews</li> </ul>  |

## 12.6 Improvement as part of ISMS formalisation

Where an organisation's ISMS is not yet ISO/IEC 27001 compliant, and the organisation wishes to reach this level of maturity, it should treat the process as a standard project or programme.

Following the ITIL continual service improvement approach, organisations can create an improvement plan by considering the following:

- What is the vision?
- Where are we now?
- Where do we want to be?
- How do we get there?
- Did we get there?

In order to consider the vision for improvement it is important to understand the level of resources available and achieve the support of top management.

### 12.6.1 Vision for improvement

Organisations may wish to consider:

- Who will provide ownership and direction for information security improvement?
- Where does information security report within the organisation (i.e. level of seniority)?
- How quickly does the organisation wish/need to change?
- How much resource can be made available?
- What is the scope and remit of the improvement programme?
- How can goals be made specific, in order to provide clear directing and measurable targets?

### 12.6.2 Where are we now?

To measure its current level of maturity of information security, the organisation can carry out benchmarking and comparisons with similar organisations. This can give an indication of relative maturity and help to prioritise certain work areas.

Assessment may also be carried out via self-assessment, internal or external audit. Self-assessment can be a useful tool, but involves time and effort from internal staff, and the level of assurance may not be as great as that provided by a more formal audit. However, this will often be an appropriate starting point for an improvement process. External audits may provide more assurance and act as a greater catalyst for improvement, but can be more costly.

### 12.6.3 Planning and implementing (where do you want to be and how to get there)

Once the organisation has analysed its current state and compared it to its desired state, the results should be documented and compared in a gap analysis, which will form the basis of the improvement programme.

The gap analysis will provide the objectives for the improvement programme, which should be prioritised according to business requirements and an assessment of how much effort is required. Certain objectives might provide the opportunity for "quick-wins", which can be useful to improve buy-in and demonstrate progress, whereas other activities may need long-term projects to achieve. Benchmarking against similar organisations can also prove to be useful during the prioritisation process.

Improvement plans for identified activities can then be planned in an incremental manner to increase the overall level of maturity in a measurable way. For example, in planning to improve awareness of individuals across the organisation, where the organisation has identified that it needs to train everyone annually, the following stages might provide observable milestones:

**Table 9 - Simple maturity model for awareness activities**

| Level of maturity | Milestone  |
|-------------------|--|
| Low               | Information security awareness training is available to all users within the organisation.   |
| Medium            | Information security awareness training is compulsory for all users within the organisation and is repeated on an annual basis   |
| High              | Information security awareness training is compulsory for all users within the organisation, is repeated on an annual basis, and awareness is tested and measured by such means as spot checks, incident simulations, tests etc. |

## 12.7 Measurement

In order to determine whether or not goals have been achieved, appropriate measurements should be used (see Chapter 10, Measurement, for further information).

### Summary

- The goal of continual improvement is to iteratively identify and implement ways to make an established ISMS more cost effective and appropriate
- Improvement activities are also necessary during the creation of an ISMS
- Continual improvement can include adapting to the current environment, or improving the efficiency of controls and/or processes
- Continual improvement should be an objective from the outset when implementing any ISMS

## Resources

No resources.

## Reading list

No items.

*This chapter forms part of Stage 1 -  
Foundations in the Toolkit Route map.*

Every organisation requires a top level policy for information security which must define clear lines of responsibility for delivery and risk ownership. The policy and associated responsibility should be developed as a result of the governance arrangements in place within the organisation (see Chapter 2, Information security governance), and in particular the policy must be approved by the highest body in the organisation's governance framework.

Managing information security risks should be part of an organisation's overall risk management strategy, and the formulation of information security policy should form part of that strategy. In organisations with a low maturity in terms of risk management, a governance structure may need to be developed specifically for the purpose of writing the information security policy and the use of a RACI matrix (Responsible, Accountable, Consulted, and Informed) may help to establish it.

The supplementary volume to this publication which, at the time of writing, is still in production, builds on the third edition of UCISA's Information Security Toolkit published in 2007 (the predecessor of this publication) and will include revised policies to comply with ISO 27001:2013.

## Summary

- The information security policy should not stand alone; it should be part of an organisation's risk management strategy and must be approved by the highest governance body in the organisation
- The organisation's policy for information security defines responsibility for delivery and risk ownership

## Resources

Template for a generic policy

## Reading list

No items.

*This Toolkit has been designed to enable organisations in the educational sector to design, establish, maintain and improve an information security management system. From getting a clear picture of the organisation is, to achieving buy-in, to selecting controls, implementing business changes and ensuring that these changes are properly embedded by the use of awareness materials, measurement and reporting, each step builds on the previous one to create something which is genuinely worth having and which continues to be relevant and cost-effective.*

In summary, it is vital for everyone in the organisation to understand that this is not a finite project that can be implemented and forgotten about. Continual improvement is crucial, for a successful ISMS will require ongoing investment. Analysis of information security threats and incidents over the years shows that there is no room for complacency, as threats and risks are ever-changing.

The battle for hearts and minds is a key one. At all times, organisations must ensure that their ISMS is as user-friendly as possible. Information security professionals should work closely with colleagues across the organisation to maintain an holistic approach. The way to ensure the continued relevance of an ISMS is to keep it closely and visibly linked to the organisation's strategic objectives and risk appetite.

The summaries for each chapter are collected below. Readers are also encouraged to review and use the resources the material referenced in the reading lists at the end of each chapter and in the Annex: Example resources to accompany the Toolkit.

A well-managed ISMS is a powerful business enabler.

## Overall summary

### 1 What is information security?

- Information security applies to all forms of information
- Threats are becoming more sophisticated and revenue-led
- Information security is the responsibility of all members of an organisation

### 2 Information security governance

- A suitable governance framework is a critical component in the development, implementation and maintenance of a successful ISMS
- Top management must endorse and be accountable for information security
- Good governance ensures ownership, scrutiny and accountability

### 3 Drivers

- Drivers can operate at a very high level (e.g. organisational reputation), or be very granular in their level of detail (e.g. researcher reputation)
- Drivers can be internal (e.g. responsibility to students and staff), but are often external (e.g. the Information Governance Toolkit)
- Managing the impact of drivers is an iterative process

### 4 Scoping

- Successfully defining and agreeing the scope of an ISMS from the beginning is a critical success factor in the implementation of any ISMS – if the scope is wrong you will not know where you are going or when you got there!
- There are different scopes involved in implementing information security in an organisation from high-level scopes covering the entire organisation to the scope of a particular project.
- Start small with your scope, demonstrate success and build from there.
- Monitor and review, and if your scope is wrong then change it accordingly

### 5 Risk assessment

- Information risk management is a systematic, consistent, iterative process where risks are identified and assessed before being treated and monitored
- Information risk treatment options should not cost more to deploy and manage than the cost of the risk itself
- Information risk management should not be done in a vacuum, but as part of the overall organisational risk management process

### 6 Controls

- Controls reduce the impact and/or likelihood of incidents
- Ready-made control sets should be considered carefully
- Controls form part of an ISMS – they do not replace it
- Controls should be traceable to the requirements/risks which they are intended to address

### 7 Information management

- An information management scheme should comprise of: a classification scheme, a labelling scheme, handling rules and processes to define how these all interact
- A classification scheme describes how information should be classified
- A handling scheme describes how information given a particular classification should be treated
- Do not have more classification levels than necessary, or practical
- Labelling can indicate both the classification and who should (and should not) see the information
- Handling rules must provide consistent protection across different media

### 8 Roles and competencies

- The organisation's information security policy should define the roles and responsibilities required of staff
- All staff have responsibility for information security; this responsibility will be included in general terms and conditions of employment as well as individual job descriptions
- An information security group should be established at a high level, chaired by a member of top management with specific responsibility for championing information security and including owners (and representatives of owners) of key information assets

- A team to monitor and implement information security measures should be established and should be represented on the information security group
- The information security policy needs to be supported by effective personnel procedures

## 9 Awareness raising

- For greatest impact, target content to match identified risks and roles within the organisation, in response to changes in the organisation environment and threat landscape
- Target learning through media, practical instruction, or theoretical instruction, using physical hand-outs such as flyers, electronic communications, fixed-place messaging like posters, and persistent messaging (such as screensavers and online training)
- Consider that security is supporting the individual to do their job well, and that there is competition for their attention – security needs to be there to help develop skills that will be applied in targeted roles

## 10 Measurement

- Measurements may be used to measure the performance of an ISMS, the effectiveness of controls, to track threat levels, and as part of controls themselves (see Chapter 6, Controls).
- Every measurement must have a purpose: to direct action, and/or to support decision making
- Suitable presentation of measures is critical to their effectiveness

## 11 When things go wrong – nonconformities and incidents

- The ISMS should aim to manage the level and severity of adverse events, not to eliminate them
- The ISMS should contain plans to respond to, and learn from, these events
- Incident response requires trusted cooperation both within and outside the organisation; trust must be established in advance

## 12 Continual improvement

- The goal of continual improvement is to iteratively identify and implement ways to make an established ISMS more cost effective and appropriate
- Improvement activities are also necessary during the creation of an ISMS
- Continual improvement can include adapting to the current environment, or improving the efficiency of controls and/or processes
- Continual improvement should be an objective from the outset when implementing any ISMS

## 13 Policies

- The information security policy should not stand alone; it should be part of an organisation's risk management strategy and must be approved by the highest governance body in the organisation
- The organisation's policy for information security defines responsibility for delivery and risk ownership



# Annex

## Example resources to accompany the Toolkit

**This section provides examples of actual documents and resources created and used successfully by organisations in the educational sector.**

**They are largely published as supplied – the text, style and tone of these documents have not been altered to match the remainder of this document.**

**They are not intended to be perfect, nor to be used verbatim by the reader, but to provide concrete examples of what has worked for others.**



# Resources for Introduction

## RESOURCES

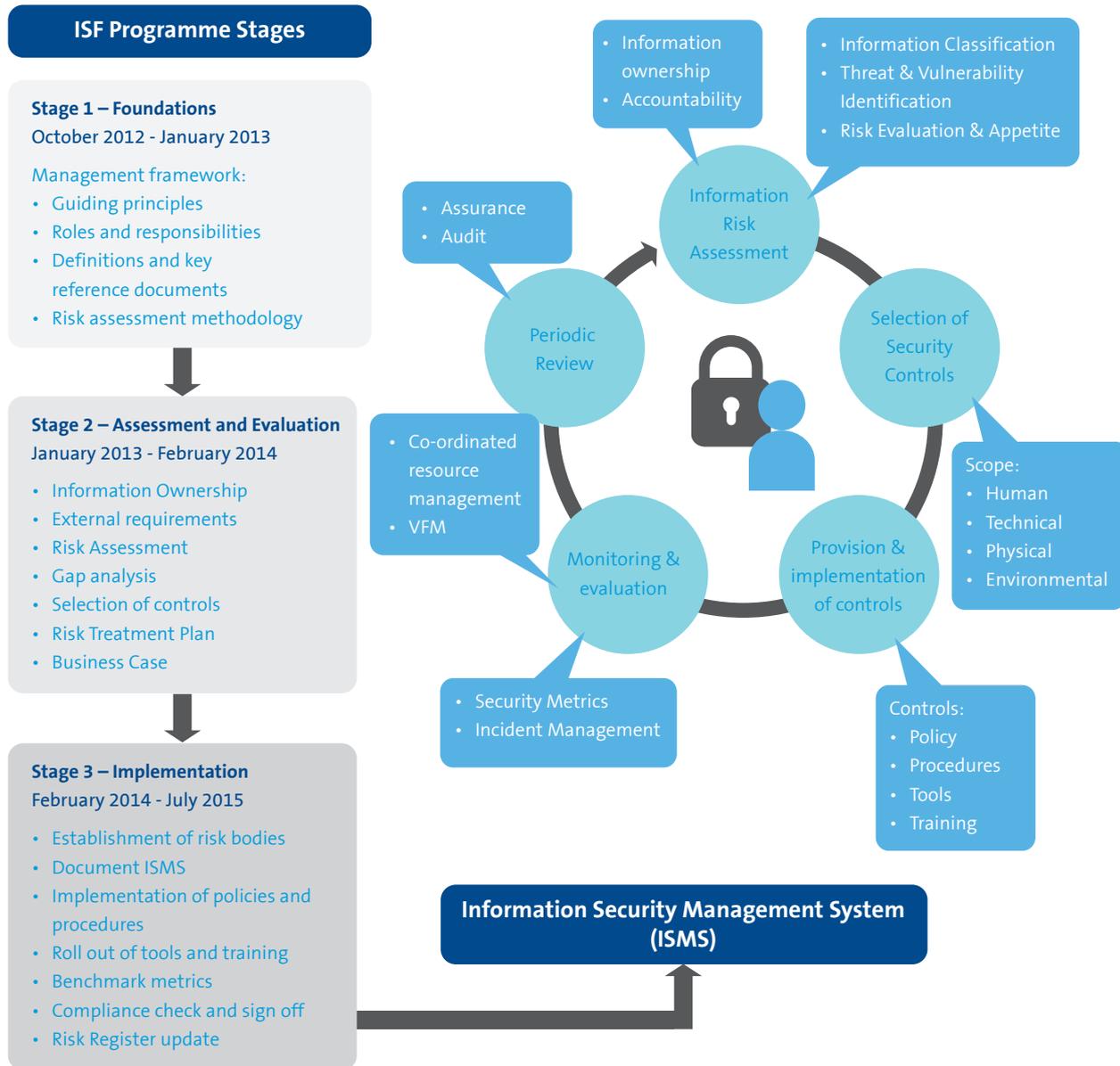
- [Different elements of an Information Security Management System – Cardiff University](#)
- [Stages for implementing an Information Security Framework \(ISF\) programme – Cardiff University](#)

## Different elements of an Information Security Management System – Cardiff University



# Stages for implementing an Information Security Framework (ISF) programme – Cardiff University

## Information Security Framework (ISF) Programme





# Resources for Chapter 1 – What is information security?

## RESOURCES

- [Template for an information security strategy proposal](#)

## Template for an information security strategy proposal

*“Reputation is like fine china: once broken it’s very hard to repair.”*

— Abraham Lincoln

Information risk management, or information security, is a crucial part of <ORGANISATION>’s operations. This document explains the case for improving our capabilities in this area, and provides an outline strategy to do so.

### What is the point of information security?

The bedrock of <ORGANISATION> is trust. Research integrity relies upon the ability to trust data. External investment depends upon <ORGANISATION>’s reputation, especially where it comes to medical data. Sharing research data with collaborators depends upon mutual trust. Equally, students and staff need to be able to trust <ORGANISATION> with their personal information.

Without adequate information security, the reputation of the University cannot be maintained. With our foundation of trust broken, funding will be awarded to other, worthier recipients, and lucrative partnerships will be dissolved. Research papers may no longer be accepted for publication. Lawsuits and fines could bring further financial losses, compounding reputational harm, and impacting <ORGANISATION>’s ability to recruit the best and brightest students and staff.

In summary, the goal of information security is to enable the University to be, and to be seen as, a safe pair of hands. The role of the <Infosec Department> is to advise, monitor and support the University in this area.

### What is the current situation?

The level of threat to the University is increasing. Previous critically damaging data breaches at other institutions (including <provide recent examples here> QMUL<sup>1</sup>, Indiana University<sup>2</sup>, Iowa State University<sup>3</sup> and the University of Maryland<sup>4</sup>) have shown that universities are seen both as sources of saleable personal information, and as resources for attackers to repurpose to suit their own needs. Information from official sources also indicates that research data may be sought for the purposes of industrial espionage. Finally, it is known that nation states are focusing strongly on the arenas of online attack and defence, and may see <ORGANISATION> as a source of intelligence.

Within <ORGANISATION>, incidents are increasing in frequency and severity <stats here>. The frequency of near misses and the risk of a catastrophe are also at <high/alarming/unacceptable> levels. <Give concrete example here>.

Other issues of relevance to our sector include:

An increasing appetite for partnerships and research collaborations handling sensitive information.

A strategic emphasis on an integrated approach to education, research and innovation.

The widespread use of unsuitable tools, such as email, for handling highly confidential information.

A lack of a coordinated approach to information security across <ORGANISATION>.

Information security is perceived as someone else’s problem, but it is everyone’s responsibility.

A widespread view that information risk management can be left until more important issues have been addressed.

### What are our options?

#### Do nothing

This is, as should be clear from the previous section, untenable. As threat levels are increasing, doing nothing actually means losing ground. This approach will result in increasing numbers of serious incidents, loss of reputation, and other damage to the University.

#### Apply stringent security measures across the whole University

This option would define a set of detailed security measures suitable for most environments, and apply them to all of the University; certain areas of greater risk would be subject to enhanced security measures. This approach has the advantage of being consistent, and is often adopted in corporate environments.

However, this “one size fits all” approach is inevitably going to be overkill in some environments, while inadequate in others. The University structure is also federated, so blanket implementation is likely to be a challenge to implement.

In short, this approach has two intrinsic defects.

- We cannot do it: it is too expensive and it is impractical.
- We should not do it: it is incompatible with the principles of federation, openness and academic freedom.

<sup>1</sup> [http://my.qmul.ac.uk/news\\_and\\_events/2014/121863.html](http://my.qmul.ac.uk/news_and_events/2014/121863.html)

<sup>2</sup> <http://news.iu.edu/releases/iu/2014/02/data-exposure-disclosure.shtml>

<sup>3</sup> <http://www.news.iastate.edu/news/2014/04/22/serverbreach>

<sup>4</sup> <http://www.umd.edu/datasecurity/> and <http://www.wusa9.com/story/news/local/2014/03/26/university-of-maryland-congress-data-breach/6942023/>

## A targeted approach

The University has legal and contractual obligations which inform our overall tolerance for risk. A targeted approach to information would focus most investment on areas of greater risk, such as those handling personal data, while providing advice and support to all University members. This would foster a culture of responsible risk taking consonant with <ORGANISATION>'s enquiring and innovative nature.

To achieve this goal, <ORGANISATION> could create three sets of good practice baseline recommendations, each relating to a level of risk. University members would be given the right support to select and tailor the most suitable baseline in any given situation. Their decisions on information risk would be independently validated<sup>5</sup> against the University's risk tolerance, while operational activities to manage information risk would be integrated into normal reporting lines.

The underlying principles of the targeted approach are as follows.

- Independent oversight by the <Infosec Department>.
- Integration with other normal University activities.
- Tailored security measures based on good practice, risk tolerance and business needs.

## Recommended option

It is recommended that the University adopt the targeted approach to information risk management, to enable a pragmatic, responsive and cost-effective implementation of its requirements.

## What action is required?

<ORGANISATION> should develop its information security approach as follows.

1. Assign overall responsibility for information risk management to a top level role.
2. Appoint a Senior Information Risk Owner for every <School/Department/Faculty>.
3. Create a detailed plan for independent governance of information risk that avoids conflicts of interest, includes segregation of duties, and leverages <ORGANISATION>'s existing resources and expertise.
4. Engage further with key areas handling medical, personal and other sensitive information to assess risks and requirements.
5. Develop information risk management baselines.
6. Formally integrate information and strategic/local risk management processes.
7. Invest in a broad-reaching programme of awareness and support for University members, with additional support for key areas.  
The key message: Information security is everyone's responsibility.

---

<sup>5</sup> In order to avoid the classic problem of "marking one's own homework".



# Resources for Chapter 2 – Information security governance

## RESOURCES

- [Template for an information security policy](#)
- [Responsibilities overview: Information ownership and risk management – Cardiff University](#)
- [Developing an information security policy – University of York, case study](#)
- [Bringing information security strategy to senior management – UCL, case study](#)
- [Key questions for top management](#)
- [Example of a presentation to sell the concept of an ISMS to top management](#)

## Template for an information security policy

### <ORGANISATION>: Information security policy

#### Introduction

[ORGANISATION]'s computer and information systems underpin all [ORGANISATION]'s activities, and are essential to [ENTER MAIN BUSINESS/FUNCTIONAL OBJECTIVES HERE].

The [ORGANISATION] recognises the need for its members, employees and visitors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this.

Security of information must therefore be an integral part of the [ORGANISATION]'s management structure in order to maintain continuity of its business, legal compliance and adhere to the University's own regulations and policies.

#### Purpose

This information security policy defines the framework within which information security will be managed across the [ORGANISATION] and demonstrates management direction and support for information security throughout the [ORGANISATION]. This policy is the primary policy under which all other technical and security related policies reside. [ENTER ANNEX LINK HERE] provides a list of all other policies and procedures that support this policy.

#### Scope

This policy is applicable to and will be communicated to [EXAMPLE: all staff, students and other relevant parties including senior and junior members, employees, visitors and contractors].

It covers, but is not limited to, any systems or data attached to the [ORGANISATION]'s computer or telephone networks, any systems supplied by the [ORGANISATION], any communications sent to or from the [ORGANISATION] and any data - which is owned either by the University or the [ORGANISATION]- held on systems external to the [ORGANISATION]'s network.

#### Organisation of information security

The [HEAD OF DEPARTMENT] is ultimately responsible for the maintenance of this policy and for compliance within the [ORGANISATION]. This policy has been approved by [SENIOR MANAGEMENT GROUP] and forms part of its policies and procedures.

[SENIOR MANAGEMENT GROUP] are responsible for reviewing this policy on an annual basis. They will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.

The [INFORMATION SECURITY ROLE] is responsible for the management of information security and, specifically, to provide advice and guidance on the implementation of this policy.

[OPTIONAL DEPENDING ON ORGANISATION SIZE]

The [INFORMATION SECURITY ADVISORY GROUP] comprising representatives from all relevant sections of the [DEPARTMENT/COLLEGE/OTHER UNIT] is responsible for identifying and assessing security requirements and risks.

It is the responsibility of all line managers to implement this policy within their area of responsibility and to ensure that all staff for which they are responsible are 1) made fully aware of the policy; and 2) given appropriate support and resources to comply.

It is the responsibility of each member of staff to adhere to this policy.

#### Policy Statement

The [ORGANISATION] is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for information security and to ensuring the continued business of the [DEPARTMENT/COLLEGE/HALL]. It is the [ORGANISATION]'s policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.

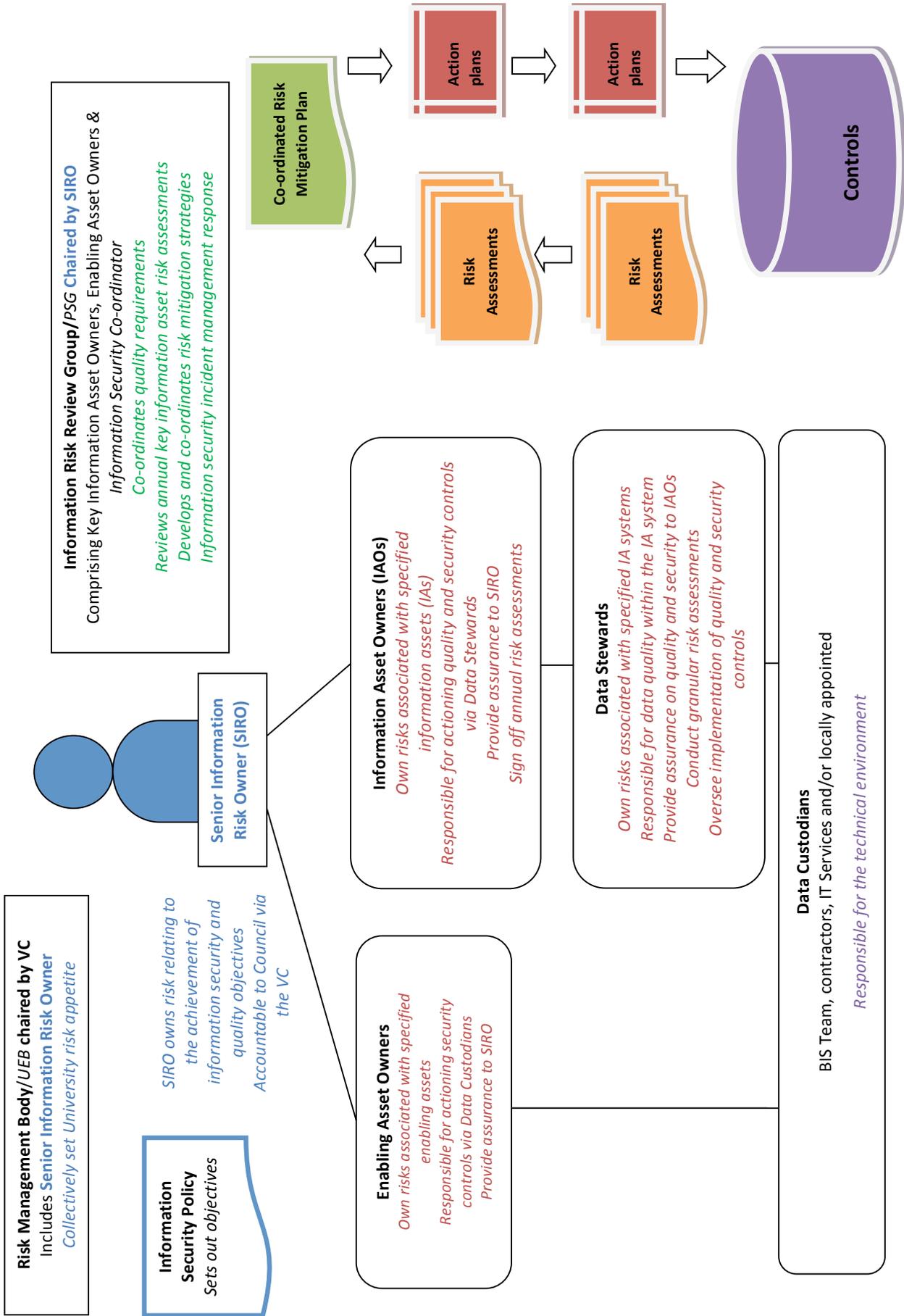
To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment shall be carried out in order to define security requirements and identify the probability and impact of security breaches.

Specialist advice on information security shall be made available throughout the [DEPARTMENT/COLLEGE/OTHER UNIT] and advice can be sought via the University's Information Security Team [ADD URL] and/or [ADD ADDITIONAL URLS, if required].

It is the [UNIT NAME]'s policy to report all information or IT security incidents, or other suspected breaches of this policy. The [UNIT NAME] will follow the University's advice for the escalation and reporting of security incidents and data breaches that involve personal data will subsequently be reported to the University's Data Protection Officer. Records of the number of security breaches and their type should be kept and reported on a regular basis to the [SENIOR MANAGEMENT GROUP/INFORMATION SECURITY ROLE].

Failure to comply with this policy that occurs as a result deliberate, malicious or negligent behaviour, may result in disciplinary action.

# Responsibilities overview: Information ownership and risk management – Cardiff University



## Developing an information security policy – University of York, case study

Like many organisations, in York we knew that our existing regulations and policies were old and increasingly inadequate. Research contracts were asking for policies which aligned with ISO/IEC 27001, our auditors were commenting on lack of policies, and IS/IT staff wanted more policy, both general and detailed to solve problems.

We had existing policy on Data Protection, Freedom of Information, Records Management and IT operations. This gave us a way of establishing the hierarchy of the new policies- but all the existing policies were rewritten during the course of the work.

Our first attempt was to take the specimen policies in the previous UCISA Toolkit and set about editing them. We thought this would be quick, but it turned out to be a disaster. The policies were too general, and in many cases did not fit with our institutional ethos. We found that such key policies are very institution based - specimen policies help to guide but very the real policies are very much about what will be tolerated and work in the setting of a given institution.

For our second attempt, we started from scratch. We agreed with institutional senior management an approval process for Information Security policies and drafted a list of policies that we needed based on ISO/IEC 27001. In our first attempt, we used existing committee structures to approve policy and the delays introduced were very large. For the new process, a senior member of staff was delegated power to approve policies in this area, with only policies that were felt to be contentious or that affected other areas taken to committee.

From there, we defined the general format of a policy. For us, a policy was to be a short (two page max) document at a high level. Underneath each policy there would be method statements and guidance containing the detail. We also agreed some basic definitions and use of terminology (e.g. *must vs. should*).

Next we agreed some overall principles:

- our aim was to help people to use data safely, not lock it away and make it hard for people
- the policies should apply to all data, irrespective of format (paper or electronic)
- avoid jargon
- exploit current good practice, introducing changes only where necessary
- we would not do any publicity or training until most of the policy suite was in place

These framework and principles helped us to get past some initial stumbling blocks around format and ensured that the suite of policies have a consistent feel, with common section and definitions and gave us some high level principles to help clarify what was in scope and not in scope for the policy suite.

Finally we agreed to avoid wide consultation early on in the process. We found it better to have something which has been worked on and is in quite good shape before opening it up for wider consultation. Without a specific document to focus on, we found that people found the issues hard to grasp and discussions were very unfocussed.

Once we had that overall process agreed, we started working our way through the list. We found some tricky issues during the process and, as ever, progress was slower than we expected in advance but overall, we have made good progress.

Even after a year of work, we are not done. Some of the subsidiary policies are not done and we are only just starting awareness raising but the policies are being referenced when new projects are started or bids submitted, the auditors are happier and external funders are being assured that the University can handle sensitive research data in a secure fashion.

### Summary

- Create policies tailored to your environment; do not copy templates blindly
- Provide well-developed documents for wider consultation, rather than a very initial draft
- Develop and agree a simple approvals process

## Bringing information security strategy to senior management – UCL, case study

At UCL, we began to formalise our information security strategy in late 2012, when the post of Head of Information Security was created.

The first stage involved finding out what was already happening, not on the process/controls level, but on the strategic and governance levels. We discovered the following:

- An existing UCL-wide risk management process, which was under further development
- The IT department was working to implement ITIL for improved process management and better customer service.
- There was a major University initiative to formalise project management.
- A role handling data protection and Freedom of Information, in the Legal Department
- A PCI DSS governance role in the Finance Department
- A Records Manager in the Library with responsibility for setting data retention policy
- A project underway to provide a secure data storage and processing facility (the Data Safe Haven project) in the School of Life and Medical Sciences. This project had already requested participation from the Information Security area.

All of the above activities revealed both organisational structures and roles with which information security management activities would have to interoperate, and existing processes which we could use or adapt.

But, although we could already see how to link information security management to some existing processes (e.g. risk management), and could see some new processes we'd need, we could not actually make any changes until we had top level buy-in: and a strategy.

We started by establishing how changes to top level university activities were normally raised, discussed and approved. It turned out that the existing management hierarchy was clearly defined and provided us with a route which looked as if it could work: through the Security Working Group and a number of other committees to the Senior Management Team of the University.

In parallel to my identification of a suitable and effective way to get the material to senior management, we began to write up an actual strategy.

Initially, we chose to create a presentation in order to keep the structure as fluid as possible, and to provide flexibility in presenting it- we could vary the path through the presentation dynamically to adapt to the audience. This also had the added benefit that we could easily present it in person for feedback during its development, rather than mailing out a document. This gave us immediate and frank feedback (e.g. if people fell asleep!) as well as the opportunity to get lots of practice in explaining the material to each audience.

While it was being developed, the presentation/strategy was presented to people and groups going up the management chain to senior management, so that each group could have a say in the content and it could continue to evolve. The net effect was that it would not, by the time it reached senior management, be a single person's take on what needed to happen, but a consensus and (hopefully) already acceptable approach. At each level, we asked for permission (and sometimes was urged) to take it to the next step in the governance chain.

The golden rule we adhered to during the development and presentation of the strategy was that, at the time of the presentation of the strategy to senior management, there should be no surprises on either side. A strategy without a suitable foundation would be less likely to be accepted. On the downside, the "excitement" was inevitably going to be diminished- but in information security and management, excitement is not generally conducive to effective operations...

To make the suggestions in the strategy more likely to be well received in a meeting with senior management, we realised that we should not rely on one route alone. It also seemed sensible to try out the draft strategy on individual members of the senior management team, to get feedback and suggestions. One obvious venue was the governance body which had arisen within the School of Life and Medical Sciences to manage sensitive data. We presented the draft strategy at one of the meetings, and received a huge amount of helpful suggestions. The ones which made the most impact were:

- It should be shorter (at the time, it ran to 60 slides...).
- It should relate to existing top level priorities. We had an overall University Strategy and five year plan- this strategy should relate directly to them.
- It should contain concrete examples- e.g. how much money could be saved by avoiding incidents.
- It should not require explanations- it should make sense by itself.

Following this meeting, the strategy was revised and improved significantly, and began to look like something which senior management would be happier with. We did not, however, add content to promise specific cost savings, as it would not have been based upon reliable data. One thing we did add to improve the immediacy of the proposal was a short list of recent incidents affecting universities.

With the strong support of my line management, and after about ten months of preparation, we were authorised to present the proposed strategy to senior management. Since the meeting format did not permit the use of presentations, we summarised the

strategy into two pages of A4 text. This was a critically important step, as it stripped the strategy and its justification back to essentials, and vastly improved them as a result.

When the date of the meeting arrived, the topic was scheduled for 10 minutes total - five minutes on the standard information security update, and five minutes on the strategy.

At the meeting, the group took some considerable interest in the information security update, but showed even greater enthusiasm for the strategy, which received unanimous support. In the end, the information security section of the meeting stretched to over 20 minutes.

The substantive feedback from UCL's senior management team was as follows:

1. They agreed to support the proposed strategy as presented.
2. They approved initial organisational changes to embed information risk management into normal operations, including the introduction of senior information risk owners at Faculty level.
3. They recognised that culture change was important to the success of information risk management across UCL.
4. They were strongly in favour of an awareness programme to improve attitudes to information risk.

Now the real work begins. We have an approved strategy, but need to make it happen. The challenges at hand are really high level and pervasive, such as culture change, and technical capabilities. The next steps we are going to take are the formalisation of information risk management across UCL, the implementation of an awareness programme, and further engagement with departments and faculties to understand their ways of working, risks and needs.

### **Summary points**

- Ensure you know how risk management is already working.
- Find out the accepted route for new ideas to be received, assessed and approved, and use it.
- Be patient: big changes which are going to stick take time to get going.
- Ensure that the strategy evolves as you present it to more people, so that it is fit for purpose.

## Key questions for top management

The university environment has some characteristics which influence the way in which information security can be managed. The organisation's senior management team, or "top management", having overall responsibility for information security, must consider these characteristics when designing the ISMS.

### Federation

Not all the information technology used within an organisation is provided (or indeed controlled) by a central IT service. This is particularly the case with IT supporting research but may also be the case in collegiate institutions or those that have a high degree of devolution. Similarly there may be specific administrative functions within departments or colleges. However, the impact of any information security breach is likely to be on the organisation, not the department.

- How do you ensure buy-in from those departments/units that operate semi-independently?
- Who, in those departments, is responsible for information security and how do they link with the institutional information security operation?
- How do you ensure that IT systems that are not under central control meet a base level of security (such as the Cyber Essentials promoted by BIS<sup>1</sup>)?

### Suggestions:

- The Senior Information Risk Owner (see Chapter 8, Roles and competencies), as part of their role, should take responsibility for selling information security to devolved departments.
- It may be appropriate for there to be a Senior Information Risk Owner for each devolved operational unit. These would have responsibility for championing information security policy and requirements within their department.
- A hybrid approach to technical security may be adopted where a base level of security is required for a given classification of information, but each operational area is provided with the tools to implement controls as they see fit. Relies heavily on independent support and oversight, quite time consuming as there is no economy of scale for a number of things.

### Autonomy

Academic staff involved in research often operate with a degree of autonomy. They bid for funding and are responsible for the use of those funds to deliver the specified research. The requirements of that research may result in the development of bespoke IT systems. Although these are effectively production systems, they are largely unsupported and may present an information security risk. Staff can and do go to retail outlets and purchase IT equipment for use in the organisation, particularly for research. Such equipment may not meet the standards of the organisation.

- How do you ensure researchers understand the sensitivity of the information they collect and store?
- Does your research ethics policy take into account information security issues?
- Do you know where collections of personal or sensitive data used in research exist?
- Do you have a procurement policy that restricts the purchase of equipment to a defined and supported product set?
- Do you have a storage strategy that mitigates the need for researchers to purchase storage outside of the institutional purchasing procedures?

### Suggestions:

- Researchers that are working in departments where they are likely to utilise personal or sensitive information should be regularly given awareness training and refresher courses;
- As a minimum, the minutes of research ethics committees should be forwarded to the information security group to allow them to advise on appropriate security measures, and log the existence of sensitive data collections.
- Consideration should be given to mandating procurement of IT equipment through established procedures to ensure that all equipment is to a standard that may be supported by the IT function.

### Home working and use of personal devices

Use of personal devices such as phones, tablets, etc by both staff and students for handling organisational information has increased to almost become the norm. Students look to access resources remotely in order to write and submit coursework, to revise, etc.

---

<sup>1</sup> <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>

Organisations increasingly accommodate home working for their staff as part of flexible working practices. Visitors bring their own devices onto the campus and access resources either within the organisation or from their own organisation. Each form of access presents a risk to information security.

How are the security risks associated with personal devices accommodated in your policies and procedures?

### **Suggestions:**

- The location of the key information assets in your organisation needs to be known and understood and appropriate measures taken to protect them.
- It may be appropriate to restrict home working to trusted devices provided by the organisation and with appropriate security measures already in place.
- The wireless network may be deemed to be untrusted given that personal devices may connect to it with little or no verification. Consequently the organisation may consider placing a firewall between the wireless part of the network and the main campus network.

### **Unclear boundaries**

The individuals who access an organisation's information are not just restricted to traditional definitions of staff and students. The permanent staff may be supplemented with visiting lecturers, research collaborations will require staff from other universities to have access to resources, alumni may have access to resources, employees from other organisations may take part in professional development activities, etc. The physical boundaries of an organisation may not be restricted to the organisation alone as buildings can be shared with commercial entities which are spun-off from research projects, and which use the same facilities as the organisation itself.

In some cases, access to resources is provided to individuals that are never physically present. The increase of distance learning means that the organisation may virtually extend to all corners of the globe. Some universities have sought to extend their reach by engaging in partnerships with overseas institutions or by setting up overseas campuses.

- How are the information security requirements of the organisation communicated to non-traditional members of the organisation?
- Should any special measures be applied to off campus students or staff?
- Were information security policies considered when the decision was made to establish an overseas campus?

### **Suggestions:**

- There needs to be a readily accessible way of making such members of the organisation aware of information security and their responsibilities for ensuring that the organisation's policies are adhered to.
- The organisation may need to consider adherence to information security policy as part of any tenancy arrangement for external organisations.
- Access to resources and systems should be time limited for temporary staff.
- There should be processes in place to determine the appropriate levels of access to organisational resources and systems for all members of the organisation.
- Organisations should consider the legislative requirements of nations where overseas campuses are being established and their impact on the institutional information security policy as part of the planning process.

### **Openness, sharing and cyber security initiatives**

There is a drive towards making the outputs from research and the data behind it publicly available. Researchers, on the other hand, have built their reputations on the research they have produced and are looking to protect their intellectual property. In addition, the Government is also pressing the higher education sector to take appropriate steps to protect the intellectual property that is generated within the organisation. The organisation will need to balance openness with the requirements to protect key research and information assets.

- Are the requirements of open access well understood at your institution?
- Have the resources been committed to meet the requirements for the sharing and archiving of research data?
- Are the locations of research data that may result in commercial benefit to the organisation known?
- Suggestions:
  - The balance between openness and individual academics' desire to protect their intellectual property is a political, not information security, issue. The organisation's top level management should drive the policy for open access.
  - Research that may deliver a commercial benefit to the organisation should be treated as a critical information asset and protected as such.

## Commercial relationships

Some research is conducted in association with or on behalf of commercial organisations. Consequently there may be specific security conditions included in the research contract to ensure that the data are protected.

- Does your organisation take a lead in defining the security requirements for commercially sensitive research data?

### Suggestions:

- A structured approach should be in place to manage contracts which may be commercially sensitive. These should build on existing business processes and ensure legal due diligence.
- The processes should be in place to ensure that, if required, the ability to provide information security oversight can be easily demonstrated.

## Communities of users

Different categories of users will have different views on information security, different appetites for risk, and different levels of understanding of the requirements of the organisation's information security policy. Culture varies across the organisation. This is not restricted to differences between staff and students nor is it to differences between administrative and academic staff. All need an understanding of information security risks and their roles in delivering the information security policy.

- How do you accommodate a wide range of skills and experience levels when implementing an institution wide policy?

### Suggestions:

- Risk management should be built into normal working practices so that staff recognise all risks, report them and take mitigating action where appropriate.
- The awareness activity needs to take cognisance of the variety of expertise, approaches and understanding members of the organisation have

## Turnover

Universities are dynamic organisations with a high turnover of personnel. Some of this turnover is known and managed; student course dates are known and established processes are in place to manage registration and, on completion, graduation. However, not everyone completes their course and there need to be processes to manage exit of those students who drop out or otherwise do not complete their studies. There will be processes to manage *regular* staff entry and exit and these will usually be the responsibility of a Human Resources function, whether centralised or devolved. The processes around *ad hoc* members of staff and other members of the organisation that have access to resources and systems also need to be well managed; these processes may be devolved to a wide range of departments or functions and so may not be so well defined.

- How well is information security awareness built into your induction processes for staff and students?
- Are ad hoc members of the organisation included in awareness activity?

### Suggestions:

- Tailor the awareness campaigns for each part of the organisation's community which matches the level of risk and the rate of turnover.
- There should be appropriate processes in place for induction, ongoing awareness and exit for all members of the organisation.

## Example of a presentation to sell the concept of an ISMS to top management

### Slide 1



### Slide 2

#### What is information security?



Protection from threats to ensure the continued:

- confidentiality
- integrity
- availability

of our information

The slide includes a graphic of a 'PROTECTED' stamp with diagonal lines, positioned to the left of the text.

Take definition from International Standard on Information Security Management - the ISO/IEC 27000 suite

- **Confidentiality** - ensuring that information is accessible only to those authorised to have access
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods by protecting against unauthorised modification
- **Availability** - ensuring that authorised users have access to information and associated assets when required
- **ISO/IEC 27001** sets out structure and process for implementation of an ISMS
- **Not just about IT** – physical and human aspects!!

### Slide 3

#### What threats?



- Damage to operations
- Damage to reputation
- Legal damage

The slide features a graphic of a red sign on a wooden post that reads 'DANGER THIN ICE', set against a background of a cloudy sky.

Any time anywhere and bring your own devices = multiple threats

Accidental or malicious loss of data and lack or failure of back up

Theft of personal data or IP

Inappropriate disclosure of information – breach of confidence

Loss of access to electronic data (viruses, denial of service)

Fines & undertakings from Information Commissioner

Inability to compete for research grants

#### Slide 4

### The Programme's Vision



The University will operate in a manner where security of information is balanced with appropriate accessibility of that information....

...providing the optimum level of risk management to support the University's strategic goal of being a world leading institution.



It's all about risk assessment and balance – need for University approach both risk assessment and mitigation resource

#### Slide 5

### Where are we now?

| RAG definition  |  |
|---|--|
|  | Information Security Management System based on international standards in place. Audit trails and evidence of compliance readily available.   |
|  | Information security policies developed, risk ownership accepted and awareness improving. Comprehensive training plan agreed. Risks assessed and toolkits developed. Baseline for metrics established.         |
|  | Patchy awareness of information security. Individuals manage security within a loose policy framework. Information security risk decisions taken in isolation. No senior risk owners for information security. |

#### Slide 6

### What does the future state look like? - Leadership



- Senior ownership of information security risk
- Strategic decisions about tolerable levels of risk

Importance of the risk appetite being set at a senior executive level. Looking at risk register and how we assess and accept risk. The all important strategic balance.

## Slide 7

### What does the future state look like? - *Organisation*



- Information assets identified, owned and risk assessed
- Co-ordination of information security resources

ISO/IEC 27001 structured approach to implementation

Information assets – concept of ownership across the institution, e.g. 'student data' no matter where it's held

## Slide 8

### What does the future state look like? - *Business Change*



- Consistent policies, procedures and decisions
- Universal tools and training
- Clear lines of accountability
- Evidence and audit

Delivering business change all important – not just an exercise in producing policies but in effecting a change in behaviour.

## Slide 9

### Benefits and Opportunities



**Your data  
is safe with us!**

# Resources for Chapter 3 – Drivers

## RESOURCES

- Incidental security improvements from sustainability policies – UCL, case study
- Information security within the research arena – Loughborough University, case study

## Incidental security improvements from sustainability policies – UCL, case study

UCL Human Factors researchers, led by Prof. Angela Sasse, collaborated with a large telecommunications company and a large utilities company. Researchers interviewed employees across a variety of roles within the companies to understand how security played a role in their working practices: specifically, the interplay between security mechanisms and individual employees' primary (productive) tasks. It was important to understand perceived frictions and benefits of security within the workforce (see Chapter 8, Roles and competencies).

The study found that there was scope for policies and organisation-wide initiatives outside of security to indirectly improve the security posture of an organisation, or otherwise encourage behaviours which were also more secure.

### Awareness

Environmentally-sound practices may be promoted side by side with health and safety, or be the focus of specific campaigns such as organisation-wide sustainability drives. In the telecommunications company, employees were encouraged, through training and visible campaigns, to consider the cost of their working behaviours to the environment, and adopt *green* thinking in practice. For some in the organisations, this *thinking green* was more approachable and had a clearer purpose than understanding security and its drivers.

Individuals can be encouraged to adopt visible practices that they can take pride in, and which the organisation can measure against targets. Training relating to sustainability was found to be a channel for recommending behaviours which were incidentally more secure than existing practices.

### Paperless approaches

Related policies included the development of a *paperless* office. This encouraged the rationalisation (and ultimately, limiting) of document printing, and - when documents were printed - having printing enabled locally at the printer with existing ID access cards. This then involved users consciously in their own printing of documents and had the potential to create a greater sense of ownership over their personal impact within the organisation, while also recording print rates per employee. This demonstrates change within already existing habits (conscious printing), incidental security (limitation of unattended printouts), as well as a clear measure of performance against company policy (the limitation of printed documents).

### Secure disposal

Secure document bins were provided, distributed in such a way as to be within easy access of all employees, further supporting involvement. Crucially this showed consideration of both employee needs (the need to dispose of sensitive documents) and the minimisation of disruption to working habits (limiting the cost to the individual to comply with the policy).

Indirect improvements included a reduced likeliness of documents being left on desks or left overnight in shared office space. There were also less physical copies of confidential documents in circulation, and there was less opportunity for individuals to pick up someone else's printouts from printers (where the action taken with those printouts could otherwise not then be tracked).

### Remote working

A paperless office also complemented remote working - individuals would tend towards carrying less print-outs with them when travelling, where otherwise printed documents might have been carried around or left over various locations for any length of time. In the utilities company, there was also a drive toward minimising travel outside of the company where possible as a means to develop sustainable practices (moving instead to (secure) communications applications) - this would incidentally limit exposure of the organisation's assets to risks present in other locations, but would have required investment and guarantees around reliable alternative solutions for communication

### Storage benefits

The utilities company also tried to minimise storage costs and adopt just-in-time resourcing practices where appropriate. Sustainable practices such as site management can then be linked to recognised standards, e.g. ISO14001 ("Environmental Management"). This demonstrates clear relation of outcomes to high-level expectations.

### Avoiding confusion

There was a need to be mindful of how policies must join up effectively. Both companies provided secure shredders, where shredded documents were then collected by a contracted outside company for disposal. Staff in the telecommunications company were instructed to direct documents either to recycling bins or to confidential document shredders based on their sensitivity classification - this had the potential to confuse employees who wanted to respect both security and the environment. In the utilities company, the policy around disposal of computers (and specifically hard drives) needed to respect data protection concerns raised by employees themselves ("*There's no way you're just taking this away to recycle it, do whatever with it.*") - individuals with knowledge of security will need assurances that other parties are protecting their information.

### Key points

- Ensure that there are tangible benefits of following organisation policies.
- Know your suppliers
- Engage with members of the organisation to understand how policies combine in practice within their roles, and where improvements can be made.

## Information security within the research arena – Loughborough University, case study

Over the last few years within Loughborough University, there has been an increased requirement for Information Security input to research project proposals, grant applications and contract agreements. Supporting research within the organisation is an important activity; but it is recognised that it is different to supporting the teaching and learning activity.

### Awareness

One of the earliest activities required was an awareness campaign within the research community. Colleagues were often in sections of academic schools which did not have the same level of cascaded information about central IT services and support. Providing focused communications explaining what support was available to researchers was greatly beneficial to increase awareness and was welcomed by the recipients.

There is a parallel theme of changing culture and improving training, which is focused across the organisation. The research community within Loughborough have welcomed these initiatives with open arms as they can sometimes feel isolated or unsure how to get the IT support required by their research. Opening a dialogue in the information security area has brought about a change in provision in other areas to the benefit of the wider organisation.

### Third party requirements

#### Auditing

As part of a pre-existing research contract, the University received a request from the commercial company supporting the research to allow a security audit of the information systems used to facilitate the research activities.

The commercial company audit team spent two days on site reviewing the written policies, technical controls and undertaking testing of the systems concerned. Whilst the activity took several days to prepare for (as the information security controls were not as mature as required), the exercise was greatly beneficial, as the University received an external and commercial perspective on the security controls required. With a small number of recommendations for improvement being received, it was a positive activity and something which has been repeated, in subsequent years, by the commercial company.

Depending on the nature of the research, organisations will engage with different companies, research organisations and other academic institutions. Based on the number of information security surveys, questionnaires, forms and interviews completed over the last ten years, there is an increasing similarity of questions being posed. From the straight forward such as “Do you have a firewall?” to providing copies of patching policies. In order to improve responsiveness to these requests for additional information, colleagues in the information security function were quick to produce a number of stock responses in a default proforma.

#### Data disposal

One of the interesting requests received was that of assurance of data disposal following previous research activities. One of the research grants required assurance that previous research information assets from a previous grant were passed to the funder to be centralised with confirmation that the data has been securely destroyed from site. This can be a challenge with modern file space provision with: volume shadow copies, tiered storage and backup robots. In the case of Loughborough University, it took a three month period for this data to be removed through a cycle of standard process activity.

#### Secure communications

The use of secure electronic mail technology has been raised a couple of times by funders; the preferred access mechanism for government related research grants appears to be the Criminal Justice Secure Email. This provides a secure webmail facility to interact with the police, government and solicitors. There is an option to integrate this into the standard desktop email client in some scenarios, depending on the Business Impact Level (BIL).

#### Information leakage

A large part of supporting research at Loughborough University has focused on a risk assessment of information leakage and what controls are required to mitigate this risk. The government Business Impact Level assessment process continues to be used, despite the new Government Security classifications introduced on 2 April 2014. The Business Impact Level provides guidance on the risk assessment process; the new classifications are not used to label the information. However, researchers do not fully understand what this means, and what systems can meet this level of data. Funding applications are starting to request a Risk Management and Accreditation Documentation Set (RMADS), which describes the Business Impact Level of the information being held/processed.

#### Managing costs

If there are any costs associated with providing information security support to a research project, it is important to investigate the funding schedule available as this tends to differ depending on the research funding partner. Based upon experience, information security costs are often overlooked when putting the research grant together. At Loughborough University this was introduced as part of the central advice provided by the research and enterprise offices. Areas which may need to be included in funding include

penetration testing, managed hosting services and a secure coding audit for middleware.

Within Loughborough, a pragmatic approach has been made to address the areas described in this case study, initially utilising the resource which is available for information security, there was no additional funding or posts provided.

### **Maintenance of “orphaned” information systems developed for research.**

At the end of a research project, there is the requirement to make the research data, methodology and reports available. However, researchers’ effort is being moved onto the next project and next grant. This leaves the previously created systems unsupported.

Based on experience in the sector, non-maintained and development systems pose a credible risk and easy attack vector.

One of the first steps to addressing this issue at Loughborough has been to require these systems to be installed on virtual machines within the infrastructure managed environment. This provides a regular three monthly vulnerability assessment of the virtual machine with exception reporting. It is important to recognise this is the first step to try and address this problem and it is not the panacea to solving the issue. Within Loughborough University, we also provide a central hosting solution for blogs based upon WordPress, to manage the security aspects of the software.

### **Research data management**

Research data management is a hot topic among many organisations. Loughborough is no different in this- we are investigating how to make research data available to the public in a secure and sustainable manner.

### **Learning Points**

- Researchers may not be aware of the Information Security support offered by your organisations, so run a campaign to make them aware.
- Some research grants or contracts may require your organisation to undertake a formal security assessment as part of the agreed terms.
- The questions which form part of research, grant or contract applications are broadly similar. Consider creating a bank of stock responses which will make the completion of these documents easier.
- Funding for research tends to be made available up front as part of the grant or contract; introduce any associated costs, for example an external penetration test, upfront.
- At the end of a research project, some information systems will become orphaned. Consider research data management and how the organisation will manage information at the end of a project to avoid information systems being left unmanaged.

# Resources for Chapter 4 – Scoping

## RESOURCES

- [Scope definition for a data safe haven – UCL, case study](#)

## Scope definition for a data safe haven – UCL, case study

The purpose of the UCL Data Safe Haven is to enable researchers to access and use sensitive identifiable data in a secure manner. It was created by the Information Services Division on behalf of the School of Life and Medical Sciences (SLMS), but a few research studies outside SLMS who need to handle sensitive identifiable data also use it.

In 2013, a decision was made to achieve certification to ISO/IEC 27001 for this environment. Work began in early 2014, and we passed our first certification audit in May 2014.

### Multiple scopes

Certification of the whole of UCL was not appropriate or feasible, so we had to think very carefully about how to define our scope: what were we controlling, what would be audited and what would be certified?

In the end, we decided that we actually had four different scopes:

- The scope of the Data Safe Haven, which we called the “organisation”, to match the term used in 27001. This was a challenging term to use, as it had to be clear that we did not mean the whole of UCL when we used the word “organisation” in project meetings
- The scope of the ISMS
- The scope of audit
- The scope for certification

We agreed that the staff of the organisation should be defined as follows:

- Staff who manage and administer the environment (physically and logically)
- Staff who use the environment for research
- Top management who make executive decisions

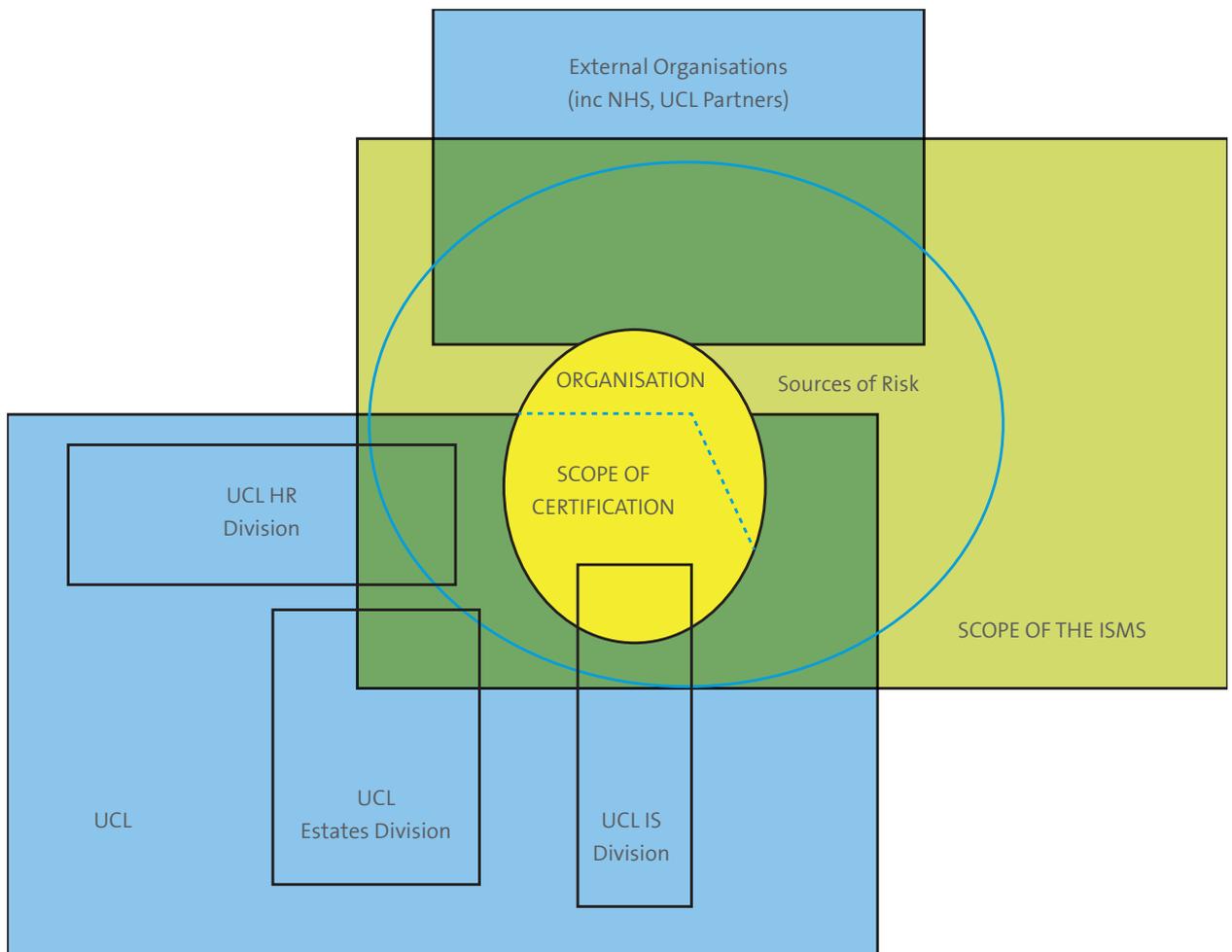


Figure 1: Scope diagram for UCL's Data Safe Haven

As can be seen in Figure 1, the scope for certification is a subset of the scope of the organisation, which is itself a subset of the scope of the ISMS. The scope of the audit was effectively the same as the scope of the ISMS, so anything within the ISMS could have been audited, but only those items within the scope for certification could have been certified.

## Understanding our scope

In order to get to this point, we had to work through a number of difficult issues.

The first problem which we had to solve was how internal third parties, such as HR and Estates, would fit into the picture. HR defines contracts and pre-employment checks, as well as carrying out some checks at the request of research units, while Estates controls physical security (e.g. card access to server rooms, and physical access to researcher offices).

It was decided that UCL parties which were outside our organisation should be treated:

- as sources of risk;
- as providers of controls.

We considered the options and agreed that the controls they carried out were within the ISMS, but external to the organisation. This was arrived at through externally facilitated workshops with members of the core project team, focusing on specific areas of risk.

What about external third parties? We could have managed service providers through contracts - but thankfully we had no external service providers. We did, however, have external entities which needed to pass data into the environment. We treated them as external potential sources of risk, rather than as part of our scope for certification.

Finally, how should we handle researchers? Most researchers were included within the scope of certification. However, one research study from another faculty was agreed to be part of the organisation, but was being treated as a “customer”, and was hence excluded from the scope of certification. This is shown in the illustration as the diagonal part of the dotted line inside the “golden egg”.

## The scope statement

Our official scope statement for our certificate was short and sweet: “The provision of the “Data Safe Haven” environment for the processing and storage of personal identifiable information in accordance with the Statement of Applicability version 1 dated 6th May 2014.” In contrast, our detailed scope document runs to seven pages, with five diagrams. This is due to be extended by adding in explicit references to external legislative, statutory and contractual requirements, at the recommendation of our external auditors.

## Learning points

- There are likely to be a number of different ideas about what scope means. At the beginning of your compliance work, put more effort than you think is necessary into clarifying the terms used, and reinforce the definitions for your chosen scopes regularly, to keep everyone on track.
- Identify your external parties and decide early on whether they are within your scope for compliance or outside it, and how you will handle the issue at audit time
- Specify all of your external drivers explicitly, so that you can justify any controls which they require, and so that their impact on your decisions about scope can be understood.



# Resources for Chapter 5 – Risk assessment

## RESOURCES

- [Template for information risk management principles](#)
- [Development and use of risk assessment templates – UCL, case study](#)
- [Project information risk assessment – Requirements and expectations – UCL](#)
- [Service information Risk assessment – Requirements and expectations – UCL](#)
- [Project information risk assessment – Capability - UCL](#)
- [Service information risk assessment – Capability - UCL](#)
- [Risk treatment plan – UCL](#)
- [Risk assessment methodology – Cardiff University](#)
- [Information asset register tool – University of Oxford](#)

## Template for information risk management principles

These top level guiding principles apply to all information handling activities, including project work and day to day operations. They are intended to be used to inform and guide organisations in their normal work, and to ensure that information is handled in a suitably secure fashion.

|    |  |   |
|----|--|---|
| 1  | Business requirements drive security requirements  | Security requirements should exist to support the requirements of a business activity and should be relevant and appropriate.   |
| 2  | Protect the confidentiality, integrity and availability of information to the right levels | Information's requirements for confidentiality, integrity and availability should be identified and security measures should be matched to these requirements.  |
| 3  | The campus network is not the security perimeter   | Because the campus network connects thousands of machines under widely varying management regimes, it should be considered in the same risk category as the open Internet. Any machine which you would not connect to the Internet without some form of protection should have the same protection installed before enabling access from the general campus network.  |
| 4  | Role-based access  | Privileges should be assigned to roles, not individual people. People should then be assigned roles.  |
| 5  | Least privilege  | Each role should have the minimum set of privileges needed to carry out the tasks required of that role.  |
| 6  | Separation of duties   | Where the risk or impact of a failure to execute a process correctly is unacceptably high, the process should require appropriate oversight before it can be completed. For example, when placing a purchase order, it has to be approved by a second person before it can be placed, or when writing software, a code review is undertaken by a second person before release.  |
| 7  | Segregation of environments handling information rated at different security levels        | Systems which store, process or transmit information classified as secret should be physically segregated from other systems which operate with information at a different level (e.g. normal). Systems which store, process or transmit other levels of information should be logically separated. Logical segregation can be achieved by appropriate network architecture. Note that it is expected that development/test and pre-production/production systems will be handling information at different levels. |
| 8  | No sensitive data on test systems  | Development systems should not hold any data rated other than <i>normal</i> . Test and pre-production systems which require data rated other than normal should be secured to the same standard (or better e.g. only accessible to a specific network or set of hosts) as the related production system.  |
| 9  | Traceability of activity to individuals  | This is restricted to operations involving information above <i>normal</i> . Actions carried out by an individual on information should be capable of being traced back to that individual.   |
| 10 | Documented security standards  | Information processing systems where data with a classification other than <i>normal</i> are processed should be designed, deployed and managed according to documented security standards (e.g. a secure software development lifecycle).  |
| 11 | Competence and training  | Individuals must be competent to carry out their responsibilities. Heads of Departments and Divisions must ensure that training to the appropriate level is provided.   |
| 12 | Responsibility and accountability  | Roles where there are activities which require access to information rated other than <i>normal</i> should have those activities clearly documented as part of the role description. In addition, the responsibility for protecting that data should also be clearly defined in the role description along with a path of accountability to the line management structure.  |
| 13 | Continuous improvement   | All roles should be responsible for identifying and highlighting opportunities for improvement to manage risk.<br><br>Systems and processes should be improved as opportunities appear.   |
| 14 | Defence in depth   | No individual security measure should be relied upon in isolation to protect information.   |
| 15 | Risk ownership   | Information risks should be owned by a role at an appropriately senior level in the organisation i.e. one with sufficient authority to ensure the risk is effectively managed.  |

## Development and use of risk assessment templates – UCL, case study

### Development of the process and templates

The risk assessment templates were initially developed from the NIST SP 800-39 methodology (Managing Information Security Risk) and adapted to suit our environment. Since they were first developed, they have been put into practice and iteratively improved.

### Using the process and templates

The process involves first completing the requirements and expectations document with the key people involved in the project/service; this looks at the type of information involved, and any internal and external requirements. The capability document is then completed; this looks at how the information is stored, processed and transmitted, and the risk scenarios involved. Once the risks have been identified and controls proposed, a risk register/treatment plan is created and managed by the project manager or service owner. If a server and/or web application is involved, then a penetration test is included in the process, and any vulnerabilities found are included in the risk register.

### Integration with the Project Delivery Framework

We were fortunate to have support from our project management office, who agreed to include our process and templates into their project delivery framework. We are also included at project gates, and before projects were given any money. This enables us to identify whether a project has been through the risk assessment process, and, if they have, whether they have implemented our recommendations. If it is found that the project has not been through a risk assessment, they are asked to complete one before they may proceed to the next stage in the project delivery framework. This has been beneficial, as previously it was possible for projects to proceed without any input from the Information Security Group.

We are also included as approvers in the yearly bid process. This involves us reviewing all the bid documents and adding comments relating to the amount of input we will need to have and whether any penetration testing needs to be budgeted for.

### Findings so far

The general consensus has been very positive. However we have found the perception before a risk assessment has taken place to be quite negative, with people presuming that we would block their project or slow it down. By integrating ourselves into the project delivery process, we are hoping to stop the possibility of us slowing projects down; this would only happen if we were not consulted until the very last minute. We now try to make it clear at the beginning of the process that we are there to help project teams achieve what they need to achieve in a safe way; we are not there to stop them. We see this whole process as continually improving; the more risk assessments we do, the more we can add changes and improve the process.

### Learning Points

- Do not reinvent the wheel - use approaches that have already been tested and adapt them to suit your organisation.
- Ensure you integrate with your organisation's project delivery process; it's the easiest way to make sure they involve you.
- Get buy-in; if those involved understand that you are ultimately trying to help them, you are less likely to find resistance.

## Project information risk assessment – Requirements and expectations - UCL

|                      |  |
|----------------------|--|
| Project Name:        |  |
| Project Manager:     |  |
| Service Owner:       |  |
| Author(s):           |  |
| Date completed:      |  |
| Date of next review: |  |
| Scope:               |  |

### Information Classification

Classification(s) of information involved:

| Classification    | Description of classification  | Is this information used, stored or affected by project? | Type(s) of Information   |
|-------------------|--|--|--|
| Secret            | Loss, tampering or disclosure would seriously damage operations as a teaching, learning and research organisation.<br><br>Example: identifiable patient information, personal financial details (bank account code, tax codes, payment card details), confidential investigations.                 | Y/N  | Describe information which has been identified as being Secret.            |
| Highly restricted | Loss, tampering or disclosure would result in significant legal liability, severe distress to individual(s), significant loss of asset value or severe damage to organisational reputation.<br><br>Example: staff appraisal records, student profiles, unpublished commercially sensitive material | Y/N  | Describe information which has been identified as being Highly Restricted. |
| Restricted        | Loss, tampering or disclosure would cause significant upset to individuals, may result in financial penalty and harm organisational relationships.<br><br>Example: main web page   | Y/N  | Describe information which has been identified as being Restricted.        |
| Normal            | Loss, tampering or disclosure would cause temporary inconvenience or minor reputational damage.<br><br>Example: email requesting the location for a meeting on fridge cleaning.  | Y/N  | Describe information which has been identified as being Normal.            |

## 1 Information Security Attributes

Requirements of the information which the project is handling:

|                 | Level of concern (low/medium/high) |
|-----------------|------------------------------------|
| Confidentiality |                                    |
| Integrity       |                                    |
| Availability    |                                    |

## 2 Internal requirements

What internal policies, procedures and other requirements apply to the security of the information being handled by the project?

## 3 External requirements

What external legislation, contracts and other requirements apply to the security of the information being handled by the project?

## 4 Penetration testing requirements

|                 |     |
|-----------------|-----|
| Web application | Y/N |
| Server          | Y/N |

## Service information risk assessment – Requirements and expectations - UCL

|                             |  |
|-----------------------------|--|
| Service Name:               |  |
| Service Owner:              |  |
| Service Operations Manager: |  |
| Author(s):                  |  |
| Date completed:             |  |
| Date of next review:        |  |
| Scope:                      |  |

### 1 Information Classification

| Classification(s) of information involved: Classification | Description of classification   | Is this information used, stored or affected by service? | Type(s) of Information   |
|---|---|--|--|
| Secret  | <p>Loss, tampering or disclosure would seriously damage operations as a teaching, learning and research organisation.</p> <p>Example: identifiable patient information, personal financial details (bank account code, tax codes, payment card details), confidential investigations.</p>                 | Y/N  | Describe information which has been identified as being Secret.            |
| Highly restricted   | <p>Loss, tampering or disclosure would result in significant legal liability, severe distress to individual(s), significant loss of asset value or severe damage to organisational reputation.</p> <p>Example: staff appraisal records, student profiles, unpublished commercially sensitive material</p> | Y/N  | Describe information which has been identified as being Highly Restricted. |
| Restricted  | <p>Loss, tampering or disclosure would cause significant upset to individuals, may result in financial penalty and harm organisational relationships.</p> <p>Example: main web page</p>   | Y/N  | Describe information which has been identified as being Restricted.        |
| Normal  | <p>Loss, tampering or disclosure would cause temporary inconvenience or minor reputational damage.</p> <p>Example: email requesting the location for a meeting on fridge cleaning.</p>  | Y/N  | Describe information which has been identified as being Normal.            |

## 2 Information Security Attributes

Requirements of the information which the service is handling:

|                 | Level of concern (low/medium/high) |
|-----------------|------------------------------------|
| Confidentiality |                                    |
| Integrity       |                                    |
| Availability    |                                    |

## 3 Internal requirements

What internal policies, procedures and other requirements apply to the security of the information being handled by the service?

## 4 External requirements

What external legislation, contracts and other requirements apply to the security of the information being handled by the service?

## 5 Penetration testing requirements

|                 |     |
|-----------------|-----|
| Web application | Y/N |
| Server          | Y/N |

## Project information risk assessment – Capability - UCL

|                      |  |
|----------------------|--|
| Project Name:        |  |
| Project Manager:     |  |
| Service Owner:       |  |
| Author(s):           |  |
| Date completed:      |  |
| Date of next review: |  |
| Scope:               |  |

### 1 Project Context

How is information stored as part of the project?

How is information processed<sup>1</sup> as part of the project?

How is information transmitted<sup>2</sup> as part of the project?

<sup>1</sup> Includes creation and destruction

<sup>2</sup> Sent and received

## 2 Risks and mitigations

| Risk scenario  | Example(s) | Controls in place | Likelihood | Impact | Proposed additional controls |
|--|------------|-------------------|------------|--------|------------------------------|
| User deliberately or accidentally leaks information            |            |                   |            |        |                              |
| User accidentally or deliberately damages information          |            |                   |            |        |                              |
| Misuse of resources  |            |                   |            |        |                              |
| Premises break-in  |            |                   |            |        |                              |
| Acts of God, vandals, and terrorists                           |            |                   |            |        |                              |
| Theft or loss of mobile devices                                |            |                   |            |        |                              |
| Theft or loss of non-mobile device                             |            |                   |            |        |                              |
| Theft or loss of paper-based information                       |            |                   |            |        |                              |
| Software failure   |            |                   |            |        |                              |
| Hardware failure   |            |                   |            |        |                              |
| Power failure  |            |                   |            |        |                              |
| Internet/communications failure                                |            |                   |            |        |                              |
| Hacking: brute-force, malicious code, spam, phishing, targeted |            |                   |            |        |                              |
| Denial of Service  |            |                   |            |        |                              |

## 3 Project Capability Rating

|                 | Low, medium or high |
|-----------------|---------------------|
| Confidentiality |                     |
| Integrity       |                     |
| Availability    |                     |

## Service information risk assessment – Capability - UCL

|                             |  |
|-----------------------------|--|
| Service Name:               |  |
| Service Owner:              |  |
| Service Operations Manager: |  |
| Author(s):                  |  |
| Date completed:             |  |
| Date of next review:        |  |
| Scope:                      |  |

### 1 Service Context

How is information stored as part of the service?

How is information processed<sup>1</sup> as part of the service?

How is information transmitted<sup>2</sup> as part of the service?

<sup>1</sup> Includes creation and destruction

<sup>2</sup> Sent and received

## 2 Risk and mitigations

| Risk scenario  | Example(s) | Controls in place | Likelihood | Impact | Proposed additional controls |
|--|------------|-------------------|------------|--------|------------------------------|
| User deliberately or accidentally leaks information            |            |                   |            |        |                              |
| User accidentally or deliberately damages information          |            |                   |            |        |                              |
| Misuse of resources  |            |                   |            |        |                              |
| Premises break-in  |            |                   |            |        |                              |
| Acts of God, vandals, and terrorists                           |            |                   |            |        |                              |
| Theft or loss of mobile devices                                |            |                   |            |        |                              |
| Theft or loss of non-mobile device                             |            |                   |            |        |                              |
| Theft or loss of paper-based information                       |            |                   |            |        |                              |
| Software failure   |            |                   |            |        |                              |
| Hardware failure   |            |                   |            |        |                              |
| Power failure  |            |                   |            |        |                              |
| Internet/communications failure                                |            |                   |            |        |                              |
| Hacking: brute-force, malicious code, spam, phishing, targeted |            |                   |            |        |                              |
| Denial of Service  |            |                   |            |        |                              |

## 3 Service Capability Rating

|                 | Low, medium or high |
|-----------------|---------------------|
| Confidentiality |                     |
| Integrity       |                     |
| Availability    |                     |

## Risk treatment plan – UCL

### Risk Treatment Overview

This document describes how risk treatment is handled; in particular it details the approach to:

- Treating risk
- Formulating Risk Treatment Plans, ensuring that necessary controls have not been omitted and gaining approval for the risk treatment plan and residual risks

### Treating risk

Risk is treated by applying controls that modify the risk in such a way that it meets the specified Risk Acceptance Criteria. This is achieved through controls which either:

- Reduce the likelihood of the risk occurring by attempting to prevent the occurrence of the event, or detect it in sufficient time for the organisation to deal with it or
- Reduce the severity of the risk by reacting to the consequence.

Through the use of controls it is hoped that the likelihood or impact of the event can either be eliminated or reduced greatly. The control may be performed by this organisation or another external organisation. The organisation also needs to consider whether, by employing a particular control to reduce a particular risk for one variety of consequence it is increased for another. Consequently it is important that a wide range of risk treatment options are considered.

### Risk Treatment Plans

#### Determination of controls

Each event is considered to determine:

- Controls which are required to prevent the event
- Controls which are required to detect the event
- Controls which are required to react to the associated consequences of the event

At the conclusion of the process the organisation must be satisfied that the residual risk is acceptable which should be reflected in the Residual Risk Level. Controls can be designed or based on commercially available technology in order to modify risk to an acceptable level.

#### Comparison with Annex A of ISO/IEC 27001:2013

In order to ensure that necessary controls have not been omitted from the Risk Treatment Plan they are compared with the controls in Annex A of the ISO/IEC 27001:2013 standard. Each control within the standard is considered and the following determined:

- Is it applicable to the organisation?
- If applicable does the organisational control exactly correspond to the version in the standard? If it is a variant the Annex A control is deemed as not being applicable and the reason for and explanation of the variant is recorded
- Why it is used? This is explained through a cross-reference to the associated event in the Risk Treatment Plan
- What is the implementation status (Implemented; In Progress or Not Started)

If as a result of this process an Annex A control is determined to be applicable, but isn't already covered the Risk Treatment Plan is revised to include it.

#### Formulating risk treatment plans

The Risk Treatment Plan is sub-divided into sections relating to each risk event. Each section will document:

1. A description of the event;
2. The risks before treatment (with corresponding Risk Rating Graph);
3. The risk treatment detailing:
  - a. Controls to prevent the event
  - b. Controls to detect the event
  - c. Controls which react to the consequences
4. The risks after treatment (with corresponding Risk Rating Graph) with an explanation of why the risk acceptance criteria are met;
5. Risk Owner and acceptance of residual risk

6. Reference to earlier versions of the plan

Calculations of residual risk are based on an appraisal of the likely outcome judged against the criteria documented in the Risk Assessment Process to ensure consistency.

**Risk owner approval**

The Information Security Group will meet with the risk owners to review the risk treatment plan. The risk owners ultimately approve the risk treatment plans. The results are recorded by both the Information Security Group and the risk owners.

# Risk assessment methodology – Cardiff University

## Section

- 1 Introduction
- 2 Risk assessment  
Methodology
- 3 Methodology – Annual Process

### Appendices

Risk Assessment Workshop Reference Documents and Templates:

- A Information Classification
- B Key Information Asset Profile
- C Key Information Asset Environment Map
- D List of Typical Threats
- E Risk Identification and Assessment Worksheet
- F Risk Measurement Criteria
- G Relative Risk Matrix and Risk Acceptance Criteria
- H Risk Register
- I Key Information Assets

## 1 Introduction

- 1.1 In order to ensure consistency, a standard methodology, which can be used across all information security risk assessments is required. The methodology selected for use at Cardiff University is described below.

## 2 Risk Assessment

- 2.1 What is an Information Security Risk Assessment?  
A risk assessment is a process that sets out to establish:
  - The existence of risks to the University's information assets (physical or electronic)
  - The probability that these risks might occur
  - The likely resultant impact of any such risk
  - Any action which could be taken to mitigate the risk either in terms of prevention or reduction of impact should it occur

## 3 Risk Assessment Methodology - Annual Process

- 3.1 The following describe the steps involved in carrying out the risk assessment process and refer to the appropriate reference documents and templates and their location within the appendices.
- 3.2 Each year a risk assessment of key information assets shall be carried out in accordance with section 4.4.2 of the University Information Security Policy.
- 3.3 The process will be initiated by the SIRO and coordinated by the Information Asset Owner for each Key Information Asset (see Appendix I).
- 3.4 The Information Asset Owner will direct Data Stewards to arrange for risk assessments of the systems or containers they manage e.g. SIMS to be carried out. N.B. These should not be carried out in isolation by the Data Steward but should involve suitable representation and input from users and administrators of the system.
- 3.5 Using the Information Classification Document (Appendix A) identify the classifications of information encompassed by the selected asset i.e. C1 Classified - Highly Confidential, C2 Classified - Confidential or NC Non-Classified.
- 3.6 Complete the Key Information Asset Profile (Appendix B).
- 3.7 Complete the Key Information Asset Risk Environment Map (Appendix C).
- 3.8 Consider the threats to the asset using the typical threats document (Appendix D) to assist in this process.
- 3.9 Brainstorm/Discuss the potential risks, ensuring you categorise their impact in terms of – confidentiality, integrity, availability and compliance.
- 3.10 Make a list of the risks to be quantified, take each in turn and using the key information asset template (Appendix E) describe

a worst-case scenario in which the risk would become an issue i.e. how the risk would manifest. Whilst using a worst-case scenario, ensure you remain realistic and minimise the number of variables contributing to the risk, that is to say you should minimise the number of different factors which all have to occur in order to see the risk crystallise as an issue. A risk should be expressed in the terms of cause, event and effect:

**Cause** - As a result of ...

**Event** - There is a risk that ...

**Effect** - Which could ...

- 3.11 Use the Risk Measurement Criteria (Appendix F) to assess the impact of each risk against each impact area i.e. you must develop the scenario to describe the likely severity of impact against each impact area in that scenario. Having done this, total up the impact scores for each of the impact areas to give an overall risk impact score (pay careful attention to the Scoring table on the last page of the risk measurement criteria).
- 3.12 Having assessed the impact of each risk, determine the probability of occurrence. Using the Risk Measurement Criteria which provide definitions of likelihood (Appendix F).
- 3.13 Once an overall impact score and probability have been determined you can plot the risk on the Risk Acceptance Matrix (Appendix G).
- 3.14 Each section of the Matrix has a colour and the colour can be translated into the appropriate risk response action. i.e. a risk with a high likelihood and high impact score would plot onto a red section and would translate as a severe pool 1 risk which must be given immediate attention and priority over all lower rated risks.
- 3.15 Having plotted the risks into the matrix and consequently identified the risk response actions, appropriate risk control (mitigation) actions should be identified, discussed and documented in a risk register (see Appendix H). For each risk there must be one owner who is accountable for the management of that risk. Since one risk may have a number of distinct control actions, the risk owner shall identify who is responsible for ensuring that each control is implemented and managed.
- 3.16 The process will generate a completed: Key Information Asset Profile, Key Information Asset Risk Environment Map, Risk Identification and Assessment Worksheet, a populated Risk Acceptance Matrix and Risk Register.
- 3.17 The Risk register shall be reviewed by the Data Steward and Asset Owner in order to determine the overall level of information risk exposure as well as to agree and sign off asset specific security requirements and priorities for implementation. However all risks which plot as Severe or Substantial should be referred via the Information Asset Owner to the SIRO for referral to the Information Security Risk Group (ISRG) to determine whether the risks should be added to the University Risk Register
- 3.18 N.B. where a risk assessment was carried out the previous year, reference should be made to the relevant paperwork as a primer for the current years risk assessment. However it is not simply enough to review the risks from the previous year as it is possible that new risks may have arisen in the intervening 12 months due to changes in legislation, reporting requirements, technological developments etc.

## Appendix A

INFORMATION CLASSIFICATION V2.0

| Category Title              | Classified C1<br>HIGHLY CONFIDENTIAL  | Classified C2<br>CONFIDENTIAL   | NC<br>Non -Classified  |
|-----------------------------|---|---|--|
| Description                 | <p>Has the potential to cause serious damage or distress to individuals or serious damage to the University's interests if disclosed inappropriately</p> <p><i>Refer to Impact levels of 'high' or 'major' on the Risk Measurement Criteria</i></p> <p>Data contains highly sensitive private information about living individuals and it is possible to identify those individuals <i>e.g. Medical records, serious disciplinary matters</i></p> <p>Non-public data relates to business activity and has potential to seriously affect commercial interests and/or the University's corporate reputation <i>e.g. REF strategy</i></p> <p>Non-public information that facilitates the protection of individuals' personal safety or the protection of critical functions and key assets <i>e.g. access codes for higher risk areas, University network passwords.</i></p> | <p>Has the potential to cause a negative impact on individuals' or the University's interests (but not falling into C1)</p> <p><i>Refer to Impact levels 'Minor' or 'Moderate' on the Risk Measurement Criteria</i></p> <p>Data contains private information about living individuals and it is possible to identify those individuals <i>e.g. individual's salaries, student assessment marks</i></p> <p>Non-public data relates to business activity and has potential to affect financial interests and/or elements of the University's reputation <i>e.g. tender bids prior to award of contract, exam questions prior to use</i></p> <p>Non-public information that facilitates the protection of the University's assets in general <i>e.g. access codes for lower risk areas</i></p> | <p>Information not falling into either of the Classified categories</p> <p><i>e.g. Current courses, Key Information Sets, Annual Report and Financial Statements, Freedom of Information disclosure</i></p>  |
| Type of protection required | <p>Key security requirements:</p> <p>Confidentiality and integrity</p> <p>This information requires significant security measures, strictly controlled and limited access and protection from corruption</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p>   | <p>Key security requirements:</p> <p>Confidentiality and integrity</p> <p>This information requires security measures, controlled and limited access and protection from corruption</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p>  | <p>Key security requirement:</p> <p>Availability</p> <p>This information should be accessible to the University whilst it is required for business purposes</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p> |

### General advice:

Always aim to keep Classified Information (C1 and C2) within the University's secure environment.

Where this is not possible consider whether the information can be redacted or anonymised to remove confidential or highly confidential information, thereby converting it to Non-Classified Information (NC).

Report any potential loss or unauthorised disclosure of Classified Information to the IT Service Desk on 74xxx

Seek advice on secure disposal of equipment containing Classified Information via the IT Service Desk on 74xxx

Use the Confidential Waste Service for disposal of paper and small electronic media xxx@cardiff.ac.uk

## Appendix B

### KEY INFORMATION ASSET PROFILE

| Name of Key Information Asset and sub category                   | Rationale for selection<br><i>Why is this information asset important to the organisation?</i>  | Description<br><i>What is the agreed-upon description of this information asset?</i> |
|--|---|--|
| Information Asset Owner <i>The role/post title of the person</i> |   |  |
| Information Classification                                       | <input type="checkbox"/> Classified - Highly Confidential<br><input type="checkbox"/> Classified - Confidential<br><input type="checkbox"/> Classified - Protect<br><input type="checkbox"/> Non-Classified |  |
| Security requirements  |   |  |
| <input type="checkbox"/> Confidentiality                         | Only authorised staff can view this information asset, as follows:  |  |
| <input type="checkbox"/> Integrity                               | Only authorised staff can modify this information asset, as follows:  |  |
| <input type="checkbox"/> Availability                            | This asset must be available for these staff to do their jobs as follows:   |  |
| <input type="checkbox"/> Compliance                              | This asset has special regulatory compliance protection requirements as follows:  |  |
| Most important security requirement <i>select as relevant</i>    |   |  |
| Confidentiality / Integrity / Availability / Compliance          |   |  |

## Appendix C

### KEY INFORMATION ASSET RISK ENVIRONMENT MAP

NAME OF KEY INFORMATION ASSET & SUB CATEGORY: .....

| Containers   | Tick all that apply | Specific locations | Owner(s) /staff depts |
|--|---------------------|--------------------|-----------------------|
| Internal (University owned)  |                     |                    |                       |
| Filestore: shared drives   |                     |                    | INSRV                 |
| Centrally maintained databases   |                     |                    | INSRV                 |
| Department maintained databases  |                     |                    |                       |
| Filestore: personal network drive  |                     |                    | INSRV                 |
| IT Network   |                     |                    | INSRV                 |
| Lotus Notes email accounts   |                     |                    | INSRV                 |
| CU web pages   |                     |                    |                       |
| PC hard drive  |                     |                    |                       |
| Laptop hard drive  |                     |                    |                       |
| University mobile device (e.g. Blackberry)                               |                     |                    |                       |
| Removable media (e.g. CD, USB stick)                                     |                     |                    |                       |
| Paper filing systems   |                     |                    |                       |
| Internal postal system   |                     |                    |                       |
| Staff  |                     |                    |                       |
| Computer Screens   |                     |                    |                       |
| External   |                     |                    |                       |
| Staff home PC  |                     |                    |                       |
| Staff owned laptop   |                     |                    |                       |
| Staff owned mobile device  |                     |                    |                       |
| Staff owned removable media  |                     |                    |                       |
| Company under University contract  |                     |                    |                       |
| Service provider not under University contract (including private email) |                     |                    |                       |
| Postal/courier service   |                     |                    |                       |
| Staff owned vehicle  |                     |                    |                       |
| Students   |                     |                    |                       |
| Computer Screen  |                     |                    |                       |

## Appendix D

### List of Typical Threats

- Fire
- Water damage – flood or leak
- Destruction of equipment or media
- Dust, corrosion, freezing
- Failure of air-conditioning or water supply system
- Loss of power supply services
- Failure of telecommunication equipment
- Remote spying
- Theft of media, documents or equipment
- Retrieval of recycled or discarded media
- Disclosure
- Tampering with hardware or software
- Equipment failure
- Saturation of the information system
- Breach of information system maintainability
- Unauthorised use of equipment
- Use of counterfeit or copied software
- Corruption of data
- Illegal processing of data
- Error in use
- Abuse of rights
- Forging of rights
- Denial of actions
- Breach of personnel availability

## Appendix E

### Information Security Framework

#### Key Information Asset – Information Asset: Risks

Guidance on using this template:

- Enter your 5 risks in order of priority with 1 being the most significant risk.
- Name the risk
- Provide a description of the risk (how it would occur and why)
- Indicate whether it would affect confidentiality, integrity, availability or compliance if it did occur
- Estimate how likely it is to occur and any controls you know about that are designed to limit or prevent it, views on their effectiveness
- What impact the risk would have on the University if the worst case scenario of this risk did occur. Referring to the Risk Measurement Criteria as a guide, then score each risk against the listed impact areas in the table.

An example risk is shown below (The risk description is fictional)

- 1.
2. Risk Name - Unauthorised staff access to information on XYZ system
3. Risk Description: Staff are able to access and amend records on the system they are not permitted to and can access information beyond that required for them to carry out their role. That access has the potential to cause significant issues with data integrity as users will be able to delete or change records which indicate invoices received. This would also have the effect of undermining the purpose of the system and the confidence that staff have in it and the organisation. It would also impact on supplier confidence in the organisation if invoices were late being paid. This risk could materialise through staff having over privileged access rights to information beyond that required to undertake their role due to permissions not being set correctly or not being amended according to role changes.
4. Confidentiality  Integrity  Availability  Compliance
5. Likelihood (and existing controls): Likelihood is high as there are a great deal of staff role changes and people joining the organisation. Current controls rest with those who administer account access and insufficient resource to administer accounts has been identified meaning there is a significant lag in access changes to XYZ system being requested and their implementation.
6. Impact: See Table

| Impact Area               | Impact Value |                |           |              |          |           | Relative Risk Score |
|---------------------------|--------------|----------------|-----------|--------------|----------|-----------|---------------------|
|                           | No (0)       | Negligible (1) | Minor (2) | Moderate (4) | High (6) | Major (8) |                     |
| Corporate Reputation      |              |                | X         |              |          |           | 2                   |
| Research Profile & Income | X            |                |           |              |          |           | 0                   |
| Student Experience        | X            |                |           |              |          |           | 0                   |
| Financial Sustainability  |              |                | X         |              |          |           | 2                   |
| Health & Safety           | X            |                |           |              |          |           | 0                   |
| Staff Experience          |              |                |           | X            |          |           | 4                   |
| Legal Obligations         |              |                |           |              | X        |           | 6                   |
|                           |              |                |           |              |          |           | 14                  |

#### Risks

Which sources of information, if compromised, would have an adverse impact on the organisation (as defined by the risk measurement criteria) if one or more of the following occurred?

- The asset or assets were disclosed to unauthorised people.
- The asset or assets were modified without authorisation.
- The asset or assets were lost or destroyed.
- Access to the asset or assets was interrupted.
  - Information Asset R1.
  - Risk Name:

- Risk Description:
- Confidentiality  Integrity  Availability  Compliance
- Likelihood (and existing controls):
- Impact: See Table

| Impact Area               | Impact Value |                |           |              |          |           | Relative Risk Score |
|---------------------------|--------------|----------------|-----------|--------------|----------|-----------|---------------------|
|                           | No (0)       | Negligible (1) | Minor (2) | Moderate (4) | High (6) | Major (8) |                     |
| Corporate Reputation      |              |                |           |              |          |           |                     |
| Research Profile & Income |              |                |           |              |          |           |                     |
| Student Experience        |              |                |           |              |          |           |                     |
| Financial Sustainability  |              |                |           |              |          |           |                     |
| Health & Safety           |              |                |           |              |          |           |                     |
| Staff Experience          |              |                |           |              |          |           |                     |
| Legal Obligations         |              |                |           |              |          |           |                     |
|                           |              |                |           |              |          |           |                     |

## Appendix F

### RISK MEASUREMENT CRITERIA (INFORMATION SECURITY FRAMEWORK) V2.0

Definitions: short term: 1 week to 5 months medium term: 6 months to one year long term: in excess of a year

| Risk Area                          | Impact   |  |  |   |   |
|------------------------------------|--|--|--|---|---|
|                                    | Negligible   | Minor  | Moderate   | High  | Major   |
| Corporate Reputation               | <p>Small number of individual correspondence/representations</p> <p>Limited social media pick up, low reach</p>                                | <p>Reputation is minimally affected with little or no targeted effort or expense required to recover;</p> <p>Low key local or regional interest media coverage</p> <p>Mild stakeholder correspondence/representations</p> <p>Negative, short term social media pick up, limited platforms (fewer than 500 followers)</p> | <p>Reputation is damaged in the short to medium term with targeted effort and expense required to recover.</p> <p>Public stakeholder comment and correspondence expressing concern</p> <p>Adverse regional or national interest media coverage</p> <p>Negative social media pick up, more than 500 followers</p> <p>Achievement of KPIs threatened</p> | <p>Significant public and private comment from stakeholders expressing serious concerns</p> <p>Adverse high profile, national media coverage from reputable/influential media, with some international interest</p> <p>Sustained social media criticism, shared across multiple platforms with wide reach</p> | <p>Reputation damaged for the long term or irrevocably destroyed – requiring re-branding</p>  |
| Research Profile & Research Income | <p>Small impact on research activity within specific teams</p> <p>short term/localised effect;</p> <p>negligible impact on research income</p> | <p>Minor impact on research income or productivity for wider group</p> <p>REF outcome remains unaffected</p>   | <p>Noticeable impact on REF profile</p> <p>Medium term effect on productivity within discipline</p> <p>Up to 1% overall reduction in research income due to loss of confidence/lack of compliance</p> <p>Achievement of KPIs threatened</p>  | <p>Significant impact on REF profile</p> <p>Medium to long term effect on productivity in more than one discipline</p> <p>1 to 4% overall reduction in research income due to loss of confidence/lack of compliance</p>   | <p>Major impact on REF profile</p> <p>Long term/pan university effect</p> <p>More than 5% reduction in research income due to loss of confidence/lack of compliance</p> |

RISK MEASUREMENT CRITERIA (INFORMATION SECURITY FRAMEWORK)

Definitions: short term: 1 week to 5 months medium term: 6 months to one year long term: in excess of a year

| Risk Area                | Impact  |   |   |   |   |
|--------------------------|---|---|---|---|---|
|                          | Negligible  | Minor   | Moderate  | High  | Major   |
| Student Experience       | <p>Student satisfaction affected (localised short term effect)</p> <p>little or no targeted effort or expense required to recover</p> <p>Individual student appeals or complaints</p> <p>No impact on student recruitment</p> | <p>Noticeable impact on NSS scores in localised area and some effort and expense required to recover</p> <p>Small increase in student appeals or complaints in specific area</p> <p>Small impact on student recruitment (number of applicants)</p> <p>Small impact on progression rates</p> | <p>Student satisfaction/NSS scores adversely affected across multiple areas and some effort and expense required to recover</p> <p>Increase in appeals across multiple disciplines or group complaints</p> <p>Significant impact on student recruitment (numbers of applicants)</p> <p>Drop in entry standards (but above quality thresholds)</p> <p>Achievement of KPIs threatened</p> | <p>Student satisfaction/NSS scores significantly adversely affected across multiple areas and significant effort and expense required to recover</p> <p>Significant increase in appeals across multiple disciplines or group complaints</p> <p>Significant decrease in progression rates</p> <p>Significant impact on student recruitment requiring drop in intake quality thresholds</p> | <p>Widespread and extreme student dissatisfaction with protests</p> <p>Quality of academic provision seriously jeopardised and long term viability undermined</p> |
| Financial Sustainability | <p>Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of less than £500K</p>  | <p>Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of between £500K-£1M</p>  | <p>Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of between £1M-£2.5M</p>  | <p>Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of between £2.5M-5M</p>   | <p>Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of greater than £5M</p>         |

RISK MEASUREMENT CRITERIA (INFORMATION SECURITY FRAMEWORK)

Definitions: short term: 1 week to 5 months medium term: 6 months to one year long term: in excess of a year

| Risk Area        | Impact   |  |  |   |  |
|------------------|--|--|--|---|--|
|                  | Negligible   | Minor  | Moderate   | High  | Major  |
| Health & Safety  | <p>Minor distress caused to individual</p> <p>environmental damage – small scale, locally contained, short term and reversible (no threat to health)</p> <p>Short term loss of/ access to facilities or specialist equipment</p> | <p>Reportable (RIDDOR) Dangerous Occurrences or Minor Injuries</p> <p>Short term minor stress caused to individual or minor distress caused to group</p> <p>environmental damage – short term, not reversible or with minor local impact on health</p> <p>Medium term loss of/ access to specific facilities or loss of specialist equipment</p> | <p>Reportable (RIDDOR) Major Injuries and incidents affecting individuals</p> <p>Moderate distress or stress caused to individuals or a group</p> <p>Individual cases of life-threatening disease</p> <p>Medium term or locally contained environmental damage with minor to moderate local impact on health</p> <p>Medium term loss of key facilities or individual buildings</p> | <p>Major life changing injuries (e.g. tetraplegia) to individual</p> <p>Major Injury, distress or stress caused to group</p> <p>Spread of life threatening disease</p> <p>Long term environmental damage</p> <p>Hazardous material escape causing external environmental damage and short term effect on public health</p> <p>Long term/ permanent loss of key facilities or individual buildings</p> | <p>Fatalities</p> <p>Hazardous material escape causing irreparable external environmental damage and serious threat to public health</p> <p>Long term/ permanent loss of use of entire sites</p> |
| Staff Experience | <p>Individual staff dissatisfied or morale of small a group minimally affected</p> <p>Small number of individual grievances</p> <p>Short term/ localised effect</p>  | <p>Staff morale of a group affected with some targeted effort required to recover</p>  | <p>Staff morale of a large group damaged with targeted effort and expense required to recover</p> <p>Significant increase in grievances</p> <p>Adverse effect on staff retention and recruitment in affected area</p>  | <p>Significant and widespread damage to staff morale and significant effort and expense required to recover</p> <p>Action short of a strike and threat of wider industrial action</p>   | <p>Widespread and extreme staff dissatisfaction, protests and industrial action</p> <p>Significant adverse effect on staff retention and recruitment</p> <p>Long term/pan University effect</p>  |

## RISK MEASUREMENT CRITERIA (INFORMATION SECURITY FRAMEWORK)

Definitions: short term: 1 week to 5 months medium term: 6 months to one year long term: in excess of a year

| Risk Area         | Impact  |   |   |  |   |
|-------------------|---|---|---|--|---|
|                   | Negligible  | Minor   | Moderate  | High   | Major   |
| Legal obligations | <p>Technical breaches which may result in complaints to the University but complainant does not resort to legal action or regulatory referral</p> <p>Breach results in minimal or no damage or loss</p> | <p>Fines or claims brought of less than £50K</p> <p>Case referred by complainant to regulatory authorities who may request information or records as a result</p> <p>Regulatory action unlikely or of only localised effect.</p> <p>Advisory/ improvement notices</p> | <p>Fines or claims brought of between £50K-£250K</p> <p>Case referred by complainant to regulatory authorities and potential for regulatory action with more than localised effect</p> <p>Enforcement action notices.</p> | <p>Fines or claims brought of more than £250K</p> <p>University required to report serious matter to regulators</p> <p>Formal external regulatory investigation into organisational practices with potential for suspension of significant elements of University operations</p> | <p>Formal external regulatory investigation involving high profile criminal allegations against management and threat of imprisonment</p> <p>Withdrawal of status or imposition of sanctions resulting in forced termination of mission critical activities</p> |

### Scoring and Weighting

| Risk Area                          | Impact    |            |       |          |      |       |
|------------------------------------|-----------|------------|-------|----------|------|-------|
|                                    | No impact | Negligible | Minor | Moderate | High | Major |
| Corporate Reputation               | 0         | 1          | 2     | 4        | 6    | 8     |
| Research Profile & Research Income | 0         | 1          | 2     | 4        | 6    | 8     |
| Student Experience                 | 0         | 1          | 2     | 4        | 6    | 8     |
| Financial Sustainability           | 0         | 1          | 2     | 4        | 6    | 8     |
| Health & Safety                    | 0         | 1          | 2     | 4        | 6    | 8     |
| Staff Experience                   | 0         | 1          | 2     | 4        | 6    | 8     |
| Legal obligations                  | 0         | 1          | 2     | 4        | 6    | 8     |

### Likelihood Definitions

| Classification | Low   | Medium  | High   |
|----------------|---|---|--|
| Likelihood     | Unlikely  | Possible  | Likely   |
| Description    | <p>0% - 20% chance of occurrence in the next 5 years.</p> <p>Slight chance of occurrence.</p> <p>Has not occurred before, but may occur in exceptional circumstances</p> <p>Not dependent on external factors</p> | <p>21 – 50% chance of occurrence in the next 5 years.</p> <p>Moderate possibility of occurrence</p> <p>History of similar occurrences, situations or near misses.</p> <p>Could be difficult to control due to external factors.</p> | <p>At least a 50% chance of occurrence in the next 5 years.</p> <p>Strong possibility of occurrence</p> <p>History of previous occurrence.</p> <p>Very difficult to control due to significant external factors.</p> |

## Appendix G

RISK ACCEPTANCE V1.0

RELATIVE RISK MATRIX

|            |                           |     |      |       |       |       |
|------------|---------------------------|-----|------|-------|-------|-------|
| High       | > 50%                     |     |      |       |       |       |
| Medium     | 21 - 50%                  |     |      |       |       |       |
| Low        | < 20%                     |     |      |       |       |       |
| Likelihood |                           |     |      |       |       |       |
|            | Impact score (cumulative) | 1-7 | 8-19 | 20-31 | 32-44 | 45-56 |

RISK ACCEPTANCE CRITERIA

|              | Description | Setting Risk Management Priorities                                   | Project based risk assessment   |
|--------------|-------------|--|---|
| Pool 1 Risks | Severe      | Immediate priority to be addressed or suspend/close activity         | Planned project should not proceed without mitigation.  |
| Pool 2 Risks | Substantial | Next priority to be addressed after pool1 risks are mitigated        | Requires very careful on-going management with frequent, regular evaluation of the risk factors.                                    |
| Pool 3 Risks | Moderate    | Next priority to be addressed after pool 1 and 2 risks are mitigated | May be acceptable for major projects but not normally acceptable in the context of individual staff activities or student projects. |
| Pool 4 Risks | Tolerable   | No active mitigation currently required                              | Lowest and preferred level of risk. Re-assessment or risk factors conducted at regular intervals.                                   |

## Appendix H

Risk Register

| Risk ID | Date Identified | Risk Description  | Likelihood            | Impact | Risk Rating                                    | Control Measure (mitigation) | Control Owner  | Target Risk Rating              | Target Date | Risk Owner   |
|---------|-----------------|---|-----------------------|--------|--|------------------------------|--|---------------------------------|-------------|--|
| 1.0     | 01/01/2013      | Risk expressed in the terms: As a result of...<br>There is a risk that...<br>Which may... | Low<br>Medium<br>High | 1 - 56 | Severe<br>Substantial<br>Moderate<br>Tolerable |                              | Is responsible (name and role) for actioning the mitigation action | Medium<br>x 31 =<br>Substantial | 01/01/2014  | Is accountable (name and role) for ensuring the risk is effectively managed. |
|         |                 |   |                       |        |  |                              |  |                                 |             |  |
|         |                 |   |                       |        |  |                              |  |                                 |             |  |
|         |                 |   |                       |        |  |                              |  |                                 |             |  |
|         |                 |   |                       |        |  |                              |  |                                 |             |  |
|         |                 |   |                       |        |  |                              |  |                                 |             |  |
|         |                 |   |                       |        |  |                              |  |                                 |             |  |

## Appendix I

### KEY INFORMATION ASSETS

#### Research information:

- Data collected for/used in analysis
- Research management info
- Research outputs
- Intellectual property

#### Financial information:

- External expenditure
- Income received
- Internal allocation
- Financial forecasting
- Assets & liabilities

#### Estates information:

- Inventory of buildings & rooms
- Consumption
- Usage (including hazardous materials)
- Maintenance
- Access control systems

#### Student & Applicant information:

- Academic record
- Administrative Info
- Pastoral support

#### Student Recruitment information:

- Marketing strategy & materials
- Open day and outreach event information
- International Foundation programme student information

#### Education information:

- Taught course delivery
- Assessment delivery
- Educational resources
- Timetabling

#### Staff information:

- Management of employment
- Training & development
- Welfare & health

#### Other business critical information:

- External engagement/ Fundraising/Alumni
- Policy & committee records
- Library catalogue and borrowing records
- Student Residences management Information

## Information asset register tool – University of Oxford

A pragmatic approach, deploying a quick and easy-to-use tool, has been used to identify information assets that are extremely important for the business of the University (crown jewel assets) and are at the same time potentially vulnerable. The tool is designed to be used by departments, faculties, colleges and institutes. 'Assets' in this context include lists or documents or tables or spreadsheets holding information which has value (either electronically or in filing cabinets).

This Information Asset Register tool enables: identification and recording of crown jewel assets; assigning those accountable for the assets; and performing a risk assessment against the identified assets. It enables a university to focus its mitigation efforts on the most important areas.

The tool has been used by Oxford and also by universities across the world. A significant level of consistency is beginning to emerge in terms of identification of specific types of crown jewel assets that are considered to be vulnerable and require mitigation.

Further details of the Information Asset Register tool are given at: <http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/information-asset-management#d.en.158803>; the tool can be downloaded from the same web page. It is intended to develop the tool, please send proposals for improvement to the email address given.



# Resources for Chapter 6 – Controls

## RESOURCES

- [Evaluating software security patches – Loughborough University, case study](#)
- [Hacking before and after: How Certified Ethical Hacking \(CEH\) training changed my perspective on hacking – UCL, case study](#)
- [Technical vulnerability management](#)
- [Penetration testing](#)

## Evaluating software security patches – Loughborough University, case study

This case study describes the steps that Loughborough University took to mitigate risk when the Heartbleed OpenSSL vulnerability was disclosed.

### Patch Management

Different teams within IT Services at Loughborough University take different approaches to how they manage patching of their services:

- Systems Team who predominantly manage Microsoft Windows Server environments have a cycle where patches are firstly deployed to non-critical systems within a test environment, secondly to critical systems within a test environment. This rollout cycle is then mirrored on production systems.
- Desktop Management Team use SCCM to manage patching on desktop systems. Their approach is to package security patches and updates within SCCM, deploy to a test machine to complete a full Q and A. Once this has been tested, patches will be deployed to IT Services managed machines and then out to the wider University one school at a time.
- Networks Infrastructure Team manages a large estate of Linux servers. As there is no scheduled release of Linux patches, systems use a list to inform administrators of outstanding patches. These are firstly tested within a test environment before being applied to production servers.

When out-of-band patches or patches to prevent zero day attacks are released, IT Security contacts within the department are called upon to evaluate the risk of a potential exploit depending on the systems which are vulnerable and the data stored on these systems.

Depending on the calculated risk, the security team will advise others within the University on how to mitigate this risk. The end goal will be to patch systems, but this is not always possible due to time of release etc.

The security team will also look to leverage border protection systems such as firewalls and IPS/IDS.

Evaluating and patching Heartbleed OpenSSL Vulnerability

On 7 April 2014, Heartbleed OpenSSL vulnerability was unleashed onto the Internet. The security team became aware of this via various sources, which are followed such as Twitter feeds, security blogs etc.

### Step 1 – Evaluate and identify

The first step in this process was to try and evaluate the vulnerability and the impact it would have on information systems.

Heartbleed was a vulnerability in OpenSSL, a popular cryptographic library which is used to secure communication across the Internet such as:

- Encrypting HTTPS traffic
- Encrypting emails and Instant messaging services
- VPN encryption

Its most popular use is with Apache web server software, which predominantly runs on Linux server to create HTTPS secure sites. Heartbleed exploits a SSL heartbeat process, in that once a secure connection has been established, periodic pings are sent to keep the encrypted tunnel alive. Specially crafting this ping packet makes the server return 64kb of data from its memory, this could include usernames, passwords, private keys etc. By sending this malicious ping packet multiple times, an attacker is able to rebuild the servers memory contents.

This vulnerability didn't just impact web services; appliances were also vulnerable such as:

- Routers / Switches
- Firewalls
- IPS/IDS
- Load balancers

Due to the nature of this vulnerability, SSL certificates were also deemed as being compromised. This meant that all SSL certificates on vulnerable services would need to be revoked and new certificates issues.

Internally this vulnerability was classified as critical due to the potential level of information disclosure that was possible. Luckily this vulnerability had been disclosed responsibly and patches were already available including a work around. Vendors such as Cisco, Juniper, F5, Palo Alto Networks were also releasing fixes for appliances.

Once the vulnerability was evaluated, the next step was to try and identify vulnerable hosts on the network. Simply getting back the version of OpenSSL would have identified if it software was vulnerable, but we could only do this on servers within our control.

The security team opted to use a script, which had been developed for NMAP, and were very quickly able to identify which hosts on the

network were vulnerable to this exploit.

## **Step 2 - Communication**

From the scan of the network, as expected not all vulnerable hosts and or services were under the control of the department. Other schools and departments around the University were also hosting services.

Internal mailing lists are used to communicate vulnerabilities and releases of patches to the wider IT community within Loughborough University.

As this was more a Linux issue, it was decided to post information to the unix security mailing list. Information about the vulnerability, links to additional information and assistance from IT Services was communicated to IT Support staff across the University.

## **Step 3 - Patching**

At this point, the security team had already configured the IPS/IDS to block any attempts at exploiting the Heartbleed vulnerability externally. This helped remove the external attack vector. The risk remained high due to possible attacks from within the network.

Individual teams patching procedures had already begun within the department, once emergency change requests were approved and testing was complete; the fix was being rolled out onto production services.

Access to management interfaces on appliances followed best practice in that this traffic is completely separate to other business critical traffic and access to this network is heavily restricted to privileged personnel. Due to this, management interfaces were less of an issue and once vendors released updates to resolve the Heartbleed vulnerability, these were scheduled and deployed accordingly.

## **Step 4 – Follow up**

The security team continued to regularly scan the entire network for Heartbleed vulnerabilities. Where services were found to still be vulnerable, service managers were contacted to ensure patches were scheduled to be implemented.

Follow up communications was posted to the internal mailing lists informing server managers that Janet was offering free replacement for SSL certificates. Help was also offered to managers wanting their services scanned to ensure fixes had worked.

## Hacking before and after: How Certified Ethical Hacking (CEH) training changed my perspective on hacking – UCL, case study

Austin Chamberlain, ISG UCL

I have been a sysadmin for almost all of my working career. I have a degree in computer science; I worked as a programmer for a year before moving on to system administration, and have worked as a sysadmin for 14 of the last 16 years.

### Being a Sysadmin

From a sysadmin perspective, security and hacking are viewed in a defensive or preemptive way. Best practice is to set up servers with strong passwords, regularly patch the servers, and work on the principle of least privilege and privilege separation. These measures are usually passive – once in place, it becomes standard working practice and doesn't require major thought to implement.

In the environments in which I have worked, password security has generally been good. Strong passwords are in use (varyingly) and storage of passwords has been good. Over time storage has improved greatly, with the adoption of tools like KeePass and Lastpass.

Regular patching is usually a work in progress. The structure is simple enough to set up, with WSUS for Windows servers and Satellite for RedHat servers. Even on systems where update processes require more sysadmin intervention, this can be automated with cron scripts or similar.

A frequent problem is older, unmaintained servers – as services are upgraded and servers are replaced, older servers remain in service to host a specific legacy application or code. Sometimes these services are business-critical, but resources are not available to upgrade and migrate the application to a newer system – or the people who wrote and understand the application have left, leaving a key application unsupported and stuck on a legacy server.

Least privilege and privilege separation are key concepts which should be emphasised. In my experience this is generally well handled, since it is mostly under the control of the sysadmin alone. If included as a routine design principle it becomes a habit for sysadmins without being onerous. I have on occasion been surprised where it hasn't been done – where a small amount of effort at the design stage could result in a large increase in overall system security.

### Being a hacker is easy

As a sysadmin, I always thought of hacking as slightly esoteric and requiring specialist skills and tools. This is not, in fact, the case. Many of the techniques used are simple and obvious to a sufficiently evil-minded sysadmin. Some of them are relatively common as diagnostic techniques, and I have used some for years. Hacking involves pointing these techniques at systems you don't own. For example, I frequently confirm connectivity between two servers by testing ports with telnet; I'll use banner-grabbing to determine what is listening on a given port. Both of these are techniques used by hackers to get more information about a system to determine which exploits will work.

Hacking tools themselves cover a wide range; at one end there are simple tools which are easily available, or installed by default on many systems. Chaining these simple tools together can be used to compromise a server quite easily. This requires some technical knowledge as many of the tools rely on command-line usage, and usually shell access is the result. The main example of this is netcat, which combined with a vulnerability that allows remote code execution, can be used to establish a remote console connection.

At the other end of the range are the complex tools, which are sadly just as easily available. These don't even require the technical knowledge needed for simpler tools; generally a GUI provides all of the options. Some are perfectly legitimate security scanning/testing tools; nmap and Nessus are good examples, since these will only provide information. Tools like Cain&Abel are slightly more suspect; although there are legitimate uses for this, cracking passwords does not come up that often. Metasploit is the black hat tool of choice; this performs the full spectrum of hacking techniques with a few clicks, ranging from system/service discovery, to compromise, to post-compromise exploitation (shell/desktop access, file transfer, keylogging, screen capture).

### Ethical hacking is harder

It is harder to hack in an ethical and systematic way, to produce a useful report on the vulnerability of a given server with the end goal of improving security. Black hat hackers of whatever kind - script kiddies, criminals, foreign government agents - are unlikely to care about the stability of a system unless they are trying to hide their tracks ... and a complete wipe of the system will hide tracks quite effectively.

For this reason ethical hacking combines the diligence of the sysadmin with the creativity and lateral thinking of a hacker. This is not a particularly difficult or rare combination, but it does require a step-by-step procedure of experimental testing, and it takes time to develop both the mindset and the process.

Overall, then, hacking is a growing threat which is becoming more accessible to unskilled users. Protecting against it is strengthened by good procedures, which if they become habit will make any organisation reasonably secure. This can be supplemented and improved by security guidance and penetration testing - but only ever supplemented. A poor base security cannot be improved much after the fact!

## Changing Perspectives

- Good practice is vital, and if enforced by policy and inculcated by training, can become habit.
- Patching – automate. Make it routine. Enforce by policy. Do whatever needs to be done to make this happen regularly and frequently.
- Password strength and least privilege design don't require much effort, and greatly increase security.

Hacking is easy and automated. Tools are free and widely available. It's not a matter of if you'll be attacked, it's a matter of how much you're being attacked right now!

## Technical vulnerability management

### Vulnerability Management

#### Key Points

- Reduce the risks organisations face resulting from exploitation of technical vulnerabilities.
- Allow organisations to setup a vulnerability scanning framework.
- Assist organisations in developing a patch management policy.
- Support organisations in procuring penetration testing services.

#### Introduction

A vulnerability is defined in ISO/IEC 27000 as “A *weakness of an asset or a group of assets that can be exploited by one or more threats*”.

Vulnerability management is the process in which vulnerabilities in Information Systems are identified and the risks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or a formal risk acceptance by the management of the organisation.

Vulnerability management provides visibility into the risks of assets deployed on the network.

#### Why we need vulnerability management

A vulnerability management process should be part of an organisation’s effort to control information security risks. This process will allow an organisation to obtain a continuous overview of vulnerabilities in their IT environment and the risks associated with them. Only by identifying and mitigating vulnerabilities in the IT environment can an organisation prevent attackers from penetrating their networks and obtaining information

#### Vulnerability scanners and their risks

As vulnerability management is the process surrounding vulnerability identification, it is important to understand how vulnerability scans are performed and what tools are available. Today, the level of technical expertise required to operate a vulnerability scanning tool is low.

There are risks involved with vulnerability scanning. Since vulnerability scanning typically involves sending a large number of packets to systems, they might sometimes trigger unusual effects such as, for example, disrupting network equipment. In order to cover these risks, it is always important to inform stakeholders within the organisation when vulnerability scanning is taking place.

#### Roles and Responsibilities

When building a vulnerability management process, the following roles should be considered within the organisation:

- **Security Officer:** The security officer is the owner of the Vulnerability Management process. This person designs the process and ensures it is implemented as designed.
- **IT Security Engineer:** The IT Security Engineer is responsible for configuring the vulnerability scanner and scheduling the various scans.
- **Service Manager:** The Service Manager is responsible for the Information system being vulnerability scanned and the information stored on the system. This role should decide whether identified vulnerabilities are mitigated or their associated risks accepted.
- **IT Systems Engineer:** The IT Systems Engineer role is typically responsible for implementing remediating actions defined as a result of detected vulnerabilities. In most cases, this is likely to be multiple Systems Engineers which could also be spread over multiple teams or departments.

In many organisations the role of the Security Officer and Security Engineer is one.

#### Vulnerability Management Process

When developing a vulnerability management process, the following phases should be considered:

1. Planning and preparation;
2. Vulnerability Scan;
3. Remediation actions;
4. Rescan.

#### Planning and Preparation

The first phase in the vulnerability management process is preparation. Initial scans should start with a small scope to prevent being

overwhelmed with hundreds of vulnerabilities. It is important to obtain agreement on which systems/services should be included and excluded from the Vulnerability Management Process.

The first step in this process is defining a scope. The following information should form part of the scope:

- Proposed vulnerability scan date;
- Whether the vulnerability scan is going to be an internal scan or an external scan. An internal scan would be conducted as an authenticated network users, where as an external scan would be conducted from outside of the firewall;
- Whether the scan is going to be an authenticated or unauthenticated. An authenticated scan would be where credentials are provided to login to the application or operating system, whereas an unauthenticated scan would test the authentication process;
- Is this an infrastructure scan or applications scan. An infrastructure scan would check the network footprint of the host or service being tested whereas an application scan would focus on the specified application.

Depending on where the organisation sees the risk will influence the scope; for example some organisations see external threats as the biggest risk and would therefore prioritise Internet facing services.

Once the scope has been defined, this should be distributed to Service Managers. It is very important to get buy-in from service managers and provide them with plenty of notice about upcoming vulnerability scans. It is the responsibility of the Service Manager to liaise with stakeholders to inform them about upcoming vulnerability scans. Depending on the criticality of the system, service managers may have requirement for example not to scan systems during the clearing process.

Plan for unexpected events which might lead to delaying a vulnerability scan depending on the nature of the event. Allow service managers to propose another suitable scan date.

If services are deemed too risky for vulnerabilities scans; this risk needs to be highlighted and the risk accepted by the appropriate senior management. Additional protection will need to be implemented such as ACLs and no external access to mitigate against internal and external threats.

## Vulnerability Scan

Once the preparation is complete, the next phase is the initial vulnerability scans are performed. Any issues, which occur during the initial, scans such as systems becoming unavailable or poor application response should be recorded since this may happen on future scans. In this case actions may be defined to reduce the impact of future scans on the stability or performance of target systems.

Vulnerability scanning tools offer a wide range of reporting options to visualize the results. It is necessary to utilize these to create reports depending on the audience:

- **Security Officer/Engineer** Interested in the risk the organisation is currently facing, this risk includes the number of vulnerabilities identified and the severity/risk ratings of the identified vulnerabilities.
- **Asset Owner** Overview of the vulnerabilities in the systems they are responsible for.
- **Systems Engineer** Technical information about the vulnerabilities identified as well as recommendations for mitigation and improvement.

## Remediation actions

In this phase, the Service Manager will work with the Security Officer/Engineer to define remediating actions. The Security Officer/Engineer will analyse the reported vulnerabilities and work with Systems Engineers to determine the associated risk and provide input on risk remediation. The risk will depend on factors such as CVSS (Common Vulnerability Scoring System) score for the vulnerability, publicity of the vulnerability, the Security Officer/Engineers personal experience and the classification of information stored on the system.

## Vulnerability remediation matrix

| Information Classification | Critical Vulnerability | High risk vulnerability | Medium risk vulnerability | Low risk vulnerability |
|----------------------------|------------------------|-------------------------|---------------------------|------------------------|
| Highly confidential        | Remediate              | Remediate               | Remediate                 | Remediate              |
| Confidential               | Remediate              | Remediate               | Remediate                 | Recommended            |
| Not classified             | Remediate              | Remediate               | Recommended               | Recommended            |

Depending on the risk, clear timelines should be provided on when remediating actions should be implemented. Sufficient time should be allowed taking into account the technical nature of the remediation and the organisations change management policies.

If remediation is not possible, this risk should be acknowledged and senior management should made aware. This risk should be documented and accepted via the organisation's risk acceptance process. Compensating controls should be identified in order to mitigate/remove the risk without correcting the vulnerability.

## Rescan

Once vulnerabilities have been remediated, a scan should be scheduled to verify the remediating actions have been implemented. The rescan should be carried out using the same vulnerability scanner, configuration and policy. The same reports should be generated as those created during the initial vulnerability scan.

The next set is for the Service Manager and the Security Office to define a schedule on how often a vulnerability scan should be carried out against systems. In order to establish a robust vulnerability management process, it is recommended scheduled scans should be conducted weekly or monthly. This will ensure rapid vulnerability detection allowing the organisation to implement mitigation controls in a timely fashion and reducing the risk.

## Patching

### Introduction

Patch management is a security best practice designed to proactively prevent the exploitation of known vulnerabilities in information systems within the organisation. The result is to reduce the time and money spent dealing with vulnerabilities and the exploitation of these vulnerabilities. Proactively managing vulnerabilities within information systems will reduce or mitigate the potential for exploitation therefore reducing staff effort in responding after exploitation has occurred.

Patches are additional pieces of code developed to address problems in software. Patches can enable additional features or address security flaws within software. Vulnerabilities are flaws that can be exploited by a malicious entity to gain greater access or privileges. Not all vulnerabilities have patches available; therefore systems administrators must also be aware of other methods of mitigation.

Timely patching of security issues is critical to maintaining the operational availability, confidentiality and integrity of information systems.

### Key Principles

New patches are released daily and it is becoming very difficult to keep abreast of all the new patches and ensuring proper deployment in a timely manner. The following high-level key principles can be used to help mitigate the risk of such exploitation.

- The organisation should have a patch management policy, which should be able to identify which patches need to be/have been applied;
- Only software needed to deliver the organisation's business should be installed. This would reduce the number of patches which need to be applied;
- Only the latest stable releases of software should be used;
- The sources of patches should be confirmed and should be evaluated before being applied to the live environment;
- Patches should be deployed as soon as possible to reduce the exposure times to known vulnerabilities;
- A good update and patch process should be encouraged to make it difficult for potential attacks to be successful.

### Types of Patches

The organisation should ensure the following information technology infrastructure is covered by the patch management policy:

| Type                                   | Patch                                   |
|--|---|
| Computers/Servers                      | BIOS, firmware, drivers, hypervisors    |
| Operating Systems                      | Patches, service packs, feature packs   |
| Application Software (databases)       | Patches, service packs, feature packs   |
| Installed Applications (Java, Adobe)   | Patches, service packs                  |
| Routers and Switches                   | Firmware                                |
| Firewall, IPS/IDS and URL Filtering    | Firmware, definition updates            |
| Anti-virus and Anti-spyware            | Data files and virus definition updates |
| Printers and Scanners                  | Firmware and drivers                    |
| Bespoke or in-house developed software | Patches, service packs, feature packs   |

## Penetration testing

### Introduction

The purpose of performing a penetration test is to verify the new and existing applications, networks and systems are not vulnerable to security risks which could lead to unauthorised access to sensitive information. A penetration test is also PCI DSS requirement 11.3.

A penetration test should be considered after a vulnerability scan has been completed and any issues identified are resolved or mitigated. A penetration test would identify vulnerabilities, which are unknown or have been missed by the scan. Depending on results it may also highlight where a Vulnerability Management process might be failing.

### What is and isn't a penetration test

A penetration test is an authorized, scheduled and systematic process of using known vulnerabilities in an attempt to perform an intrusion into a host, network or application resource. It usually involves the use of automated and manual tools to test resources.

A penetration test is not an uncoordinated attempt to access an unauthorized resource.

### Penetration Testing Types

There are two types of penetration test, which can be conducted, black box and white box testing.

- **Black Box** – This form of testing requires no previous information and usually takes the approach of an uninformed attacker. The penetration tester has no previous knowledge about the target system, network or application.
- **White Box** – This form of testing provides information to the penetration tester about aspects of the system or application they are testing. This could be usernames and passwords to access the system, information on how the application is built such as database access etc.

### Internal or External Penetration Testing

The threat the organisation is trying to replicate should factor into the decision on how the tests should be conducted. External testing is intended to identify vulnerabilities against hosts and or services, which are accessible via the Internet. Internal testing is intended to identify vulnerabilities with physical access, exposure to social engineering and vulnerabilities to systems, which are accessed via an authorised network connection.

### Penetration Testing Scope

Along with the type of testing to conduct, organisations need to decide what they wish to test against, whether it be network testing or a specific application. Other considerations should be whether the testing is conducted internally or externally.

- **Network Penetration Testing** – This will test all services, which are offered by the organisation via the Internet. These include email, DNS, firewall effectiveness and web services. This type of test would also indicate vulnerable software and firewall misconfigurations.
- **Application Penetration Testing** – This type of test could be conducted either internally or externally depending on its availability and testing would be limited to the specified application. An example might be a web application.
- **Social Engineering Penetration Testing** – This type of test focuses on identifying and verifying vulnerabilities associated with employee's ability to understand documented policies and follow procedures and security best practices.

### Consideration for using third parties

If the organisation has decided to use a third party to conduct the penetration tests, some effort should be made to confirm the qualification of the company. What are the qualification of the employees and their backgrounds and reference sites. The following penetration testing qualification might be useful to look for when selecting a partner to work with:

- CHECK certified
- Tiger Scheme certified
- CEH (Certified Ethical Hacker) certification

When provisioning a penetration test using an external testing company, ensure a detailed scope of work has been provided and that it meets all of the organisation's testing needs. The following information should form the scope of work:

- What is going to be tested (infrastructure or application test and whether this is an internal or external test) and the type of test (black or white box).
- When is the tests going to be conducted
- Who is the lead contact at the organisation and contact details
- Who is the lead tester and contact details

- Details of any other testers and contact details.

The lead tester and a senior member at the organisation who is authorized to allow the testing to commence should sign the scope of work.

### **After Penetration Testing**

Once the testing is complete, the organisation should request a report, which documents all the vulnerabilities, which were identified by the penetration testing team. This report should also provide remediation advice on how to resolve issues identified.

The report should be held in the strictest of confidence as the report could hold information that would reduce the overall security of the organisation. The organisation should act upon the issues identified as part of a penetration test, this might be implementing remediation steps or accepting the risks and implementing mitigating controls to reduce the identified risk.

# Resources for Chapter 7 – Information management

## RESOURCES

- [Information Classification Scheme – University of York](#)
- [Development of an Information Classification and Handling Policy – Cardiff University, case study](#)
- [Information Classification and Handling Policy – Cardiff University](#)
- [University Guidance on Classification of Information – University of Oxford](#)

## Information Classification Scheme – University of York

An information classification scheme for University information is being introduced to:

- protect information from accidental or deliberate compromise, which may lead to damage, and/or be a criminal offence
- help to meet legal, ethical and statutory obligations
- protect the interests of all those who have dealings with the University and about whom it may hold information (including its staff, students, alumni, funders, collaborators, business partners, supporters etc.)
- promote good practice in relation to information handling.

The classification scheme encompasses all data held by the University, in any format (electronic and hard-copy).

| Level        | Rationale  | Examples  |
|--------------|--|---|
| Public       | This is information which does not require protection and is considered 'open' or 'unclassified' and which may be seen by anyone whether directly linked with the University or not.   | Prospectus, programme and course information<br>Press releases (not under embargo)<br>Open content on the University web site<br>Fliers and publicity leaflets<br>Published information released under the Freedom of Information Act |
| Restricted   | Non-confidential information where dissemination is restricted in some way eg to members of the University, partners, suppliers or affiliates<br><br>Access to this information enhances University operations by facilitating communication and collaboration between staff, students and external partners, but access is restricted and governed by appropriate policies or contracts   | Some committee minutes<br>Departmental intranets<br>University timetable<br>On-line directory of contact details<br>Teaching materials<br>Procurement documents   |
| Confidential | Information which is sensitive in some way because it might be personal data, commercially sensitive or legally privileged, or under embargo before being released at a particular time.<br><br>It also includes information in a form that could not be disclosed under Freedom of Information legislation.<br><br>Covers data about an individual, and data about the institution.<br><br>This information, if compromised, could: <ul style="list-style-type: none"> <li>• cause damage or distress to individuals</li> <li>• breach undertakings to maintain the confidence of information provided by third parties</li> <li>• breach statutory restrictions on the use or disclosure of information or lead to a fine, e.g. for a breach of the Data Protection Act or Competition Law</li> <li>• breach contractual agreements</li> <li>• breach a duty of confidentiality or care</li> <li>• cause financial loss or loss of earning potential to the University</li> <li>• disadvantage the University in commercial or policy negotiations with others</li> <li>• prejudice the investigation or facilitate the commission of crime</li> <li>• undermine the proper management of the University and its operations</li> </ul> | Student personal details<br>Staff personal details<br>Press releases<br>Financial transactions<br>Internal reports<br>Commercial contracts<br>Research data   |

Information may also be marked with a descriptor, which identifies the reason why the classification is applied. The expiry date for the current level may also be given. For example:

- Confidential - personal
- Confidential - commercially sensitive
- Confidential - exams - expires 1 July 2013 and becomes public

Qualifying descriptors may also be used to incorporate/map to protective markings from other classification schemes, where staff are working with external partners, data and schemes (e.g. the Government Protective Marking Scheme). For example: Confidential - GPMS  
Secret

| Class      | Description   | Storage  | Dissemination and access  | Exchange and collaboration  | Disposal   |
|------------|---|--|---|---|--|
| Public     | University information that can be seen by anyone.  | Electronic information should be stored using UoY provided IT facilities to ensure appropriate management, back-up and access. | Information can be shared via the web without requiring a UoY username.<br><br>Electronic and hard copy information can be circulated freely subject to applicable laws e.g. copyright, contract, competition<br><br>May be accessed remotely and via portable and mobile devices without encryption.   | Information can be exchanged via email or file sharing without needing encryption.  | Electronic information should be deleted using normal file deletion processes in accordance with any retention schedule.<br><br>Printed copy should be disposed of via the University paper recycling scheme and in accordance with any retention schedule.  |
| Restricted | Non-confidential information where dissemination is restricted in some way e.g. information restricted to members of the University, a committee, project or partnership. | Electronic and paper-based Information must be stored using UoY provided facilities.   | Information can be shared via the web but the user must provide UoY authentication.<br><br>Electronic and hard copy information can be circulated on a need-to-know basis to University members subject to applicable laws (e.g. copyright) and University Regulations<br><br>May be accessed remotely and via disk-encrypted portable and mobile devices without further encryption. | Information can be sent in unencrypted format via email.<br><br>Information can be shared using UoY IT facilities e.g. wiki, shared filestore.<br><br>Information can be printed and circulated via the University internal mail service. | Electronic equipment holding this information must be disposed of using the University secure IT waste disposal service and in accordance with any retention schedule.<br><br>Printed copy should be disposed of via the University confidential waste scheme and in accordance with any retention schedule. |

| Class        | Description   | Storage  | Dissemination and access  | Exchange and collaboration   | Disposal  |
|--------------|---|--|---|--|---|
| Confidential | <p>Information which is sensitive in some way because it may be personal data, commercial or legal information, or be under embargo prior to wider release.</p> <p>Includes data about individuals, and data about the institution.</p> <p>May also include data provided to the University by other organisations e.g. research datasets</p> | <p>Information must be stored using UoY IT facilities. Portable devices must have full disk encryption.</p> <p>Unencrypted removable media (e.g. USB sticks) must not be used.</p> <p>Encrypted removable media are not permitted without undertaking evaluation of other options.</p> | <p>Access to confidential data must be strictly controlled by the Data Owner who should conduct regular access reviews.</p> <p>Some types of confidential information may be shared with authorised users via UoY IT facilities, including remote access, subject to UoY authentication. For web access encryption must be used.</p> <p>Confidential data must not be extracted from University IT systems and stored on local IT systems.</p> <p>If a portable device (e.g. a laptop, tablet or phone) is used to access University confidential information, the device must be encrypted and require a password or PIN to access</p> | <p>The method to be used for exchanging confidential information must take account of the nature and volume of the data to be exchanged so that the impact of inappropriate disclosure can be assessed and an appropriate method selected.</p> <p>Confidential data must be encrypted prior to exchange.</p> <p>Exchange must be conducted using UoY provided facilities.</p> <p>Duplicate copies of confidential information must be avoided.</p> <p>Where copies are necessary the protective marking must be carried with the data. Where paper copies are required for circulation or sharing, secure delivery methods must be used.</p> <p>Paper and electronic copies must be marked 'Confidential' and the intended recipients clearly indicated. An optional descriptor, to state the reason for confidentiality, may be used.</p> | <p>Electronic equipment holding this information must be disposed of using the University secure IT waste disposal service and in accordance with any retention schedule.</p> <p>Printed copy should be disposed of in accordance with any retention schedule via the University confidential waste scheme or departmental shredding facilities.</p> <p>Large accumulations of data should not be downloaded or copied.</p> |

### Examples of documents that may be marked PUBLIC

All documents that are published under the University's Freedom of Information Act Publication Scheme, for example the Annual Report and Financial Statements; policies once they are approved, minutes and papers of Court, Council and other committees. Note that documents marked 'Public' may not be re-classified to any other level, but that documents in the two other levels are likely, over time, to move into the 'Public' classification.

### **Examples of documents that may be marked RESTRICTED**

Such documents might include internal briefing papers. The documents may be restricted to the University, or to a group in it, or to a group in the University and an external partner. Note that documents marked 'Restricted' might lose this marking over time.

### **Examples of documents that may be marked CONFIDENTIAL**

This is the highest level of marking, and, for some documents, might persist for considerable periods of time. It is advisable to note clearly the group who may have access to such documents. Such documents might include papers relating to possible redundancies, patient-level research data, data that is commercially sensitive to a project or a company providing research funds, and data relating to living individuals, whether employees of this University or not.

### **Examples of documents that move through ALL THREE marking levels**

Exam scripts start their life as 'Restricted'; once the exam has been held they might become 'Confidential' (to the University and its students, to protect intellectual property in module design and examination) for a period of years, and then become 'Public' as their sensitivity declines over time.

## Development of an Information Classification and Handling Policy – Cardiff University, case study

### Introduction

As part of the University-wide Information Security Framework Programme following ISO/IEC 27001 principles, we identified the need to establish an Information Classification, i.e. a University-wide system of categorising information in relation to its sensitivity and confidentiality, together with associated rules for the handling of each category of information in order to ensure the appropriate level of security (confidentiality, integrity and availability) could be applied.

### Information Classification Development

A review of other universities' classification systems was undertaken as well as those of our key partners such as the NHS and government. Both the NHS and the government's classifications were under review at the time and what was in place could not for various reasons simply be transplanted to the University setting. Whilst a few universities had developed classifications with elements that we liked there was not one single scheme, at the time that we wished to follow in its entirety. Instead it was decided to develop our own classification looking to:

- keep it simple,
- make the labels intuitive and
- base it on impact of disclosure or loss and align this with our newly defined risk assessment impact scales.

We originally came up with a 4 point scale – with two categories relating to confidentiality ('Highly Confidential' and 'Confidential') and one category relating to criticality/integrity ('Protect'). The fourth category was Non-Classified. It became obvious after a short while however that the Protect category did not work in the same way as the other two classified categories so we decided to drop it as a category in itself and build in the relevant criticality/integrity policy considerations into each of the other categories.

A conscious decision was taken not to treat Personal Data or Sensitive Personal Data (as defined by the Data Protection Act) as a categories in themselves as the impact of disclosure did not always correlate. Some Sensitive Personal Data and much Personal Data is already public domain and not therefore 'sensitive' or confidential at all. We wanted to keep the focus of the categories on the scale of impact of inappropriate disclosure on the institution, groups or the individual. The definitions of the two classified categories (Highly Confidential and Confidential) were designed to include both confidential personal data (such as salaries) and confidential non-personal data (such as competitive business strategy, security codes, etc.).

Examples were given for each category. The short definitions of the categories are below:

- **C1 – Highly Confidential** - Has the potential to cause serious damage or distress to individuals or serious damage to the University's interests if disclosed inappropriately
- **C2 – Confidential** - Has the potential to cause a negative impact on individuals' or the University's interests (but not falling into C1)
- **NC – Not Classified** - Information not falling into either of the Classified categories

### Policy

Having got the Programme Steering group to approve the Information Classification we then developed a handling rules and a supporting policy. It was determined that the scope of the policy would cover all information held by and on behalf of the University and the handling rules would apply to members of the University and to third parties handling University information. We also decided that where the University holds information on behalf of another organisation with its own information classification agreement shall be reached as to which set of handling rules shall apply – acknowledging that some data handling requirements from external organisations may be very stringent and require specific security arrangements to be put in place.

### Handling Rules development

The Handling Rules were then drawn up to set out the aspirational policy in relation to the handling of University information depending upon whether that information is classified (Highly Confidential C1 or Confidential C2) or not, where and how (i.e. paper or electronic) it is held, and the environmental context. The rules attempt to address the variance in risks associated with the different combinations of information, format or device, and environment. As well as the University context, the document covers the rules around use of personal devices in respect of classified information as well as non-University owned applications that staff may wish to use to transfer or hold University information. The University is currently reviewing 'Bring Your Own Device' which is widely used by staff, so the draft Handling Rules had to attempt to introduce some level of security to the riskiest types of remote and mobile working without an outright ban on BYOD. The rules were drawn up with a view to the existing state of security controls at the time as well as known future improvements, so they contain statements such as 'avoid download' and 'read only' on personal devices where we know we can't currently stop this use but wish to discourage it. We tried to make the security controls consistent between paper and digital information so that Highly Confidential information was treated with equal concern whether it was in hard copy files or on a laptop. It was also important that the rules were presented in a user friendly format and work well on the web.

## Consultation

The draft Handling Rules were developed by a small project team involving staff from both Governance and IT, then posted on an internal collaborative community which included senior representatives of the Colleges and Professional Services as well as School Managers and local IT representatives working closely with academics. Over 100 members of the community downloaded the file and 18 staff provided a total of over 50 comments. All comments were helpful and supportive of the aims of the document. A feedback table was compiled indicating what action had been taken in response to the comments received, and this was made available to the community.

## Approval and Equality Impact Assessment

The draft Handling Rules were presented to the Steering Group and the University's Executive Board. It was noted that there would be some financial implications in terms of: a) future procurement of equipment that meets a minimum security specification and b) demands for University equipment to be purchased to replace personally owned equipment. In accordance with the Equality Act we also undertook an Equality Impact Assessment of the rules. This found a likely adverse impact on specific protected characteristic groups if they were currently using personally owned equipment to handle Classified (C1 or C2) information in the context of institutionally approved flexible working/reasonable adjustment. The proposed mitigation involves the prioritisation of provision of appropriate University owned equipment for those affected staff.

The draft Handling Rules are currently approved only as guidelines until such time as the programme has delivered some specific tools (such as enterprise encryption and a secure but user friendly file sync and share alternative) to support the more aspirational statements. Other tools may enable more differentiation between the rules relating to C1 and C2 information. In addition we will add in disposal and printing as handling processes that are currently not included and continue to gather feedback on the practical aspects of implementation. At this point the 'Handling Rules' will be reviewed, turned into enforceable policy and promoted through mandatory information security training. We will also develop a similar, but different document for contractors' use of University information.

The Information Classification policy and draft Handling Rules are available here: <http://sites.cardiff.ac.uk/isf/handling/>

# Information Classification and Handling Policy – Cardiff University

## 1 Purpose

The purpose of this policy is to establish a University-wide system of categorising information in relation to its sensitivity and confidentiality, and to define associated rules for the handling of each category of information in order to ensure the appropriate level of security (confidentiality, integrity and availability) of that information.

## 2 Scope

This policy covers all information held by and on behalf of Cardiff University and the handling rules shall apply to members of the University and to third parties handling University information. Where the University holds information on behalf of another organisation with its own information classification agreement shall be reached as to which set of handling rules shall apply.

## 3 Relationship with existing policies

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy and all supporting policies.

## 4 Policy Statement

All members of Cardiff University and third parties who handle information on behalf of Cardiff University have a personal responsibility for ensuring that appropriate security controls are applied in respect of the information they are handling for the University. Appropriate security controls may vary according to the classification of the information and the handling rules for the relevant category shall be followed.

## 5 Policy

- 5.1 All information held by or on behalf of Cardiff University shall be categorised according to the Information Classification (Annex 1). The categorisation shall be determined by the originator of the information and all information falling into the classified categories shall be marked as such.
- 5.2 Information shall be handled in accordance with the Information Handling Rules (Annex 2) and where information falls within more than one category, the higher level of protection shall apply in each case
- 5.3 Where a third party will be responsible for handling information on behalf of Cardiff University, the third party shall be required by contract to adhere to this policy prior to the sharing of that information
- 5.4 Where the University holds information on behalf of another organisation with its own information classification, written agreement shall be reached as to which set of handling rules shall apply prior to the sharing of that information

## 6 Responsibilities

- 6.1 The Senior Information Risk Owner shall ensure that the Information Classification and associated Handling Rules are reviewed regularly to ensure they remain fit for purpose.
- 6.2 It shall be the responsibility of every individual handling information covered by this policy, to mark classified material as such, to apply the appropriate handling rules to each category of information, and to seek clarification or advice from a line manager or the Information Security Co-ordinator where they are unsure as to how to label or handle information.
- 6.3 All members of the University shall report issues of concern in relation to the application of this policy, including alleged non-compliance, to the Information Security Co-ordinator.

## 7 Compliance

Breaches of this policy may be treated as a disciplinary matter dealt with under the University's staff disciplinary policies or the Student Disciplinary Code as appropriate. Where third parties are involved breach of this policy may also constitute breach of contract.

## Annex 1 – Information Classification v2

| Category Title              | Classified C1<br>HIGHLY CONFIDENTIAL   | Classified C2<br>CONFIDENTIAL   | NC<br>Non -Classified   |
|-----------------------------|--|---|---|
| Description                 | <p><b>Has the potential to cause serious damage or distress to individuals or serious damage to the University's interests if disclosed inappropriately</b></p> <p><i>Refer to Impact levels of 'high' or 'major' on the Risk Measurement Criteria</i></p> <ul style="list-style-type: none"> <li>• Data contains highly sensitive private information about living individuals and it is possible to identify those individuals <i>e.g. Medical records, serious disciplinary matters</i></li> <li>• Non-public data relates to business activity and has potential to seriously affect commercial interests and/ or the University's corporate reputation <i>e.g. REF strategy</i></li> <li>• Non-public information that facilitates the protection of individuals' personal safety or the protection of critical functions and key assets <i>e.g. access codes for higher risk areas, University network passwords.</i></li> </ul> | <p><b>Has the potential to cause a negative impact on individuals' or the University's interests (but not falling into C1)</b></p> <p><i>Refer to Impact levels 'Minor' or 'Moderate' on the Risk Measurement Criteria</i></p> <ul style="list-style-type: none"> <li>• Data contains private information about living individuals and it is possible to identify those individuals <i>e.g. individual's salaries, student assessment marks</i></li> <li>• Non-public data relates to business activity and has potential to affect financial interests and/or elements of the University's reputation <i>e.g. tender bids prior to award of contract, exam questions prior to use</i></li> <li>• Non-public information that facilitates the protection of the University's assets in general <i>e.g. access codes for lower risk areas</i></li> </ul> | <p><b>Information not falling into either of the Classified categories</b></p> <p><i>e.g. Current courses, Key Information Sets, Annual Report and Financial Statements, Freedom of Information disclosures</i></p>   |
| Type of protection required | <p>Key security requirements:</p> <p><b>Confidentiality and integrity</b></p> <p>This information requires significant security measures, strictly controlled and limited access and protection from corruption</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p>   | <p>Key security requirements:</p> <p><b>Confidentiality and integrity</b></p> <p>This information requires security measures, controlled and limited access and protection from corruption</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p>   | <p>Key security requirement:</p> <p><b>Availability</b></p> <p>This information should be accessible to the University whilst it is required for business purposes</p> <p>Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?</p> |

## Annex 2 – Handling Guidelines v2

General advice:

- Always aim to keep Classified Information (C1 and C2) within the University's secure environment.
- Where this is not possible consider whether the information can be redacted or anonymised to remove confidential or highly confidential information, thereby converting it to Non-Classified Information (NC).
- Report any potential loss or unauthorised disclosure of Classified Information to the IT Service Desk on 74xxx
- Seek advice on secure disposal of equipment containing Classified Information via the IT Service Desk on 74xxx
- Use the Confidential Waste Service for disposal of paper and small electronic media xxx@cardiff.ac.uk

### INFORMATION HANDLING - Electronic/digital information storage

| Location   | Default Features   | Classified C1<br>HIGHLY CONFIDENTIAL   | Classified C2<br>CONFIDENTIAL  | NC<br>Non -Classified  |
|--|--|--|--|--|
| Shared R: or S:                                      | Controlled access ✓<br>Shared space ✓<br>Central back-up ✓<br><i>Service delivers high availability and resilience</i> | Use restricted access folders<br><br><i>Consider:</i><br>file password protection for most sensitive files   | Use restricted access folders or password protect files  | ✓  |
| Home H:  | Controlled access ✓<br>Shared space ✗<br>Central back-up ✓<br><i>Service delivers high availability and resilience</i> | <i>Consider:</i><br>file password protection for most sensitive files  | <i>Consider:</i><br>file password protection for most sensitive files  | <i>Consider:</i><br>Does information need to be shared with colleagues - if so enable folder sharing or move to shared drive |
| School/Department based server                       | Controlled access ?<br>Shared space ?<br>Central back-up ?   | Seek advice from local IT on default access rights, physical security of server and back-up<br><br><b>No storage or creation permitted unless</b> server environment is equivalent to IT Services server security environment)<br><br>If yes then required to use restricted access mechanisms where online access is shared<br><br><i>Consider password protection for most sensitive files</i><br><br><i>Consider:</i><br>Any back-up requirements | Seek advice from local IT on default access rights, physical security of server and back-up<br><br><b>No storage or creation permitted unless</b> server environment is equivalent to IT Services server security environment)<br><br>If yes then required to use restricted access mechanisms where online access is shared<br><br><i>Consider:</i><br>Any back-up requirements | <i>Consider:</i><br>Any back-up requirements   |
| Other IT Services maintained service (e.g. database) | Controlled access ✓<br>Shared space ?<br>Central back-up ✓   | Seek advice from IT Services on default access rights<br><br>Use restricted access mechanisms where online access is shared  | Seek advice from IT Services on default access rights<br><br>Use restricted access mechanisms where online access is shared  | ✓  |

## INFORMATION HANDLING - Electronic/digital information storage

| Location   | Default Features  | Classified C1<br>HIGHLY CONFIDENTIAL   | Classified C2<br>CONFIDENTIAL  | NC<br>Non -Classified  |
|--|---|--|--|--|
| University desktop PC<br>hard drive C: or D:                   | In non-public areas:<br>Controlled access ✓<br>Shared space ✗<br>Central back-up ✗                    | Encrypt drive<br>Lock screen when unattended   | Either encrypt drive or password protect files<br>Lock screen when unattended  | Lock screen when unattended<br><i>Consider:</i><br>Any back-up requirements  |
|  | In public areas (e.g. Open Access PCs):<br>Controlled access ✗<br>Shared space ✗<br>Central back-up ✗ | <b>Use not permitted</b><br><i>High risk of incidental disclosure</i>  | <b>Use not permitted</b><br><i>High risk of incidental disclosure</i>  | <i>Consider:</i><br>Any back-up requirements   |
| Personally owned (e.g. home) desktop PC<br>hard drive C: or D: | Controlled access ✗<br>Shared space ?<br>Central back-up ✗  | <b>No storage or creation permitted on device</b><br><i>May be used for read only remote connection to access files if used in a private environment.</i><br>Do not download files to device.<br>Do not leave logged in and unattended<br>Clear browser cache after read only use. | <b>No storage or creation permitted on device</b><br><i>May be used for read only remote connection to access files if used in a private environment.</i><br>Do not download files to device.<br>Do not leave logged in and unattended<br>Clear browser cache after read only use. | <b>No master copy storage permitted</b><br><i>May be used for remote connection to access files</i><br>Do not leave logged in and unattended<br>Created documents must be saved on University network or University owned device |

## INFORMATION HANDLING - Electronic/digital information storage

| Location                | Default Features   | Classified C1<br>HIGHLY CONFIDENTIAL  | Classified C2<br>CONFIDENTIAL   | NC<br>Non -Classified   |
|-------------------------|--|---|---|---|
| University owned Laptop | Controlled access ✘<br>Shared space ✘<br>Central back-up ✘ | <p>Encrypt device – use strong password with maximum of 10 minutes inactivity until device locks.</p> <p>Use secure remote connection (e.g. Cardiff Portal or WebDav) to access files and avoid download or storage</p> <p>Do not use to store master copy of vital records</p> <p>Do not work on files in public areas</p> <p>Do not leave logged in and unattended</p> <p>Do not share use of device with non-University staff</p> <p><i>Consider:</i><br/>Any back-up requirements</p> | <p>Encrypt device – use strong password with maximum of 10 minutes inactivity until device locks.</p> <p>Use secure remote connection (e.g. Cardiff Portal or WebDav) to access files and avoid download or storage</p> <p>Do not use to store master copy of vital records</p> <p>Do not work on files in public areas</p> <p>Do not leave logged in and unattended</p> <p>Do not share use of device with non-University staff</p> <p><i>Consider:</i><br/>Any back-up requirements</p> | <p>Do not use to store master copy of vital records</p> <p>Do not leave logged in and unattended</p> <p>Do not share use of device with non-University staff</p> <p><i>Consider:</i><br/>Any back-up requirements</p>                               |
| Personally owned Laptop | Controlled access ✘<br>Shared space ✘<br>Central back-up ✘ | <p><b>No storage or creation permitted on device</b></p> <p><i>May be used for read only remote connection to view files if used in a private environment</i></p> <p>Do not download files to device.</p> <p>Do not leave logged in and unattended</p> <p>Clear browser cache after read only use.</p>  | <p><b>No storage or creation permitted on device</b></p> <p><i>May be used for read only remote connection to view files if used in a private environment</i></p> <p>Do not download files to device.</p> <p>Do not leave logged in and unattended</p> <p>Clear browser cache after read only use.</p>  | <p><b>No master copy storage permitted</b></p> <p><i>May be used for remote connection to access files</i></p> <p>Do not leave logged in and unattended</p> <p>Created documents must be saved on University network or University owned device</p> |

## INFORMATION HANDLING - Electronic/digital information storage

| Location                                 | Default Features   | Classified C1<br>HIGHLY CONFIDENTIAL   | Classified C2<br>CONFIDENTIAL  | NC<br>Non -Classified   |
|--|--|--|--|---|
| Personally owned<br>Smartphone or tablet | Controlled access ?<br>Shared space ✘<br>Central back-up ✘ | <b>No storage or creation permitted on device</b><br><br><i>May be used for read only remote connection to access files if used in a private environment</i><br><br>Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks.<br><br>Encryption setting to be enabled where available.<br><br>Clear browser cache after read only use.  | <b>No storage or creation permitted on device</b><br><br><i>May be used for read only remote connection to access files if used in a private environment</i><br><br>Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks.<br><br>Encryption setting to be enabled where available.<br><br>Clear browser cache after read only use.  | <b>No master copy storage permitted</b><br><br><i>May be used for remote connection to access files</i><br><br>Created documents must be saved on University network or University owned device |
| University owned<br>Smartphone or tablet | Controlled access ?<br>Shared space ✘<br>Central back-up ? | Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks.<br><br>Encryption setting to be enabled where available.<br><br>Services to locate device and remote wipe in case of loss/theft to be enabled.<br><br>Do not leave device unattended in public areas.<br><br>Do not share use of device with non-University staff<br><br>Avoid storage of highly confidential information on device.<br><br>May be used for secure remote connection (e.g. Cardiff Portal or WebDav) to access files but do not work on highly confidential files in public areas<br><br><i>Consider:</i><br><br>Any back-up requirements | Device to be protected by strong password, with maximum of 10 minutes inactivity until device locks.<br><br>Encryption setting to be enabled where available.<br><br>Services to locate device and remote wipe in case of loss/theft to be enabled.<br><br>Do not leave device unattended in public areas.<br><br>Do not share use of device with non-University staff<br><br>Avoid storage of confidential information on device.<br><br>May be used for secure remote connection (e.g. Cardiff Portal or WebDav) to access files but do not work on confidential files in public areas<br><br><i>Consider:</i><br><br>Any back-up requirements | Do not leave device unattended in public areas<br><br>Do not share use of device with non-University staff<br><br><i>Consider:</i><br><br>Any back-up requirements                              |

## INFORMATION HANDLING - Electronic/digital information storage

| Location   | Default Features   | Classified C1<br>HIGHLY CONFIDENTIAL  | Classified C2<br>CONFIDENTIAL  | NC<br>Non -Classified   |
|--|--|---|--|---|
| Small capacity portable storage devices<br>(e.g. USB, CD,)         | Controlled access ✘<br>Shared space ✘<br>Central back-up ✘ | <b>Avoid use where possible</b><br><br><i>Consider alternative means of access instead e.g. use secure remote connection (e.g. Cardiff Portal or WebDav) to access files with no download</i><br><br>If no alternative to use then encrypt media – strong passcode<br><br>Do not use to store master copy<br><br>Keep in lockable cabinet/drawer which is locked when unattended. | Encrypt media - strong passcode<br><br>Not suitable for long term storage<br><br>Do not use to store master copy<br><br>Keep in lockable cabinet/drawer which is locked when unattended. | Not suitable for long term storage<br><br>Do not use to store master copy |
| Large capacity portable storage devices (i.e. external hard drive) | Controlled access ✘<br>Shared space ✘<br>Central back-up ✘ | Encrypt device – strong passcode<br><br>Do not use to store master copy<br><br>Keep in lockable cabinet/drawer which is locked when unattended.   | Encrypt device – strong passcode<br><br>Do not use to store master copy<br><br>Keep in lockable cabinet/drawer which is locked when unattended.  | Do not use to store master copy   |

## INFORMATION HANDLING - Electronic Collaboration and Synchronisation

| Location   | Default Features   | Classified C1<br>HIGHLY CONFIDENTIAL   | Classified C2<br>CONFIDENTIAL  | NC<br>Non -Classified           |
|--|--|--|--|---------------------------------|
| University's virtual learning environment  | Controlled access ✓<br>Shared space ✓<br>Central back-up ✓ | <b>No storage permitted</b>  | <b>Requirement:</b><br>Use restricted access folder  | ✓                               |
| University collaborative workplace<br>(e.g. Connections, Quickr Teamplace)   | Controlled access ✓<br>Shared space ✓<br>Central back-up ✓ | <b>No storage permitted</b><br><br><i>Use University solutions e.g. (Quickr or Filr where available) instead</i> | <b>No storage permitted</b><br><br><i>Use University solutions e.g. Quickr (or Filr where available) instead</i> | Do not use to store master copy |
| External 'cloud' storage/ file sync provider non-University contract e.g personal Onedrive, individually set up Dropbox accounts | Controlled access ?<br>Shared space ?<br>Central back-up ✘ | <b>No storage permitted</b><br><br><i>Use University solutions e.g. (Quickr or Filr where available) instead</i> | <b>No storage permitted</b><br><br><i>Use University solutions e.g. Quickr (or Filr where available) instead</i> | Do not use to store master copy |

## INFORMATION HANDLING - Electronic Transmission

| Location   | Default Features   | Classified C1<br>HIGHLY CONFIDENTIAL  | Classified C2<br>CONFIDENTIAL   | NC<br>Non -Classified   |
|--|--|---|---|---|
| From: @cardiff.ac.uk<br>To: @cardiff.ac.uk<br><br>Sending from University hosted email account to same                     | Controlled access ✓<br>Shared space ?<br>Central back-up ✓ | Only as password protected attachment, marked confidential and double check recipient<br><br><i>Consider whether sender or recipient may have delegated authority to others to access the account</i>   | Marked confidential and double check recipient<br><br><i>Consider whether sender or recipient may have delegated authority to others to access the account</i>  | ✓   |
| From: @cardiff.ac.uk<br>To: @xxx.xxx<br><br>Sending from University hosted email account to an external account            | Controlled access ✓<br>Shared space ?<br>Central back-up ✓ | Only as password protected attachment, marked confidential, double check recipient and get their permission to use that account<br><br><i>Consider whether sender or recipient may have delegated authority to others to access the account</i> | As password protected attachment, marked confidential and double check recipient and get their permission to use that account<br><br><i>Consider whether sender or recipient may have delegated authority to others to access the account</i> | ✓   |
| From: @xxx.com<br>To: @xxx.xxx<br><br>Sending from an externally provided personal email account (e.g. hotmail, gmail etc) | Controlled access ✗<br>Shared space ?<br>Central back-up ✗ | <b>Not permitted - unless sending to @cardiff.ac.uk</b><br><br>Use University provided alternative to send message instead  | <b>Not permitted- unless sending to @cardiff.ac.uk</b><br><br>Use University provided alternative to send message instead   | <b>Not permitted- unless sending to @cardiff.ac.uk</b><br><br>Use University provided alternative to send message instead |

## INFORMATION HANDLING - Electronic Transmission

| Location                                    | Default Features   | Classified C1<br>HIGHLY CONFIDENTIAL  | Classified C2<br>CONFIDENTIAL  | NC<br>Non -Classified |
|---|--|---|--|-----------------------|
| Fastfile - a secure web based file transfer | Controlled access ✓<br>Shared space ✓<br>Central back-up ✓ | Only as password protected attachment, marked confidential and double check recipient<br><br><i>Consider whether sender or recipient may have delegated authority to others to access the account</i> | As password protected attachment, marked confidential and double check recipient<br><br><i>Consider whether sender or recipient may have delegated authority to others to access the account</i> | ✓                     |

## INFORMATION HANDLING - Paper records and other records storage

| Location     | Classified C1<br>HIGHLY CONFIDENTIAL   | Classified C2<br>CONFIDENTIAL  | NC<br>Non -Classified   |
|--------------|--|--|---|
| Paper copies | <p><b>Consider:</b></p> <p>Protection from fire and flood damage</p> <p>In restricted access University areas:</p> <p><b>Requirement:</b></p> <p>In lockable cabinet/drawer which is locked when not in active use.</p> <p>No papers left out unless being actively worked on.</p> <p>In <b>unrestricted</b> access University areas:</p> <p style="text-align: center;"><b>✘</b></p> <p><b>Not permitted</b></p> <p><i>Alternative: create as/convert to electronic documents and use secure remote connection with permitted device</i></p> <p>Off-site working:</p> <p style="text-align: center;"><b>✘</b></p> <p><b>Not permitted</b></p> <p><i>Alternative: create as/convert to electronic documents and use secure remote connection (e.g. Cardiff Portal or WebDav) with permitted device</i></p> | <p><b>Consider:</b></p> <p>Protection from fire and flood damage</p> <p>In restricted access University areas:</p> <p><b>Requirement:</b></p> <p>In lockable cabinet/drawer which is locked when office is unattended.</p> <p>No papers left out when desk unattended.</p> <p>In <b>unrestricted</b> access University areas:</p> <p><b>Requirement:</b></p> <p>In lockable cabinet/drawer which is locked when not in active use.</p> <p>No papers left out unless being actively worked on.</p> <p>Off-site working:</p> <p><b>Requirement:</b></p> <p>If needed to be taken off site a back-up copy must be made beforehand.</p> <p>Not to be left unattended and to be locked away in secure building when not in use.</p> | <p>In restricted access University areas:</p> <p style="text-align: center;">✓</p> <p>In <b>unrestricted</b> access University areas:</p> <p style="text-align: center;">✓</p> <p>Off-site working:</p> <p><i>Consider making a back-up copy before taking off site</i></p> |

## INFORMATION HANDLING - Paper and other media transmission

| Location                | Classified C1<br>HIGHLY CONFIDENTIAL  | Classified C2<br>CONFIDENTIAL   | NC<br>Non -Classified  |
|-------------------------|---|---|--|
| Internal postal service | <p style="text-align: center;"><b>✘</b></p> <p style="text-align: center;"><b>Not permitted</b></p> <p><i>Alternative:</i><br/>request specific hand delivery instead</p> <p><b>Consider:</b><br/><i>Making a back-up copy before posting</i></p>                 | <p><b>Requirement:</b><br/>In sealed envelope marked confidential and with sender details</p> <p><b>Consider:</b><br/><i>Making a back-up copy before posting</i></p>   | <p style="text-align: center;">✓</p> <p><b>Consider:</b><br/><i>Making a back-up copy before posting</i></p> |
| External postal service | <p><b>Requirement:</b><br/>Via tracked and delivery recorded service, double wrapped (2 envelopes) and marked confidential.</p> <p><b>Consider:</b><br/><i>Making a back-up copy before posting</i></p>   | <p><b>Requirement:</b><br/>Via tracked and delivery recorded service, and marked confidential.</p> <p><b>Consider:</b><br/><i>Making a back-up copy before posting</i></p>  | <p style="text-align: center;">✓</p> <p><b>Consider:</b><br/><i>Making a back-up copy before posting</i></p> |
| Fax machine             | <p><b>Requirement:</b><br/>if recipient has verified security of receiving machine and is at machine awaiting receipt</p> <p><b>Consider:</b><br/><i>Converting to an electronic format and using secure electronic transfer method instead e.g. Fastfile</i></p> | <p><b>Requirement:</b><br/>if recipient has verified security of receiving machine and is at machine awaiting receipt</p> <p><b>Consider:</b><br/><i>Converting to an electronic format and using secure electronic transfer method instead e.g. Fastfile</i></p> | <p style="text-align: center;">✓</p>   |

## University Guidance on Classification of Information - University of Oxford

| LABEL        | DESCRIPTION  | EXAMPLE CONTROLS  |
|--------------|--|---|
| CONFIDENTIAL | <ul style="list-style-type: none"> <li>• Confidential information should be available only to small, tightly restricted groups of authorised users.</li> <li>• Disclosure of such information will have a severe adverse impact on the business of the University, its reputation, or the safety or wellbeing of its staff/ members.</li> <li>• Unauthorised disclosure of such information may have a severe financial impact on the University.</li> <li>• The confidentiality of such assets will far outweigh the importance of their availability.</li> <li>• Information assets in this category would include highly sensitive personal information as well as those with a high financial value, legal requirements for confidentiality and information, which is critical to the business operation of the University.</li> </ul> | <ul style="list-style-type: none"> <li>• Information classified as CONFIDENTIAL should be stored in such a way as to ensure that only authorised persons may access the information.</li> <li>• Information should be stored in a physically secure manner with appropriate defence against unauthorised entry. Physical access should be monitored and appropriate audit trails of access should be maintained.</li> <li>• File or disk encryption may be considered as an additional layer of defence or where physical security is considered insufficient.</li> <li>• Copies of such information should be kept to an absolute minimum and an audit trail should be maintained and secured for all copies of the information. It is assumed that the confidentiality of such information outweighs the need for availability and loss or destruction of such information would be preferable to unauthorised disclosure.</li> <li>• Such information may be stored on machines that are isolated from the network. Where remote access is required this must be controlled via a well-defined access control policy and tight logical access controls designed to allow the minimum access necessary.</li> <li>• Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.</li> <li>• All users accessing CONFIDENTIAL information must be authenticated and an audit trail of all access must be secured and maintained. This should be kept for a minimum of 6 months or longer where applicable. Authentication should be appropriate, but where passwords are used there clearly defined policies should be in place and implemented. Other forms of authentication should be considered in addition.</li> <li>• Preferably, such information should be kept on on-site systems and users should not be able to make local copies of such information. Where this is required the information must be encrypted in transit and in storage.</li> <li>• Strict policies and procedures must be in place for the secure disposal/destruction of such information.</li> <li>• Any users having access to this information should be vetted as appropriate.</li> <li>• All users must be made aware of their responsibilities for handling such information. Any breach of policy regarding such information will be investigated and disciplinary action is a likelihood.</li> <li>• Any breach of the confidentiality of such information must be reported to the owner of that information. Other parties such as OxCERT and the University Data Protection Officer should also be informed.</li> <li>• Any security incident relating to computers or users having access to such information must be reported to OxCERT and investigated.</li> </ul> |

| LABEL     | DESCRIPTION  | EXAMPLE CONTROLS  |
|-----------|--|---|
| SENSITIVE | <p>Information classed as SENSITIVE should only be available to groups of users who require access as part of their role within the University.</p> <ul style="list-style-type: none"> <li>• Disclosure of such information may have an adverse effect on the business of the University, its reputation or may cause distress to its staff/members.</li> <li>• Unauthorised disclosure of such information may have a financial impact on the University.</li> <li>• Information assets in this category would include sensitive personal information and other personal information to which access is only required by a subset of users. The information may have a substantial financial value and it is highly likely there will be legal requirements for maintaining its confidentiality.</li> </ul> | <ul style="list-style-type: none"> <li>• Information classified as SENSITIVE should be stored in such a way as to ensure that only authorised persons may access the information.</li> <li>• Information should be stored in a physically secure manner with appropriate defence against unauthorised entry. Physical access should be monitored and appropriate audit trails of access should be maintained.</li> <li>• File or disk encryption may be considered where physical security is considered insufficient.</li> <li>• An audit trail should be maintained and secured documenting all copies of the information.</li> <li>• Remote access must be controlled via a well-defined access control policy and appropriate logical access controls.</li> <li>• Remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.</li> <li>• All users accessing SENSITIVE information must be authenticated and an audit trail of all access must be secured and maintained. This should be kept for a minimum of 6 months or longer where applicable.</li> <li>• Authentication should be appropriate, but where passwords are used clearly defined policies should be in place and implemented. Other forms of authentication may be considered in addition.</li> <li>• Users may need to make local copies of such information in which case it is likely that encryption in transit and in storage would be required.</li> <li>• Policies and procedures should be in place for the secure disposal/ destruction of such information.</li> <li>• Users should be made aware of their responsibilities for handling such information. Any breach of policy regarding such information will be investigated and disciplinary action is a possibility.</li> <li>• Any breach of the confidentiality of such information must be reported to the owner of that information. Other parties such as OxCERT and the University Data Protection Officer should also be informed where appropriate.</li> <li>• Any security incident relating to computers or users having access to such information must be reported to the IT support staff responsible for the information system. The local ITSS will then decide whether the incident should be reported to OxCERT.</li> </ul> |

| LABEL        | DESCRIPTION  | EXAMPLE CONTROLS   |
|--------------|--|--|
| RESTRICTED   | <ul style="list-style-type: none"> <li>● Information classed as RESTRICTED should only be available to staff/ members of the University, sub-groups within the University and/or specifically authorised third parties.</li> <li>● Disclosure of such information is unlikely to have an adverse effect on the business of the University or its reputation. However it may have a negative impact on smaller groups or individuals within the University.</li> <li>● Unauthorised disclosure of such information is unlikely to have a significant financial impact on the University.</li> <li>● Information assets in this category may include some personal information, which should be processed fairly and with the consent of the data subject.</li> <li>● Information in this category is unlikely to have a substantial financial value.</li> </ul> | <ul style="list-style-type: none"> <li>● Users accessing RESTRICTED information should be authenticated and an audit trail maintained. This should be kept for a minimum of 3 months or longer where applicable.</li> <li>● Users are likely to make local copies of such information though encryption is likely not to be necessary.</li> <li>● Restricted information should be deleted when it is no longer necessary for the task in hand.</li> <li>● Any breach of policy regarding such information may be investigated though disciplinary action is unlikely.</li> <li>● Breaches of the confidentiality of such information would be reported to the owner of that information where appropriate.</li> <li>● Security incidents relating to computers or users having access to such information should be reported to the IT support staff responsible for the information system. The local ITSS may report the incident to OxCERT.</li> </ul> |
| UNRESTRICTED | <p>This classification can be used to indicate positively that no protective marking is required. Such information is likely to already exist in the public domain. Its disclosure will have a negligible effect on the University or on any sub-group or individual within the University.</p>  | <p>Information in this category should not need users to be authenticated to access it.</p> <p>Such information should be deleted when it is no longer needed.</p>   |

# Resources for Chapter 8 – Roles and competencies

## RESOURCES

- [Job description template - Information Security Manager](#)
- [Job description template - Senior Information Security Specialist](#)
- [Job description template - Information Security Specialist](#)
- [SFIA competencies](#)
- [Collaboration between security administrators and academic researchers – UCL, case study](#)

## Job description template - Information Security Manager

Job grade Management and Specialist Grade

### Job purpose

- Provides leadership and guidelines on information assurance security expertise for the organisation, working effectively with strategic organisational functions such as legal experts and technical support to provide authoritative advice and guidance on the requirements for security controls.
- Provides for restoration of information systems by ensuring that protection, detection, and reaction capabilities are incorporated.
- Develops strategies for ensuring both the physical and electronic security of automated systems.
- Ensures that the policy and standards for security are fit for purpose, current and are correctly implemented.
- Reviews new business proposals and provides specialist advice on security issues and implications.

### Duties and responsibilities

- Develops information security policy, standards and guidelines appropriate to business, technology and legal requirements and in accordance with best professional and industry practice.
- Prepares and maintains a business strategy and plan for information security work which addresses the evolving business risk and information control requirements, and is consistent with relevant IT and business plans, budgets, strategies, etc.
- Operates as a focus for IT security expertise for the organisation, providing authoritative advice and guidance on the application and operation of all types of security control, including legislative or regulatory requirements such as data protection and software copyright law.
- Manages the work of all other IT security specialist staff, including project and task definition and prioritisation, quality management and budgetary control, and management tasks such as recruitment and training when required.
- Manages the operation of appropriate security controls as a production service to business system users.
- Develops implementation approach, taking account of current best practice, legislation and regulation. Ensures implementation of information security strategy in automated systems and ensures operations of security systems. Analyses results of investigations into complex, or highly sensitive security violations, to determine whether standards are fit for purpose, are current and are correctly implemented.
- Reports any significant breaches in security to senior management. Interviews offenders in conjunction with the relevant line manager or on own authority if the breach warrants it. Where appropriate, participates in forensic evidence gathering, disciplinary measures, and criminal investigations.
- Ensures that procedures are in place for investigation of system access enquiries referred by support staff and for handling all enquiries relating to information security, contingency planning as they affect the activities of the organisation, function or department. Authorises implementation of procedures to satisfy new access requirements, or provide effective interfaces between users and service providers.
- Devises new or revised procedures relating to security control of all IT environments, systems, products or services in order to demonstrate continual improvement in control including creation of auditable records, user documentation and security awareness literature.
- Authorises and initiates the provision of training, guidance and support to other security administrators and their agents within the employing organisation, in all aspects of security policy and control.
- Reviews new business proposals and planned technical changes and provides specialist guidance on security issues and implications.
- Maintains knowledge of the technical specialism at the highest level.
- Keeps in close touch with and contributes to current developments in the technical specialism within employing organisation, own industry and in appropriate professional and trade bodies. Is fluent at articulating best practice and is a recognised authority in the technical specialism.
- Be familiar with relevant University IT-related procedures and policies (acceptable use, data protection, freedom of information, information security, purchasing etc) and advise colleagues and end-users accordingly.
- Undertake various other tasks on an occasional basis at the request of more senior staff in the department, and to a level commensurate with training, knowledge, grade and skills.

*Note: This job description was created in the spirit of the BCS (The Chartered Institute for IT), SFIA (Skills for the Information Age) level 6 with support from the BCS.*

## Organisational Responsibility

**Responsible to:** <line manager> but may receive strategic instruction from the Director of IT.

**Responsible for:** A team of <x> colleagues, staff at the senior level may be asked to deputise for their line manager in case of absence.

**Hours:** 37 hours per week, within the hours of 8:00 to 18:00 Mon to Thursday and 8:00 to 17:30 Friday, including 1 hour lunch period. The precise pattern of working within these guidelines will be agreed in advance with your manager.

## Special Conditions

Many staff carry mobile phones which allow them to be paged by various systems at all reasonable hours of the week. When monitoring, diagnosis and configuration of services needs to be done outside normal working hours, it can sometimes be appropriate for the work to be carried out remotely at home when convenient.

Attendance on site outside normal working hours is occasionally necessary, for example during major system changes and maintenance. Such out-of-hours working as is necessary is scheduled in negotiation with the group of staff with relevant skills, and takes account of the personal commitments and wishes of individuals.

**For purposes of system management, IT Services staff often have enhanced access to data, files and computer systems and must at all times respect the privacy of information to which they have enhanced access. The only exception to this will be investigations authorised by IT Services Director or his/her nominee.**

**Please note: <organisation> is working towards equal opportunities and observance of our equal opportunities policy will be required.**

## PERSON SPECIFICATION

**Job Title:** Information Security Manager

**Job Grade:** Management and Specialist Grade

**Department:** IT Services

All staff have a statutory responsibility to take reasonable care of themselves, others and the environment and to prevent harm by their acts or omissions. All staff are therefore required to adhere to the University's Health, Safety and Environmental Policy & Procedures.

|            | Essential  | Desirable   | Stage to be assessed     |
|------------|--|---|--------------------------|
| Experience | Demonstrates extensive knowledge of good security practice covering the physical and logical aspects of information products, systems integrity and confidentiality                    |   | Shortlisting             |
|            |  | Experience in managing a customer facing service. | Shortlisting             |
|            | Demonstrates strong examples of the use of: Principles, practices, tools and techniques of IT auditing.  |   | Interview                |
|            |  | Experience within the HE/FE sector.               | Shortlisting             |
|            | Displays a responsible attitude to following procedures, keeping records, and caring for equipment and other assets.   |   | Shortlisting & Interview |
|            | Demonstrated success in deploying methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing. |   | Shortlisting & Interview |

|                                       | Essential  | Desirable  | Stage to be assessed     |
|---------------------------------------|--|--|--------------------------|
| Skills and abilities                  | Shows aptitude for analysing and managing problems arising from incidents in the operation of information systems, combined with the ability to provide innovative technical solutions |  | Shortlisting & Interview |
|                                       |  | Technical background in multiple modern Operating Systems (Windows, Mac OS X, Linux etc) | Shortlisting             |
|                                       | High levels of technical investigation skills, the ability to research and collate information from a variety of sources into technical reports and recommendations.                   |  | Shortlisting             |
|                                       |  | Expert skills in the application of forensic techniques.                                 | Shortlisting             |
|                                       | Demonstrates excellent communication skills with an aptitude for dealing with users, colleagues and suppliers.   |  | Interview                |
|                                       |  | Technical authoring experience and proven documentation track record.                    | Shortlisting & Interview |
|                                       | Familiar with Methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing.                     |  | Shortlisting & Interview |
|                                       | Excellent written skills to write technical procedures, reports, system specifications etc.  |  | Shortlisting             |
|                                       | Excellent time management  |  | Shortlisting             |
|                                       | Ability to schedule your own workload and prioritise your work.  |  | Interview                |
| Training and Education/Qualifications | A willingness to undertake further training and to learn and adopt new procedures as and when required.  |  | Interview                |
|                                       | Ability to assimilate technical information and keep up-to-date in your field.   |  | Shortlisting & Interview |
|                                       | Degree with relevant IT/Computing content OR relevant professional IT qualifications and/or experience.  |  | Shortlisting             |
|                                       |  | Information Security related qualifications: CISSP, CISM or similar                      | Shortlisting             |
|                                       |  | ITIL Foundation training and accreditation.  | Shortlisting             |
|                                       |  | Formal management training   | Shortlisting             |
| Other                                 | To observe the organisation's Equal Opportunities policy at all times.   |  | Interview                |

Stages in assessment: **Shortlisting, Test (where appropriate) and Interview**

### Conditions of Service

The appointment will be on a **full time, open ended** contract on **Management and Specialist Grade (salary, discretionary to salary per annum)\*** at a starting salary commensurate with experience and qualifications.

\*The appointment will be subject to the University's normal Terms and Conditions of Employment for **Academic and Related** staff, details of which can be found at:

<Terms and Conditions Link>

### Informal Enquiries

Informal enquiries should be made to <name>, <title> by email at: <email address> or by telephone on <telephone number>.

### Application

The closing date for receipt of applications is <insert>.

## Job description template - Senior Information Security Specialist

Job grade Management and Specialist Grade

### Job purpose

- Obtains and acts on vulnerability information and conducts security risk assessments for business applications and computer installations; provides authoritative advice and guidance on security strategies to manage the identified risk.
- Investigates major breaches of security, and recommends appropriate control improvements. Interprets security policy and contributes to development of standards and guidelines that comply with this.
- Performs risk assessment, business impact analysis and accreditation for all major information systems within the organisation.
- Ensures proportionate response to vulnerability information, including appropriate use of forensics.
- Drafts and maintains the policy, standards, procedures and documentation for security.
- Monitors the application and compliance of security operations procedures and reviews information systems for actual or potential breaches in security.
- Ensures that all identified breaches in security are promptly and thoroughly investigated.
- Ensures that any system changes required to maintain security are implemented. Ensures that security records are accurate and complete.

### Duties and responsibilities

- Conducts security control reviews across a full range of control types and techniques, for business applications and computer installations. Seeks guidance from more experienced or specialised practitioners as required. Recommends appropriate action to management.
- Identifies threats to the confidentiality, integrity, availability, accountability and relevant compliance of information systems. Conducts risk and vulnerability assessments of business applications and computer installations in the light of these threats and recommends appropriate action to management.
- Conducts investigation, analysis and review following breaches of security controls, and manages security incidents. Prepares recommendations for appropriate control improvements, involving other professionals as required.
- Provides authoritative advice and guidance on the application and operation of all types of security controls, including legislative or regulatory requirements such as data protection and software copyright law. Contributes to development of standards and guidelines.
- Drafts and maintains policy, standards, procedures and documentation for security administration, taking account of current best practice, legislation and regulation. Ensures that all identified breaches in security are promptly and thoroughly investigated. Interviews offenders in conjunction with the relevant line manager or on own authority if the breach warrants it.
- Reviews information systems for actual or potential breaches in security, and investigates complex, or highly sensitive violations referred by more junior staff or colleagues, handling issues imaginatively, efficiently and professionally. Obtains factual information, and formulates opinions regarding exposed violations, through interview with all levels of staff. At all times, undertakes to bring to the attention of management any actual or potential breaches in security.
- Investigates system access enquiries referred by support staff and all enquiries relating to information security, contingency planning, as they affect the activities of the organisation, function or department. Implements and adopts known techniques to satisfy new access requirements, or provides an effective interface between users and service providers when existing facilities are considered inadequate.
- Recognises requirements for, and creates, auditable records, user documentation and security awareness literature for all services and systems within IT Security Management, ensuring that the records provide a comprehensive history of violations, resolutions and corrective action.
- In consultation with senior security personnel, devises and documents new or revised procedures relating to security control of all IT environments, systems, products or services (including physical security) in order to demonstrate continual improvement in control. Ensures that any system changes required to maintain security are implemented.
- Advises on, and assists with the assessment of the potential impact on existing access security mechanisms of specific planned technical changes, in order to help ensure that potential compromise or weakening of existing security controls is minimised. Also assists in the evaluation, testing and implementation of such changes.
- Drive liaison with customers and stakeholders in order to pursue continual service improvement and produce customer-driven and well-supported services.
- Delivers and contributes to the design and development of specialist IT security education and training to IT and system user

management and staff.

- Manages the operation of appropriate security controls as a production service to business system users.
- Monitors the application and compliance of security operations procedures, and reports on non-compliance.
- Ensures that training, guidance and support is provided to other security administrators, in all aspects of security policy and control.
- Plans and manages the work of small teams of security staff on complex IT security specialism projects.
- Maintains knowledge of the technical specialism at the highest level.
- Keeps in close touch with and contributes to current developments in the technical specialism within employing organisation, own industry and in appropriate professional and trade bodies. Is fluent at articulating best practice and is a recognised authority in the technical specialism.
- Be familiar with relevant University IT-related procedures and policies (acceptable use, data protection, freedom of information, information security, purchasing etc) and advise colleagues and end-users accordingly.
- Undertake various other tasks on an occasional basis at the request of more senior staff in the department, and to a level commensurate with training, knowledge, grade and skills.

*Note: This job description was created in the spirit of the BCS (The Chartered Institute for IT), SFIA (Skills for the Information Age) level 5 with support from the BCS.*

### **Organisational Responsibility**

**Responsible to:** <line manager> but may receive strategic instruction from the Director of IT.

**Responsible for:** None, staff at the senior level may be asked to deputise for their line manager in case of absence.

**Hours:** 37 hours per week, within the hours of 8:00 to 18:00 Mon to Thursday and 8:00 to 17:30 Friday, including 1 hour lunch period.

**The precise pattern of working within these guidelines will be agreed in advance with your manager.**

### **Special Conditions**

Many staff carry mobile phones which allow them to be paged by various systems at all reasonable hours of the week. When monitoring, diagnosis and configuration of services needs to be done outside normal working hours, it can sometimes be appropriate for the work to be carried out remotely at home when convenient.

Attendance on site outside normal working hours is occasionally necessary, for example during major system changes and maintenance. Such out-of-hours working as is necessary is scheduled in negotiation with the group of staff with relevant skills, and takes account of the personal commitments and wishes of individuals.

**For purposes of system management, IT Services staff often have enhanced access to data, files and computer systems and must at all times respect the privacy of information to which they have enhanced access. The only exception to this will be investigations authorised by IT Services Director or his/her nominee.**

**Please note: <organisation> is working towards equal opportunities and observance of our equal opportunities policy will be required.**

### **PERSON SPECIFICATION**

**Job Title:** Senior Information Security Specialist

**Job Grade:** Management and Specialist Grade

**Department:** IT Services

- All staff have a statutory responsibility to take reasonable care of themselves, others and the environment and to prevent harm by their acts or omissions. All staff are therefore required to adhere to the University's Health, Safety and Environmental Policy & Procedures.

|  | Essential   | Desirable  | Stage to be assessed     |
|--|---|--|--------------------------|
| Experience                             | Demonstrated experience in methods and techniques for risk management, business impact analysis, countermeasures and contingency arrangements.  |  | Shortlisting             |
|  |   | Experience of Penetration Testing  | Shortlisting             |
|  | Demonstrates examples of the use of: Principles, practices, tools and techniques of IT auditing.  |  | Interview                |
|  |   | Experience within the HE/ FE sector.   | Shortlisting             |
|  | Experience of software development and code review  |  | Shortlisting & Interview |
|  | Demonstrated success in deploying methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing.  |  | Shortlisting & Interview |
| Skills and abilities                   | Shows aptitude for analysing and managing problems arising from incidents in the operation of information systems, combined with the ability to provide innovative technical solutions. |  | Shortlisting & Interview |
|  |   | Technical background in multiple modern Operating Systems (Windows, Mac OS X, Linux etc) | Shortlisting             |
|  | High levels of technical investigation skills, the ability to research and collate information from a variety of sources into technical reports and recommendations.                    |  | Shortlisting             |
|  |   | Expert skills in the application of forensic techniques.                                 | Shortlisting             |
|  | Demonstrates above average communication skills with an aptitude for dealing with users, colleagues and suppliers.  |  | Interview                |
|  |   | Technical authoring experience and proven documentation track record.                    | Shortlisting & Interview |
|  | Familiar with Methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing.                      |  | Shortlisting & Interview |
|  | Excellent written skills to write technical procedures, reports, system specifications etc.   |  | Shortlisting             |
|  | Excellent time management   |  | Shortlisting             |
|  | Ability to schedule your own workload and prioritise your work.   |  | Interview                |
| Training and Education/ Qualifications | A willingness to undertake further training and to learn and adopt new procedures as and when required.   |  | Interview                |
|  | Ability to assimilate technical information and keep up-to-date in your field.  |  | Shortlisting & Interview |
|  | Degree with relevant IT/Computing content OR relevant professional IT qualifications and/or experience.   |  | Shortlisting             |
|  |   | Information Security related qualifications: CISSP, CISM or similar                      | Shortlisting             |
|  |   | ITIL Foundation training and accreditation.  | Shortlisting             |
| Other                                  | To observe the organisation's Equal Opportunities policy at all times.  |  | Interview                |

**Stages in assessment: Shortlisting, Test (where appropriate) and Interview**

### Conditions of Service

*The appointment will be on a full time, open ended contract on Management and Specialist Grade (salary, discretionary to salary per annum)\* at a starting salary commensurate with experience and qualifications.*

\*The appointment will be subject to the University's normal Terms and Conditions of Employment for Academic and Related staff, details of which can be found at:

<Terms and Conditions Link>

### **Informal Enquiries**

Informal enquiries should be made to <name>, <title> by email at: <email address> or by telephone on <telephone number>.

### **Application**

The closing date for receipt of applications is <insert>.

## Job description template - Information Security Specialist

Job grade Management and Specialist Grade

### Job purpose

- Investigates identified security breaches in accordance with established procedures and recommends any required actions.
- Assists users in defining their access rights and privileges, and administers logical access controls and security systems. Maintains security records and documentation
- Conducts security risk and vulnerability assessments for defined business applications or IT installations in defined areas, and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls (e.g. the key controls defined in ISO/IEC 27001).
- Performs risk and vulnerability assessments, and business impact analysis for medium size information systems. Investigates suspected attacks and manages security incidents.

### Duties and responsibilities

- Conducts security control reviews in well-defined areas. Assesses security of information and infrastructure components. Investigates and assesses risks of network attacks and recommends remedial action.
- Conducts business risk and vulnerability assessments and business impact analysis for well-defined business applications or IT installations.
- Reviews compliance with information security policies and standards. Assesses configurations and security procedures for adherence to legal and regulatory requirements.
- Reviews network usage. Assesses the implications of any unacceptable usage and breaches of privileges or corporate policy. Recommends appropriate action.
- Provides advice and guidance on the application and operation of elementary security controls (e.g. the key controls defined in ISO/IEC 27001) and communicates information assurance issues effectively to users of systems and networks.
- Supervises and/or administers the operation of appropriate security controls (such as physical or logical access controls), as a production service to business system users.
- Investigates suspected attacks and manages security incidents.
- Maintains awareness of the implication of any legislation or other external regulations, which affect security within any defined scope of activity.
- Investigates and reconciles violation reports and logs generated by automated policing mechanisms in accordance with established procedures and security standards. Investigates any other identified security breaches in accordance with established procedures. Interviews minor offenders and compiles reports and recommendations for management follow-up.
- Assists users in defining their needs for new access rights and privileges. Operates and administers logical access controls and directly associated security services relating to all platforms used in order to provide continuous and secure access to information services.
- For all services and systems within IT Security Management, maintains auditable records and user documentation. Assists in the preparation and maintenance of other documentation such as business recovery plans, particularly in the data collection and compilation/production/distribution phases of the exercise.
- Provides advice and handles enquiries relating to other security, contingency planning and related activities.
- Maintains knowledge of the technical specialism.
- Be familiar with relevant University IT-related procedures and policies (acceptable use, data protection, freedom of information, information security, purchasing etc) and advise colleagues and end-users accordingly.
- Undertake various other tasks on an occasional basis at the request of more senior staff in the department, and to a level commensurate with training, knowledge, grade and skills.

*This job description was created in the spirit of the BCS (The Chartered Institute for IT), SFIA (Skills for the Information Age) level 4 with support from the BCS.*

### Organisational Responsibility

**Responsible to:** <line manager> but may receive strategic instruction from the Director of IT.

**Responsible for:** None, staff at the senior level may be asked to deputise for their line manager in case of absence.

**Hours:** 37 hours per week, within the hours of 8:00 to 18:00 Mon to Thursday and 8:00 to 17:30 Friday, including 1 hour lunch period. The precise pattern of working within these guidelines will be agreed in advance with your manager.

## Special Conditions

Many staff carry mobile phones which allow them to be paged by various systems at all reasonable hours of the week. When monitoring, diagnosis and configuration of services needs to be done outside normal working hours, it can sometimes be appropriate for the work to be carried out remotely at home when convenient.

Attendance on site outside normal working hours is occasionally necessary, for example during major system changes and maintenance. Such out-of-hours working as is necessary is scheduled in negotiation with the group of staff with relevant skills, and takes account of the personal commitments and wishes of individuals.

**For purposes of system management, IT Services staff often have enhanced access to data, files and computer systems and must at all times respect the privacy of information to which they have enhanced access. The only exception to this will be investigations authorised by IT Services Director or his/her nominee.**

**Please note: <organisation> is working towards equal opportunities and observance of our equal opportunities policy will be required.**

## PERSON SPECIFICATION

**Job Title:** Information Security Specialist

**Job Grade:** Management and Specialist Grade

**Department:** IT Services

All staff have a statutory responsibility to take reasonable care of themselves, others and the environment and to prevent harm by their acts or omissions. All staff are therefore required to adhere to the University's Health, Safety and Environmental Policy & Procedures.

|                      | Essential  | Desirable   | Stage to be assessed     |
|----------------------|--|---|--------------------------|
| Experience           | Familiar with the concepts of risk management, business impact analysis, countermeasures and contingency arrangements.   |   | Shortlisting             |
|                      |  | Experience in an Information Security role.   | Shortlisting             |
|                      | Familiar with the use of: Principles, practices, tools and techniques of IT auditing.  |   | Interview                |
|                      |  | Experience within the HE/FE sector.   | Shortlisting             |
|                      | Displays a responsible attitude to following procedures, keeping records, and caring for equipment and other assets.   |   | Shortlisting & Interview |
|                      | Demonstrated success in the methods, techniques and standards for writing concise and effective reports.   |   | Shortlisting & Interview |
| Skills and abilities | Shows an analytical and systematic approach to problem solving.  |   | Shortlisting & Interview |
|                      |  | Technical background in at least one modern Operating Systems (Windows, Mac OS X, Linux etc)                  | Shortlisting             |
|                      | High levels of technical investigation skills, the ability to research and collate information from a variety of sources into technical reports and recommendations. |   | Shortlisting             |
|                      |  | Awareness of forensic techniques and/or penetration testing.  | Shortlisting             |
|                      | Good communication skills with an aptitude for dealing with users and colleagues.  |   | Interview                |
|                      |  | Is familiar with the principles and practices involved in development and maintenance and in service delivery | Shortlisting & Interview |
|                      | Familiar with Methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing.   |   | Shortlisting & Interview |
|                      | Good written skills to write technical procedures, reports and documentation.  |   | Shortlisting             |
|                      | Excellent time management  |   | Shortlisting             |
|                      | Ability to schedule your own workload and prioritise your work.  |   | Interview                |

|                                       | Essential   | Desirable   | Stage to be assessed     |
|---------------------------------------|---|---|--------------------------|
| Training and Education/Qualifications | A willingness to undertake further training and to learn and adopt new procedures as and when required. |   | Interview                |
|                                       | Ability to assimilate technical information and keep up-to-date in your field.                          |   | Shortlisting & Interview |
|                                       | Degree with relevant IT/Computing content OR relevant professional IT qualifications and/or experience. |   | Shortlisting             |
|                                       |   | Information Security related qualifications: CISSP, CISM or similar | Shortlisting             |
|                                       |   | ITIL Foundation training and accreditation.                         | Shortlisting             |
| Other                                 | To observe the organisation's Equal Opportunities policy at all times.                                  |   | Interview                |

Stages in assessment: **Shortlisting, Test (where appropriate) and Interview**

### Conditions of Service

The appointment will be on a **full time, open ended** contract on **Management and Specialist Grade (salary, discretionary to salary per annum)\*** at a starting salary commensurate with experience and qualifications.

\*The appointment will be subject to the University's normal Terms and Conditions of Employment for **Academic and Related** staff, details of which can be found at:

[<Terms and Conditions Link>](#)

### Informal Enquiries

Informal enquiries should be made to **<name>**, **<title>** by email at: **<email address>** or by telephone on **<telephone number>**.

### Application

The closing date for receipt of applications is **<insert>**.

## SFIA competencies

The SFIA (Skills Framework for the Information Age) framework from the British Computer Society defines core competencies for a range of IT related disciplines.

The core competencies for information security professionals are listed below:

- Demonstrates extensive knowledge of good security practice covering the physical and logical aspects of information products, systems integrity and confidentiality.
- Has expert knowledge of the employing organisation's security policies and all relevant legislation and industry trends which affect security within the defined scope of authority.
- Exhibits leadership qualities and is persuasive. Is familiar with the principles and practices involved in development and maintenance and in service delivery.
- Has extensive technical understanding and the aptitude to remain up to date with IT security and developments.
- Possesses a comprehensive understanding of the business applications of IT. Is effective and persuasive in both written and oral communication.
- Exhibits a meticulous method of working and attention to detail
- Demonstrates thorough knowledge of good security practice covering the physical and logical aspects of information products, systems integrity and confidentiality.
- Is thoroughly familiar with the employing organisation's security policies and all relevant legislation and industry trends which affect security within the defined scope of authority.
- Has extensive knowledge of the principles and practices involved in development and maintenance and in service delivery.
- Has good technical understanding and the aptitude to remain up to date with IT security and developments.
- Possesses a general understanding of the business applications of IT.
- Is effective and persuasive in both written and oral communication.

## Collaboration between security administrators and academic researchers – UCL, case study

The UCL Security Working Group (SWG) partnered with UCL Human Factors researchers (led by Prof. Angela Sasse) from 2012, consulting regularly to ensure that the expectations of the user-facing password policy within the university were realistically achievable.

Related issues were presented by the SWG, and research expertise was shared by Prof. Sasse's group. Password policy was shared with researchers within the university.

Password policy was considered, but wider options for investment were also explored (such as alternative authentication technologies). After a series of meetings discussing organisation-wide password policies and authentication capabilities, business-driven decisions were presented which served to bound options for refining the password policy. Specific advice was tailored by researchers to match the university infrastructure (e.g. password length and complexity, password renewal intervals), based on research knowledge.

Viable changes were integrated into the password policy, reflecting the outcomes of discussions with researchers. These were discussed further with researchers, identifying potential future directions for investment and changes to policy, as well as challenges which may be faced as the organisation itself changed (in terms of population, available technologies, etc.).

This consultation explored ways to make better use of existing security systems, through communication with on-site researchers with related expertise. Consultation with researchers identified future challenges and informed procurement decisions. The process served to transfer expertise in both directions - researchers gained understanding of the deployment of authentication technologies and related security measures in practice within a large organisation, and SWG expanded understanding of the human factor of security. Both sides then demonstrated additional value to other functions within and outside the university. IT administrators developed a greater appreciation of the principles of human factors in security, and researchers gained insights that informed their research efforts at similar levels with other organisations.

Dialogue with researchers informed and influenced elements of authentication principles and password principles adopted at practitioner meetings. A new password policy developed, and was approved by the university's governance group.

### Key Points

- Organisations can consider how cutting-edge or multi-disciplinary expertise already present within the organisation can be utilised in a way that benefits both security administrators and researchers.
- This case study also highlights that organisations should be aware of changes in the operating environment, and how these influence the bodies of expertise necessary to make informed decisions about policy and procurement.
- This is an example of an organisation actively identifying ways to minimise the impact of core security Responsibilities while maintaining an adequate level of security across the organisation (specifically the creation and management of suitably secure passwords which can be maintained over time by members of the organisation).



# Resources for Chapter 9 – Awareness raising

## RESOURCES

- Raising user awareness of information security – Cardiff University, case study
- Development and use of a phishing exercise to raise awareness of phishing as an issue – Cardiff University, case study

## Raising user awareness of information security - Cardiff University, case study

This case study describes the approach taken by Cardiff University in its attempt to increase and improve user awareness of information security and thus mitigate, to an extent, information security risk.

### The Case

Cardiff University is a member of the Russell Group, a group of 24 leading UK research intensive universities. It is the 12th largest university in the UK in terms of student numbers and features amongst its academic staff two Nobel Prize winners Professor Sir Martin Evans and Professor Robert Huber.

In July 2012 the Information Security Framework (ISF) programme was initiated. The aim of the three year programme was to create a framework by which the University can manage the significant financial and reputational risks involved in collecting, storing and using personal and other data and to assure external stakeholders that the University can be regarded as secure in relation to the way it manages its information/data. The programme considers all aspects of information security, both technological and organisational.

The programme was split into three stages: Foundations, Assessment and Evaluation and Implementation.

### Challenge

The University employs a wide range of individuals carrying out a diverse set of roles. From staff tasked with managing the University estate to academic staff engaged in novel research, delivering education and so on. Engaging with such a diverse audience is not straightforward.

A further challenge when trying to engage individuals with the subject of information security, is the preconception that information security is a concern for the IT department alone, that information security is all about the confidentiality of information and that information security is about stopping people from doing things, creating barriers to using new technology (Cloud Storage for example).

Finding a mechanism for engaging and educating a broad range of individuals then, is the challenge.

### The Study

The below activities cover the primary awareness raising activities delivered by the Information Security Framework Programme between January 2013 and June 2014.

In addition to the below, briefings and updates about the programmes objectives and progress were delivered through a range of regular communication channels: staff meetings in Schools, various departmental briefings, updates in a range of internal publications/newsletters, emails etc.

### Connections

At the outset of the programme an online Information Security Community was created using the Universities online collaborative workspace called 'Connections'. The purpose of this community was to have an area, accessible only to members of staff, where updates about the programme could be posted, key documents shared for comment and review, and to blog about important information security news stories which related to the work of the programme.

### Information Security Risk Assessment Workshops

These workshops were carried out as part of the Assessment and Evaluation phase of the programme in order to identify the most significant risks affecting the University's information assets. Workshops involved academic and professional services staff and on average involved 10 participants. The workshops ran from February 2013 to July 2013 were carried out to assess the risks to each of the Universities information assets. The risks scored as part of the workshops were compiled into formal reports and circulated to participants after the workshop. Participants were subsequently invited to the Connections Community in order that they could continue to engage with the programme. The products of all the workshops, sixteen in total, were consolidated into an Overall Risk Report and used as the basis for identifying suitable control measures which could be delivered through the programme.

Whilst the workshops were not a communications exercise they did serve to create a core of individuals who were aware of the programme and had experienced the chosen risk assessment methodology.

### Survey

In March 2013, the first of an annual, all-staff, information security survey was released. The survey asked staff for their views on a range of information security questions, from how secure they feel the University keeps their data, to what measures they take at home to protect personal computers from which they connect to the University.

The survey was announced in an email to all staff sent in the Vice Chancellors name, it was also advertised via an internal news feed, through the Connections Community, the programmes Operational Group (a cross discipline team with representatives from the Universities Colleges and Professional Services departments) and through various meetings.

The survey attracted an 11% response rate (655 of 6000 staff)

The 2014 survey will ask staff the same questions with the addition of two questions around increasing awareness of information security and importance of information security.

## Teaser campaign

During the initial stages of the implementation phase of the project, one of the key deliverables was an information security website <http://cardiff.ac.uk/isf>.

In order to generate interest in the run up to the launch of the website the concept of a teaser campaign was used. This took the form of a life sized robot (Appendix 1) carrying a sack of data. This decal was installed in buildings across the University campus in areas of high foot fall in order to get staff and students curious about what it was for, so that when subsequent communications and activities took place there was a pre-established interest.

Once the robot had been on display for two working weeks a set of 6 posters (Appendix 2) were deployed across the campus (in both English and Welsh language). Each poster provides advice on a specific information security topic. The topics for the posters being chosen to resonate with issues which affect users both in their personal lives as well as in a University context. To accompany the posters a set of stickers were also distributed across campus (Appendix 3). The stickers consisted of a robot from the posters as well as the URL or the information security website and were located in unexpected areas to catch the eye of passers-by and generate traffic to the website.

## Website

The culmination of the teaser campaign was the launch of the Cardiff University Information Security Website <http://cardiff.ac.uk/isf>.

The website provides information about the ISF programme, advice on a variety of information security topics, a home for the new information security policies generate by the programme, information to assist researchers when completing information security questionnaires as part of research bids, hosts the University Information Classification Scheme and associated handling rules, and a blog for the programme to share information security news.

In the first 3 months the site has received over 1500 unique visitors and 6872 page views with visitors viewing an average of 5 pages per visit.

## Phishing Exercise

During early June 2014 the programme initiated a phishing exercise. An email purporting to be from the University IT department, but sent from a .co.uk domain and containing various other 'give-aways' was distributed to all University staff (some 10,000 email addresses) over a period of 3 weeks. The aim of the exercise being to test susceptibility to phishing and provide a metric for the programme to measure over time. Upon receipt of the phish, the user was prompted to click on a link advertised as taking the user to a site to login using their University credentials and apply for extra network drive capacity. The page which the user is actually taken to <http://sites.cardiff.ac.uk/isf/cardiff-university-phishing-exercise/> provided the user with advice on how they could have identified the email as a phish and how to avoid such scams in the future.

Statistics were generated about both the numbers of staff reporting the email as suspicious through the IT Service Desk as well as numbers of unique visitors to the web page.

## Password Change

Whilst not an awareness raising exercise in itself, the ISF programme has initiated a project to change the University Password Policy. As part of this project the robot from the 'Passwords can be very predictable' poster has been deployed to all University managed workstations as an icon. The icon launches a web browser to the ISF website page describing the changes to the policy.



## Next Steps

### Evaluation

To evaluate the responses to the 2014 information security survey and assess the effectiveness of the programme in changing the levels of awareness of information security and to identify areas for further effort.

### Training

One of the next steps for the programme is the development and roll out of mandatory information security awareness training for all staff and Post Graduate Researchers. This will further communicate to staff the importance of information security awareness but in a more formal setting where there will be enforcement around compliance.

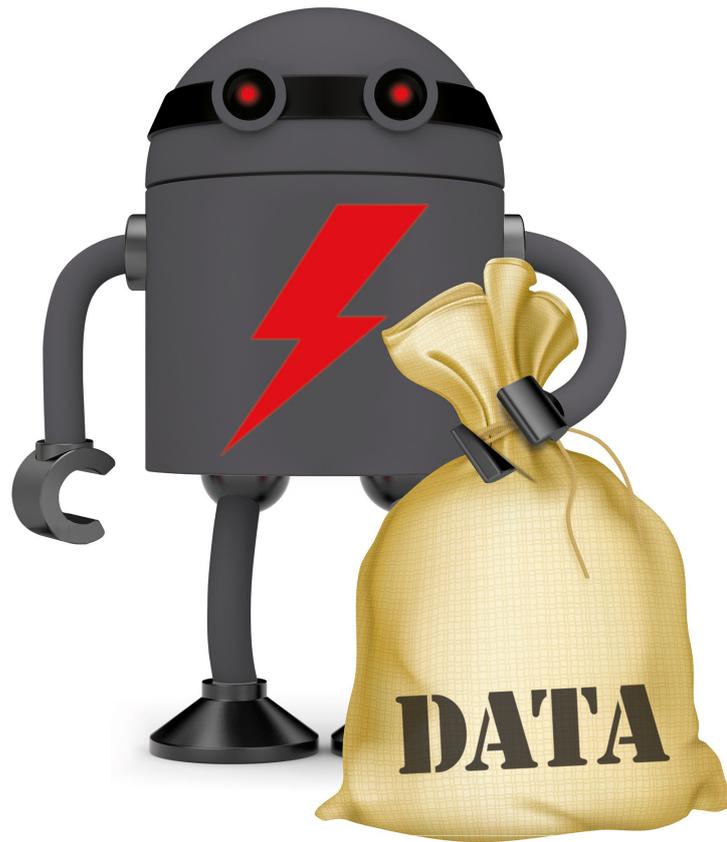
Appendices

Appendix 1 – Dark Robot Decal

Appendix 2 – ISF Posters

Appendix 3 – ISF Example Sticker

Appendix 1 Dark Robot Decal



## Appendix 2 - ISF Posters



Protecting your identity online **is easy**

- Simply...**
- Use firewall protection
  - Use anti-virus protection
  - Use anti-spyware protection
  - Seek help if you see warning signs
  - Update your anti-virus software regularly



For more information visit: [www.cardiff.ac.uk/isf](http://www.cardiff.ac.uk/isf)



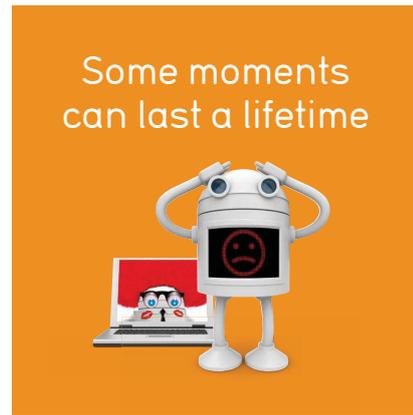
Protecting yourself online **is easy**

In a Phishing scam, a criminal sends you an email message that appears legitimate (e.g. your bank). The message will usually contain a link asking you to 'verify' or 'confirm' your information. This link will take you to a counterfeit website.

- Simply...**
- Delete suspicious messages immediately
  - Never respond to email requests for personal info



For more information visit: [www.cardiff.ac.uk/isf](http://www.cardiff.ac.uk/isf)



Protecting yourself online **is easy**

- Simply...**
- Always check your privacy settings
  - Consider carefully how much personal information you make public online
  - Think before uploading embarrassing pictures



For more information visit: [www.cardiff.ac.uk/isf](http://www.cardiff.ac.uk/isf)

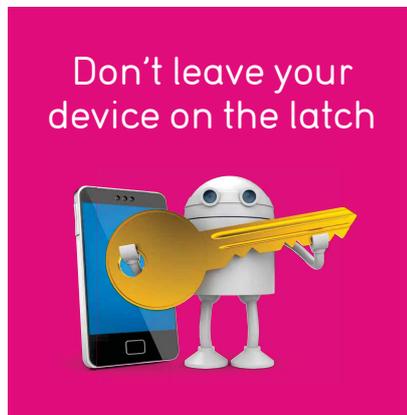


Protecting yourself online **is easy**

- Simply...**
- Use a strong password
  - Use a mix of letters, numbers and symbols
  - Use different passwords for each account
  - Protect your personal data at home and work



For more information visit: [www.cardiff.ac.uk/isf](http://www.cardiff.ac.uk/isf)



Protecting your identity online **is easy**

- Simply...**
- Always lock your device
  - For added security set your device to automatically lock when it goes to sleep
  - An unlocked device leaves access to your data



For more information visit: [www.cardiff.ac.uk/isf](http://www.cardiff.ac.uk/isf)



Protecting your identity online **is easy**

- Simply...**
- Keep your security software up to date
  - Allow automatic updates for security patches
  - Install firewall and anti-virus software
  - Scan external devices (e.g. USB sticks) for viruses



For more information visit: [www.cardiff.ac.uk/isf](http://www.cardiff.ac.uk/isf)

## Appendix 3 - ISF Example Sticker



## Development and use of a phishing exercise to raise awareness of phishing as an issue - Cardiff University, case study

### What is a phish?

Phishing is the name given to the practice of sending emails at random, purporting to come from a genuine organisation. This sort of email attempts to trick the recipient into entering confidential information, such as credit card or bank details, usernames and passwords. The links contained within the message are false, and often re-direct the user to a fake web site.

### Commissioning the exercise

As part of the University wide Information Security Framework programme, and as a method for addressing a specific risk around user awareness of phishing, it was identified that an exercise to raise awareness of phishing would be beneficial.

Authorisation for carrying out the exercise was secured through the Information Security Framework programme Steering Group and communicated to the University Business Change Portfolio Oversight Group. Both bodies include representation from senior Professional Services and Academic members of staff.

### Carrying out the exercise

The exercise consisted of sending all University staff an email which was representative, in terms of the level of sophistication, of the sorts of phishing emails routinely received by University staff.

The email warned recipients that they were running low on storage quota and to follow a link to enter their credentials and apply for extra storage.

The email contained a number of tell-tale signs of being a phish including, spelling mistakes, a non 'ac.uk' originating email address, URGENT markings and an embedded hyperlink taking users to an address different to that which it advertised.

Those recipients who subsequently clicked on the hyperlink were taken to a University hosted 'landing page' (via a redirected web address with a domain matching the one from which the email was sent) which informed them that the email had been a phishing exercise run by the University, provided a reassuring message about the purpose of the exercise, highlighted the tell-tale signs that the email was a phish and provided advice and links to further information on phishing. By using this mechanism targeted education on how to avoid falling for phishing emails was provided to those most likely to fall victim to such attacks.

The email and landing page can be viewed here <http://sites.cardiff.ac.uk/isf/advice/phishing/cardiff-university-phishing-exercise/>

By keeping awareness of the details of the exercise to a limited group (IT Service Desk and Programme Team) it was possible to ensure that the reactions of staff, including the responses of devolved IT staff within Departments and Schools were as they would be had the email been a real phishing attack.

Where individuals contacted the IT Service Desk, or read the content of the landing page they were encouraged to keep their awareness of the exercise to themselves and not warn colleagues.

Unique hits to the landing page were measured using Google Analytics (access to the landing page was only possible through receiving and clicking on the link in the phish).

### Facts and Figures

- Emails were sent over a period of approximately one month to 9001 email addresses at a rate of 500 emails per day.
- A total of 1905 users followed the link in the phishing email which represents 21% of the email recipients.
- A total of 291 calls were placed to the IT Service Desk to report the phish (3.2%)

### Learning Points

- Some staff, particularly those who work in IT, recognised the email was a phish, but chose to click on the link to see what would happen/where it would take them. It was not possible to quantify the number of these 'curiosity clicks' and so they cannot be disaggregated from the results.
- There may be staff who avoided the phish by virtue of not reading the email, in future exercises it may be desirable to be able to send a follow-up or chase email.
- Levels of reporting to the IT Service Desk were relatively low (3.2%) and work is needed to encourage staff to report such threats.
- There was evidence of local reporting mechanisms at School and Department level which are not formally recorded and which may have significantly increased the percentage figure for staff reporting the phish.
- The exercise tests whether users will click on potentially dangerous links, but as an inherent assumption that they would then enter their credentials. As above some staff, in order to investigate how 'good' a phish it was were clicking on the link out of curiosity but would not have entered credentials.

When repeating the exercise in the future, users should be delivered to a screen on which to enter ones credentials, doing so and selecting enter should then deliver the user to the landing page.

### **Next Steps**

- The outcomes of the exercise will be communicated to the University Information Security Review Group.
- The outcomes of the exercise will be publicised across the University to further raise awareness and to flag the advice to those who have not already accessed it through the phishing email.
- A further exercise is to be planned taking on board the learning points.



# Resources for Chapter 10 – Measurement

## RESOURCES

- Evaluating a measurement

## Evaluating a measurement

The organisation should assess any existing or proposed measurement against these qualities to determine which are likely to be most informative. If the answer to any of these questions is “No”, explore other possible measures or look to compensate for shortcomings.

| Is my measure ...                       |   |
|---|---|
| RELIABLE?                               | <p>Can it be consistently measured in a repeatable way?</p> <p>Is it reproducible? If NOT, are there known explanations of sources of uncertainty which are acceptable to all stakeholders (even if they dominate the values)?</p>  |
| SUSTAINABLE?                            | <p>Is it cheap to gather? If it needs to be computed frequently, is the metric’s source data cheap to gather?</p> <p>Can it be quickly evaluated? Are the costs of evaluation low enough that it is useful for those who will use it?</p> <p>Is solid data readily available?</p>   |
| MEASURABLE?                             | <p>Can it be expressed as a cardinal number or percentage?</p> <p>Is there an accepted unit of measure?</p> <p>Can it be accurately measured? If NOT, is the distance between “true” and “real” measurement acceptable to stakeholders?</p> <p>Is it precise enough to be useful?</p> <p>Are measurements current enough to be useful, or time-stamped to a precision that makes them traceable?</p>              |
| OBJECTIVE?                              | <p>Are measurements free of influence from the measurer’s will or personal feeling?</p> <p>Is it unbiased?</p> <p>Can it be determined as being correct in an objective way?</p> <p>Is the process or system for collecting measurements correct according to its specification?</p>  |
| SCOPED?                                 | <p>Is it contextually specific?</p> <p>Is the domain in which it applies clearly defined? Conversely, does it overlap with other measurements?</p> <p>Is it meaningful to stakeholders, and does it reflect the meaning of what it is expected to be measuring?</p> <p>Is it relevant to stakeholders?</p> <p>Is it easy to interpret?</p>  |
| INSTRUMENTABLE?                         | <p>Can it be automated through tool support?</p> <p>Is it sufficiently non-intrusive?</p> <p>Is the measurement process scalable?</p> <p>Is the measurement process portable to other environments?</p> <p>Can the measurement process, and environment being measured, be adequately controlled?</p>   |
| TRANSPARENT?                            | <p>Can it be proved that it actually measures what it is supposed to?</p> <p>Can real evidence be gathered to demonstrate that it meets objectives?</p> <p>Is there an intended audience within or outside the organisation?</p> <p>Can the distance between the specified state (“should be”-state) and the real operational state (“as is”-state) be known?</p> <p>Is it objective, rather than subjective?</p> |
| PROGRESSIVE?<br>(Information Assurance) | <p>Over time, can it demonstrate progression toward a goal?</p> <p>Is it possible to compare a measurement to previous measurements, targets, or benchmarks?</p> <p>Does it relate to a specific business goal?</p> <p>Are targets linked with achievable expectations?</p> <p>Are there stakeholders within the organisation capable of creating, using, and refining it?</p>                                    |

# Resources for Chapter 11 – When things go wrong: non-conformities and incidents

## RESOURCES

- [Developing an Information Security Incident Response Plan based on ISO/IEC 27035:2011 – University of Oxford](#)
- [Example of an information security incident response scheme](#)
- [Information Security Service: Information Security Incident Management Process – UCL](#)
- [Investigations and Data Access Policies – University of York, case study](#)
- [Data breach – case study](#)

# Developing an Information Security Incident Response Plan based on ISO/IEC 27035:2011 – University of Oxford

## Introduction

Information security incidents are, one way or another, inevitable but the response to an incident can still reduce the overall risk to an organisation by way of reducing the impact of any given incident. The key to good incident management is good communication and ensuring all stakeholders are aware of their roles and responsibilities. In order to achieve this, roles, responsibilities procedures and protocols need to be defined, agreed and tested. ISO/IEC 27035:2011 Information Technology – Security techniques – Information security incident management provides the outline of one method for implementing an incident response scheme and this study documents some of the applications and lessons learned from following such an approach in a University setting.

## Motivation for Developing an Incident Response Plan

Having a formal incident response plan can help to ensure that an organisation is well informed of the current threat landscape and risks. This can be particularly important in devolved environments such as Universities where individual units may handle incident response well in isolation. Where there is no overall coordination, formal escalation or reporting of security incidents it is unlikely that lessons learned will be followed up and acted upon or shared with other relevant parts of the organisation. Similarly if incidents are escalated to senior members of an organisation it is important that those senior stakeholders understand the information they are being presented with, why they are being informed and what action they need to take. The goals of an incident response plan are therefore to ensure that:

- Incidents are detected and reported in a timely manner
- Incidents are properly investigated and handled efficiently and effectively
- The impact of incidents is minimized and action taken to prevent further damage
- Incidents are communicated appropriately and appropriate levels of University management are involved in the response
- External bodies or data subjects are informed as required
- Evidence is gathered, recorded and maintained appropriately
- Details of incidents are recorded and documented
- Incidents are reviewed and subsequent improvements made to policies and procedures

## Observations and lessons learned

Policy and Governance It is critical to the success of an incident response plan to be ratified and signed off at a senior level within the organisation. Typically this will be a senior information security board or other senior committee that owns information security risk. An incident response policy should first be agreed so that it is clear what the intentions of the plan are and in order that progress (and problems) can be monitored and measured. Although the policy and plan will be owned by a senior board it should be made accessible and communicated to all departments within the organisation.

## Incident Detection/Reporting

Clear guidance needs to be given on when to report incidents, what to report, how and to whom. Many incidents may not be reported centrally either because they are not recognised as security incidents or because policy and/or process for reporting has not been widely communicated and understood. As a result the number and type of incidents dealt with across an organisation will not tell the whole story, hampering informed decision making based on a true understanding of risk.

The definition of a security incident may need to be reviewed. Typically IT security related incidents have been dealt with in isolation but, with a general move towards greater focus and maturity in information security, it is now necessary to expand the definition of an incident to include breaches of information security regardless of the format. It is, however, important to clearly define when events become incidents and should be reported. To this end guidance should be produced for individual departments to understand clearly what types of incident need to be reported and how. For example ongoing incidents may need to be reported immediately as assistance or escalation is required (e.g. compromised server, stolen laptop with personal data). Other incidents might only be useful for statistical purposes and they can be reported periodically (e.g. number of malware infections dealt with by a department in the past month).

Whether an incident should be reported immediately will depend on the potential impact on the organisation as a whole. Therefore criteria should be agreed in advance with senior stakeholders and appropriate guidance should be provided to local departments. Incidents should be reported within departments or sections initially and the guidance should be used to make a decision as to whether to report centrally. A single point of contact should be provided for reporting centrally and, ideally, will be made use of by specific departmental liaisons. However it should be recognised that incidents will be reported to alternative contacts. It is therefore important to ensure that staff within departments (particularly those providing central services) are aware of where to forward incident reports.

## Communication, Coordination and Escalation

Incidents should be communicated and handled efficiently. This requires all stakeholders in incident response to be identified, informed in a

timely manner and be aware of their responsibilities. Where an incident will (or may) have an adverse impact on an organisation's primary assets then senior members of the organisation should be made aware, as soon as is practicable, in such a way as to make it clear what the impact of an incident is (or might be) and what is required of them. This may be simply for information purposes (e.g. to warn of potential impact) or to require some intervention, backing or ruling on reactive measures. Particularly in a devolved environment, tensions often arise between incident handlers and service providers. The owner of a website used (for example) for receiving job applications will be particularly keen to get the site up and running again quickly, whilst the incident handler will not be happy to restore the site until the vulnerability has been identified and fixed. Where such tensions arise it is extremely useful to have the backing of senior stakeholders within the organisation and/or allow senior stakeholders to make informed decisions on corrective actions based on the risk vs. the impact to the business.

A clear and concise format for escalation reports should be agreed upon in advance. Escalation reports might (for example) include the current impact, potential impact and how likely that is, as well as any specific action required of anyone receiving the reports. This will lead to far fewer queries when escalating incidents thus considerably improve efficiency and speed of communication.

Responding to incidents often requires coordination amongst different business functions. Depending on the nature of the incident this could include physical security services, legal services, data protection offices, the press office etc. Having a small core of initial incident responders and senior stakeholders will mean that the right people are immediately informed of incidents and may bring other stakeholders in (such as legal services and the press office) as required. Ensuring the incident response and escalation team include senior stakeholders representative of the organisation will help to ensure that appropriate backing is received when dealing with incidents. To ensure that stakeholders are fully aware of mitigating actions that are taken regular updates (particularly changes in status) should therefore be communicated to the immediate response team.

## Classifying and Categorisation

In order to ensure that senior stakeholders get the information they require and, are appropriately informed about incidents, it is important to ensure those stakeholders agree in advance the circumstances under which they should be informed. Generally this means categorising incidents in terms of their nature and impact and so impact criteria should be defined and agreed. So as not to create overly complex and new impact criteria it is useful to use existing criteria where possible – for example using criteria for risk assessment. The number of overall incident classifications (e.g. Major, Moderate, Minor) should also be kept to a minimum (similarly to information classification schemes).

It is also worth noting that the criteria used for escalation of incidents is primarily used as a tool by initial incident responders but is aimed at senior stakeholders. In other words incident responders tend to be experienced and know when something should be escalated. The impact criteria can therefore be seen as a means for initial incident responders to explain why an incident has been escalated. If the criteria are not useful for incident responders in this way they should be revised.

## Roles and responsibilities

All members of the incident handling team should understand their roles and responsibilities, which should include providing appropriate support and leadership in dealing with incidents. Having these agreed in advance is, again, advantageous though specific roles and actions may need to be assigned throughout the incident lifecycle. For example, incidents should have a designated incident owner who is responsible for making executive decisions and providing senior support for a given incident. This person should be authorised and readily available throughout the duration of the incident so as to avoid unnecessary delays in resolving incidents.

It is particularly beneficial to understand and agree the responsibilities of initial incident handlers, particularly in terms of ascertaining the right level of information in order to make an informed decision as to the potential impact of an incident and maximise efficiency when incidents are escalated. For example, agreeing in advance with the data protection officer the questions that need to be asked in terms of the level of personal data involved in a breach means that the initial incident handler can complete the triage stage. This allows stakeholders, such as the data protection officer, to make quicker, informed decisions and reduces the amount of correspondence and communication channels required. Incidents involving personal data (or potentially involving personal data) are now dealt with much more efficiently.

## Summary of main lessons learned

- Having an incident response plan improves the efficiency of handling major incidents and leads to a more coordinated, university-wide approach.
- Policies for incident response should be agreed in advance and signed off by senior management as should subsequent processes in the scheme
- The plan should be simple to follow.
- Criteria for escalation and reporting should be agreed with senior stakeholders in advance.
- Roles and responsibilities of stakeholders should be agreed in advance.
- Good communication of incidents means that senior stakeholders are informed quickly and understand the impact of security incidents
- Specific incident owners should be explicitly assigned for each incident
- An appropriate governance structure is required in order to present reports on incidents, findings, vulnerabilities and risks
- All university members should understand what they should report and how they should report it.

## Example of an information security incident response scheme

### Introduction

The purpose of this scheme is to provide detailed documentation describing the policies activities and procedures for dealing with information security events and incidents. The scheme includes definitions of information security events and incidents and should be used as a guide for:

- responding to information security events
- determining whether an event becomes an incident
- detecting and reporting information security events/incidents
- classifying information security incidents
- response to, and escalation of, information security incidents
- roles and responsibilities for dealing with information security incidents
- identifying lessons learnt and making improvements

### Information Security Incident Management Policy

#### Scope

This policy forms part of the information security management framework and supplements the University's information security policy. It applies to events and incidents affecting any University information assets or information system. It applies to and will be communicated to all those with access to University information systems, including staff, students, visitors and contractors.

#### Objective

The University recognizes the importance of, and is committed to, effective information security incident management in order to help protect the confidentiality and integrity of its information assets, availability of its information systems and services, safeguard the reputation of the University and fulfil its legal and regulatory obligations.

The University will ensure that:

- Incidents are detected and reported in a timely manner
- Incidents are properly investigated and handled efficiently and effectively
- Incidents are communicated appropriately and appropriate levels of University management are involved in the response
- The impact of incidents is minimized and action taken to prevent further damage
- Incidents are reviewed and subsequent improvements made to policies and procedures
- Evidence is gathered, recorded and maintained appropriately
- Incidents are recorded and documented
- External bodies or data subjects are informed as required

#### Policy

1. Information systems which are known to be (or suspected of being) compromised will be isolated from the University network until the incident has been investigated, resolved and risks sufficiently reduced.
2. Guidance and procedures for the detection, assessment, communication, reporting and escalation of security vulnerabilities, events and incidents will be provided via the information security website, training programs and other communication channels.
3. All information security incidents must be reported via the appropriate management channels.
4. Responsibilities for the reporting and escalation of security vulnerabilities, events and incidents should be clearly defined and communicated to all relevant personnel.
5. Security events and incidents should be assessed according to the event/incident classification scale provided via the information security toolkit and, where necessary, escalated accordingly.
6. An information security incident response team (or teams) comprising representatives from all relevant parts of the University, shall coordinate the management of and response to incidents which require escalation in accordance with an Information Security Incident Response Plan.
7. Incidents involving personal data will be reported to the Data Protection Officer.
8. Incidents which involve personal safety, security or require the involvement of law enforcement will be reported to the head of physical security.

9. Details of the Information Security Incident Response Plan will be made available via the information security website.
10. All information security incidents will be recorded for later analysis.
11. Post incident reviews will be carried out in order to identify where improvements in policies, procedures and information security controls can be made.
12. The types, volumes and impact of security incidents will be recorded and reviewed and summary reports will be used as input to the University's information security risk register.
13. Specific incident reports will be reviewed by the Information Security Working Group who may advise on corrective action in the future.
14. Information security incident procedures will be communicated to all relevant personnel and tested periodically.
15. Technical support and guidance will be provided by the IT department.

### **Information Security Incident Response Team (ISIRT)**

The ISIRT refers to the group of people who will be the first responders for information security incidents and will act as the point of contact for information security incidents. The ISIRT will be responsible for the initial response, mitigation and (where appropriate) escalation of information security incidents. The roles and responsibilities for the ISIRT are as follows:

### **Computer Security and Incident Response Team (CSIRT)**

The CSIRT are responsible for:

- Monitoring network traffic to identify compromised or potentially compromised systems within the University network;
- Receiving internal and external reports on compromised systems;
- Protecting the security and integrity of the University backbone network and its core ;information systems and services by blocking network access to any compromised machine;
- Informing and liaising with local IT staff to ensure that computer security incidents are dealt with promptly and effectively;
- Ensuring that compromised systems are fully cleaned and patched against known vulnerabilities, or the risk otherwise mitigated, before being reconnected to the network;
- For providing advice and guidance on dealing with computer and network security;
- Maintaining a register of computer security incidents;
- Initial investigation into the type and quantity of personal (or otherwise confidential) data involved in a compromise;
- Appropriate escalation of computer security incidents in accordance with the information security incident management scheme/ plan.

### **Information Security Officer**

The Information Security Officer is responsible for:

- Coordination of the ISIRT with regards incident response
- The maintenance and communication of the incident response policy and scheme;
- Creating, maintaining and communicating the information security incident response scheme, incident classification scale and other relevant procedures and guidance;
- Coordination of University-wide responses to information security incidents via the crisis/escalation team;
- Receiving reports on information security incidents and breaches of the information security policy;
- Appropriate escalation of information security incidents in accordance with the information security incident management scheme/plan;
- Reporting incidents involving personal data to the Data Protection Officer.
- Reporting of incidents to other appropriate bodies in a timely manner;
- Maintaining and updating the information security risk register to reflect recorded incidents;
- Writing and presenting appropriate incident reports to the Information Security Working Group and information systems/risk owners and including recommended remediations and lessons learnt.

### **Crisis/Escalation Team**

Some incidents will require escalation above the ISIRT in order that senior management within the University are made aware of, and may respond accordingly, to serious and potentially serious information security incidents. The Crisis/Escalation Team consists of senior members of relevant University departments. Not all members of the Crisis/Escalation Team will need to be alerted to all information

security incidents immediately. The classification scheme and requirements for escalation set out below will be used by the ISIRT to determine when the various parts of the Crisis/Escalation Team will be called into action.

The Crisis/Escalation Team will be made up of a core set of senior staff and will therefore consist of (e.g.):

- Director of IT Risk Management
- Data Protection Officer
- Head of Compliance
- CIO
- The head of physical security

Additionally other key stakeholders will need to be informed, consulted and respond as appropriate. It will be the responsibility of the core Crisis/Escalation Team to report to relevant stakeholders and increase the crisis team appropriately. These stakeholders include but are not limited to:

- Press Office
- The Registrar
- HR
- Legal Services Office

## **Roles and Responsibilities for the Crisis/Escalation Team**

The roles and responsibilities for the Crisis/Escalation Team are as follows:

### **Director of IT Risk Management**

The Director of IT Risk Management is specifically responsible for:

- Authorizing corrective actions to be taken by the ISIRT.
- Overseeing, measuring and monitoring the performance of the ISIRT and incident response scheme.
- Providing senior support and seeking sufficient resource in order to successfully implement and maintain the incident response scheme
- Ensuring incidents are escalated appropriately to other members of the crisis/escalation team.
- Leading the coordination and response of the crisis/escalation team.

### **Data Protection Officer Responsibilities**

The University's Data Protection Officer is responsible for:

- Receiving reports of known and potential data protection breaches
- Initiating and leading investigations into suspected or known data protection breaches
- Ensuring that information security breaches received directly are reported to the information security team
- Appropriate escalation of information security incidents in accordance with the information security incident management scheme/plan.
- Decisions to report and subsequent reporting of data protection incidents to the Information Commissioner
- Communication to relevant staff of correspondence with the Information Commissioner

### **Head of Compliance**

- Receiving reports of incidents that have been escalated and confirming the classification of those incidents
- Ensuring that the Registrar, Press Office, Legal Services, HR and any other relevant senior stakeholders are fully informed and updated on the progression of incidents as appropriate
- Providing senior management support for the incident response scheme

### **CIO**

- Receiving reports of incidents that have been escalated and confirming the classification of those incidents
- Advising on and authorizing mitigating actions and responses that either have a direct or indirect effect on the IT department, or that the IT department will implement but may have considerable implications for other departments and/or the University
- Providing senior management support for the ISIRT and the incident response scheme.

## The Head of Physical Security

- Receiving reports of incidents that have been escalated
- Decisions to report information security incidents to law enforcement
- Reporting and liaising with law enforcement
- Responding to physical security issues as a result of information security incidents

## Reporting and Escalation of Information Security Incidents

### Information security events and incidents

For the purposes of the University's information security incident response scheme:

**Information security events** are described as:

Identified occurrences of systems, services or networks that have the potential to breach information security policies

**Information security incidents** are described as:

A single or series of unwanted events that compromise (or are likely to compromise) the confidentiality, integrity or availability of University data and/or breach University information security policies

Some examples of information security events and incidents can be found below:

| Information security events                  | Information security incidents                   |
|--|--|
| Network scanning                             | Lost or stolen laptops or mobile devices         |
| Brute force attempts/multiple login attempts | Server compromises                               |
| Unsuccessful SQL injection attacks           | Botnet infections                                |
|  | Successful SQL (or other code) injection attacks |
|  | Compromised accounts (e.g. accounts spamming)    |
|  | Denial of Service attacks                        |
|  | Unauthorised access to information systems       |

### Reporting Security Incidents

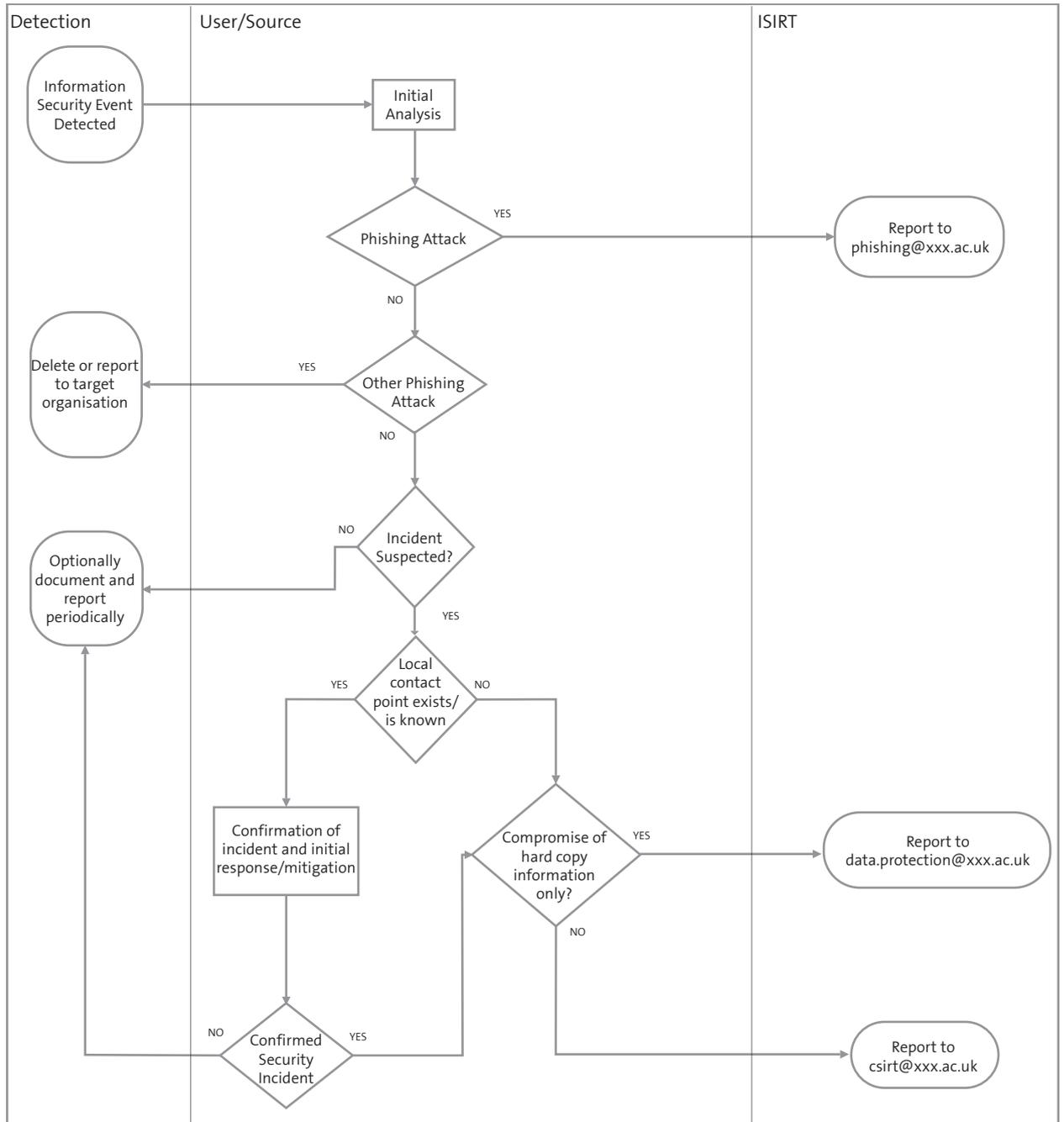
Reporting information security events and incidents can be important for information purposes (e.g. as an input into risk assessment) and/or in order to limit the impact of an incident. The purpose of this section is to provide information on what should be reported, when and to whom.

Information security **events** need not be reported immediately but **may** be reported periodically for information purposes. Usually information security events will be recorded automatically in log files relating to IT systems. These can be reported, by local IT support staff either manually or automatically. Other information security events should be reported to a local point of contact or via line managers who will decide whether to pass on the reports. No response should be expected to reports of information security events unless specific problems are identified.

All information security **incidents** must be reported. The University operates a devolved model for support when it comes to IT and information security, therefore users should usually report security incidents to identified local contacts. If there is any doubt then incidents should be reported to a user's direct line manager who will be responsible for deciding whether further action and/or reporting is required. Information security incidents should then be reported according to the initial incident reporting protocol described below.

## Initial Incident Reporting Protocol

Information security incidents should be reported according to the following protocol:



## Central Incident Response and Escalation

The ISIRT will be responsible for initial incident handling including investigation, initial response and classification of the incident in accordance with the classification scheme described in appendix A.

Initial incident handling will typically be handled by the CSIRT in accordance with their standard processes and practices. Additionally the CSIRT will make standard enquiries into the level of personal (or otherwise confidential) data that may have been exposed as a result of any incident. For the purposes of personal data details are given in Appendix B as to the information required by the Data Protection Officer.

The incident classification scheme will be used in the first instance for determining whether incidents should be escalated to other members of senior management throughout the University. Clearly the full impact of an incident will not be known at the time of initial response. The full impact will therefore be assessed in separate reporting and review of incidents at a later date. This information can be used to assess how appropriate the escalation process was based on the classification at the time. Incidents will be escalated based on their current impact. In order that incidents are escalated appropriately therefore the classification scheme needs to take into account the potential impact. This is reflected by including “importance of information system” in the classification scheme. Incidents affecting important or critical information systems will therefore always create a higher level of alert.

In order to provide senior staff within the escalation team the information they require in order to determine what (if any) action is required, incidents escalation reports will include the following information:

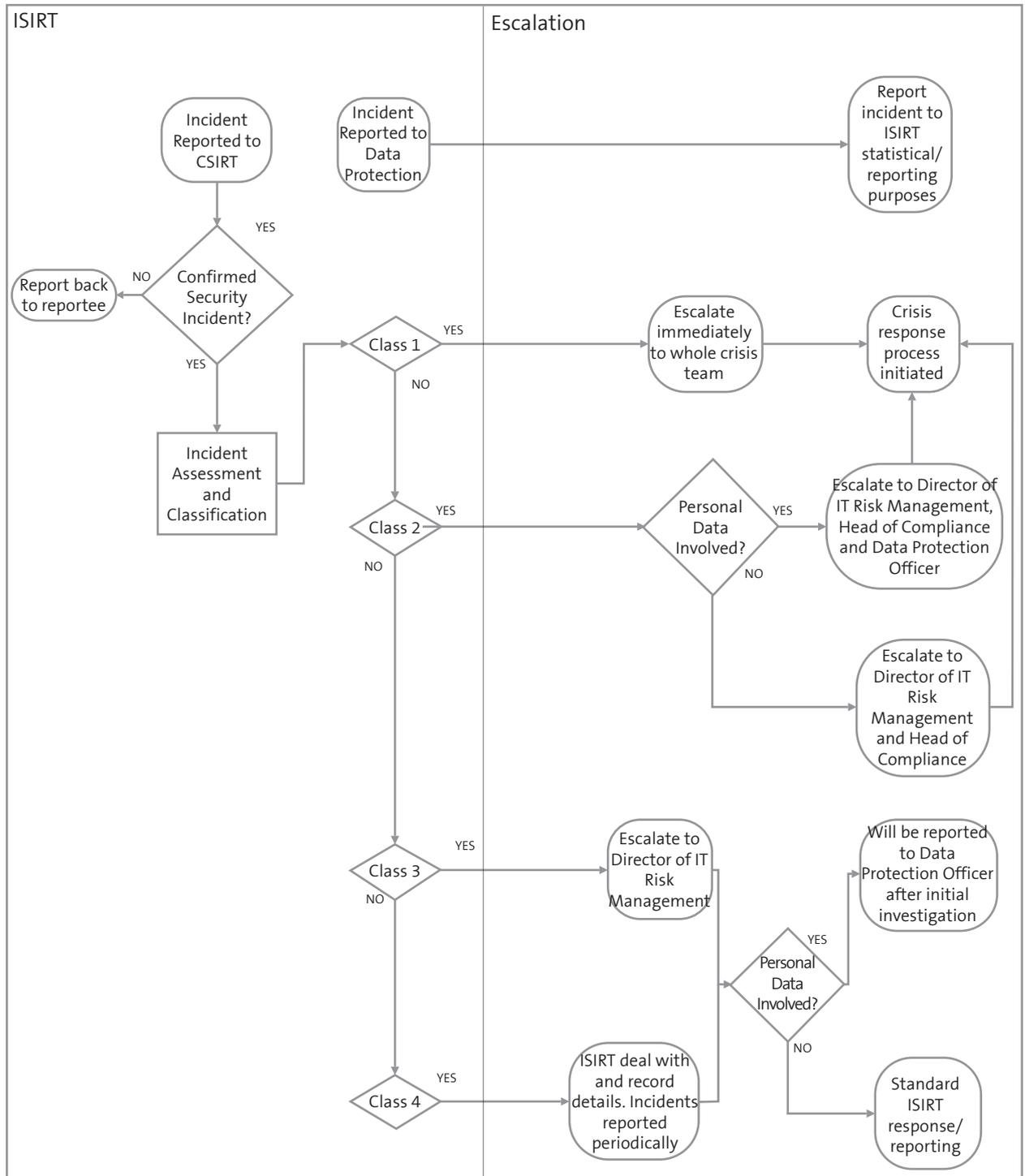
- Suspected date/time of incident
- Detection date/time
- Method of detection
- Incident category
- Current incident classification
- Basis for current classification
- Current status of investigation
- Current mitigating actions
- Potential incident classification
- Basis for potential incident classification (i.e. impact category)
- Estimate of actions/events that may lead to potential classification/impact
- Estimate of likelihood of potential classification/impact
- Notes and/or specific actions required of the Crisis/Escalation team

Updates to the status of an incident will be provided by the ISIRT either in accordance with the Crises/Escalation process described below or when the current classification of an incident changes (i.e. based on the current impact).

Further details on the process involved in escalating incidents according to the classification scheme can be found in Appendix C.

## Incident Escalation Protocol

Incidents will be escalated by the ISIRT in accordance with the protocol described below:



## Crisis/Escalation Process

When information security incidents are escalated one person should take overall responsibility for coordinating the crisis response. It is assumed that this will be the Director of IT Risk Management unless explicitly stated for a particular incident. The lead coordinator will be responsible for ensuring the ISIRT provide updates as appropriate and will be responsible for overseeing and authorizing responsive action (including meetings of the response team), further escalation and eventually resolution of the incident. All members of the crisis response team have their responsibilities outlined above and are responsible for requesting relevant information for their area of responsibility.

## Reporting of Information Security Incidents

All information security incidents will be reported at Information Security Working Group meetings and it is the responsibility of the Information Security Officer to ensure that incidents are presented and reported appropriately to this group. Class 3 and Class 4 incidents will be reported statistically to the IS Working Group noting any particular concerns or trends. Class 1 and Class 2 incidents will be reviewed in more detail noting the eventual impact and any lessons learned. Further details are presented in Appendix C.

## Appendix A: Classification of Information Security Events/ Incidents

### Incident Category

The following table provides categories and descriptions for various incident types:

| Category                                 | Description   | Examples   |
|--|---|--|
| Malware incident/<br>Malicious Code      | Incidents primarily concerning malware infections or outbreaks.   | Viruses, worms, Trojans, botnets, APTs, infostealer infections.  |
| Technical Attack/<br>Unauthorised Access | Network attacks and attacks exploiting software vulnerabilities to execute code.                            | Network scanning, exploitation of vulnerability, backdoors, brute force attacks, SQL injection attacks, unauthorized elevation of privileges, buffer overflows, defacements, phishing                        |
| Denial of Service                        | Deliberate and accidental DoS attacks   | DDoS and DoS attacks, electromagnetic radiation, jamming etc.  |
| Technical Failure                        | Failures and faults in systems, infrastructure and services that support the running of information systems | Hardware failures, software failures, power failures, networking failures, air conditioning failures etc.  |
| AUP Breach                               | Deliberate or accidental breaches of policies, regulations and/or laws                                      | Unauthorised use of resources, copyright infringement, misconfiguration of devices, abuse of privileges, forging of rights   |
| Physical compromise of information       | Deliberate or accidental compromise of confidentiality, integrity, availability etc                         | Loss/theft of devices such as laptops, tablets, phones etc; Compromise of hard copy data such as Loss of documents (e.g. sent via post), theft of documents, transmission to wrong recipient (e.g. via fax). |
| Physical Damage                          | Deliberate or accidental physical events  | Flood, wind, lightning, fire, theft loss, vandalism etc.   |
| Other incidents                          | Catch all for not categorised   |  |

### Impact Categories

All incidents will be categorized according to their impact. The impact will be either CRITICAL, MAJOR, MODERATE or MINOR based on the impact categories below. The greatest impact from the five different types of impact will determine the impact category assigned to an incident. When incidents are reported the current and potential impact should be reported along with some indication of how likely escalation may be (or what would need to happen for the potential impact to be realized)

## Importance of Information System

| Category | Description   | Examples   |
|----------|---|--|
| Critical | Business-critical systems fundamental to the daily operations of the University supporting teaching, learning, research or the administration of the University. Compromise of a critical system would cause significant disruption or reputational damage to the University. 'Significant' in this context is defined as impacting the operations of multiple University departments; the disruption may be more significant at certain times of the year. | Email systems; Financials systems; Core Infrastructure systems (such as routers, DNS); Primary University Web Server |
| Major    | <b>EITHER</b><br>A system that is critical to the operations of a single department but may also impact other departments. Loss of a Major system would cause significant disruption to the affected department and may cause inconvenience to other departments.<br><br><b>OR</b><br>A system that supports multiple departments but is not business-critical. Loss of a Major system would cause inconvenience to multiple departments.                   | Departmental directory server; Main departmental web servers;  |
| Moderate | A system that supports services internal to individual departments. Loss of a moderate service would cause inconvenience to the department in question.   | Departmental web servers;  |
| Minor    | All other systems   | Desktops; Laptops; Mobile devices  |

## Service impact

| Category | Description  | Examples   |
|----------|--|--|
| Critical | University is no longer able to provide some core services to any users.   | Central Email service is unavailable; Backbone network connectivity is lost or significantly impaired. |
| Major    | <b>University is unable to provide a core service to a subset of users</b>   | Central email relays blacklisted for certain emails  |
| Moderate | University is able to provide core services to users but secondary services may be unavailable and/or services may be impaired for a period of time. |  |
| Minor    | No effect on the University's ability to provide core services to users.   |  |

## Privacy Impact

| Category | Description   | Examples   |
|----------|---|--|
| Critical | <b>EITHER</b><br>A potential or known breach of confidentiality where the release of data could cause a significant risk of individuals suffering substantial detriment, including substantial distress<br><br><b>OR</b><br>Exposure of personal data of 10000+ users | Unauthorised access to/disclosure of sensitive personal data such as medical records or individuals working on animal research |
| Major    | <b>EITHER</b><br>A potential or known breach of confidentiality where the release of data could cause a risk of individuals suffering substantial detriment, including substantial distress<br><br><b>OR</b><br>Exposure of personal data of 1000 – 10000 users       | Unauthorised access to/disclosure of application data  |
| Moderate | Exposure of limited personal data affecting 100 – 1000 users  | List of user details (such as names and addresses) exposed (e.g. access to the Global Address List)                            |
| Minor    | Exposure of limited personal data affecting < 100 users.  | Unauthorised access to system containing limited, non-private information (e.g. usernames or email addresses.)                 |

## Financial Impact

| Category | Description                              | Examples  |
|----------|--|---|
| Critical | Financial loss or impact exceeding £1m.  | Example of financial impact could include fines or charges levied (e.g. non PCI compliance), loss of grant/funding income, cost of replacing systems, insurance premiums etc. |
| Major    | Financial loss or impact of £100k - £1m. |   |
| Moderate | Financial loss or impact of £20k - £100k |   |
| Minor    | Financial impact of < £20k               |   |

## Reputational Impact

| Category | Description  | Examples   |
|----------|--|--|
| Critical | EITHER sustained or ongoing negative national media publicity OR a negative change across all national or international HE sector rankings                   | Significant data breach, compromise or unavailability of critical University system; Compromise of major and/or sensitive research project |
| Major    | EITHER one-off negative national, or ongoing local, media publicity OR a negative change across the majority of national or international HE sector rankings | Compromise of non-critical but high-profile system   |
| Moderate | EITHER negative media publicity likely, but avoidable or controllable with management OR a negative view of individual departments at Council level          | Loss or theft of unencrypted laptops containing confidential information.  |
| Minor    | Negative view limited to within a department   | Incident affecting limited number of users within a single department.   |

## Incident classification

Having been assigned an overall category and given an impact score, incidents will then be classified according to the following criteria:

|                     |   |
|---------------------|---|
| Emergency (Class 1) | Critical information system is affected<br><b>AND</b><br>Results in critical business, financial, reputational or information impact.   |
| Critical (Class 2)  | Critical or major information system is affected <b>AND</b> results in Major business, financial, reputational or information impact;<br><b>OR</b><br>Results in critical business, financial or reputational impact.             |
| Major (Class 3)     | Major or moderate information system is affected <b>AND</b> results in moderate business, financial, reputational or information impact;<br><b>OR</b><br>Results in Major business, financial, reputational or information impact |
| Minor (Class 4)     | Moderate or minor information systems affected <b>AND</b> results in minor business, financial, reputational or information impact;<br><b>OR</b><br>Results in Moderate business, financial, reputational impact                  |

## Appendix B: Information required by the Data Protection Officer for incidents involving personal data

The following questions will be used as the basis for investigating information security incidents involving personal data. This reflects the information that the Data Protection Officer will need to ascertain in order to make a decision on whether to pursue the incident and potentially report to the Information Commissioner's Office.

1. What is the full range of data exposed
2. What is the nature of the data (personal, sensitive personal etc.)
3. What is the quantity/volume/number of users affected
4. What is the evidence of data having been being exposed and what is the nature of the exposure (i.e. data already in the public domain, data exposed but unlikely to be the target of the attack/incident etc.)
5. For how long has the data been stored/kept
6. Is the data still current i.e. for how long should it have been stored/kept
7. What measures were in place to protect the data
8. Have any complaints been received
9. Was the attack specifically targeted/what was the likely motivation of the attack
10. What was the cause/vulnerability
11. What measures have been put in place to mitigate

## Appendix C: Escalation and Reporting of Incidents

**Class 4** incidents usually require no escalation. Records of the incident will be maintained for statistical purposes by the ISIRT. Where appropriate further investigations will take place by the ISIRT team to ascertain whether the incident needs to be escalated and/or the extent to which personal (or otherwise confidential) data is involved. Where personal data is involved a report will be provided to the Data Protection Officer

Statistics of all Class 4 incidents will be reported at ISAG meetings.

**Class 3** incidents will be escalated to the the Director of IT Risk Management who will make a judgement as to whether further investigation is required. Incidents will normally not need to be escalated immediately but the Director of IT Risk management will ultimately be informed of all such incidents. Where personal information is involved the ISIRT will carry out initial investigations into the nature and extent of the information and the exposure, before sending a report of the incident to the Data Protection Officer.

Statistics of all Class 3 incidents will be reported at Information Security Working Group meetings.

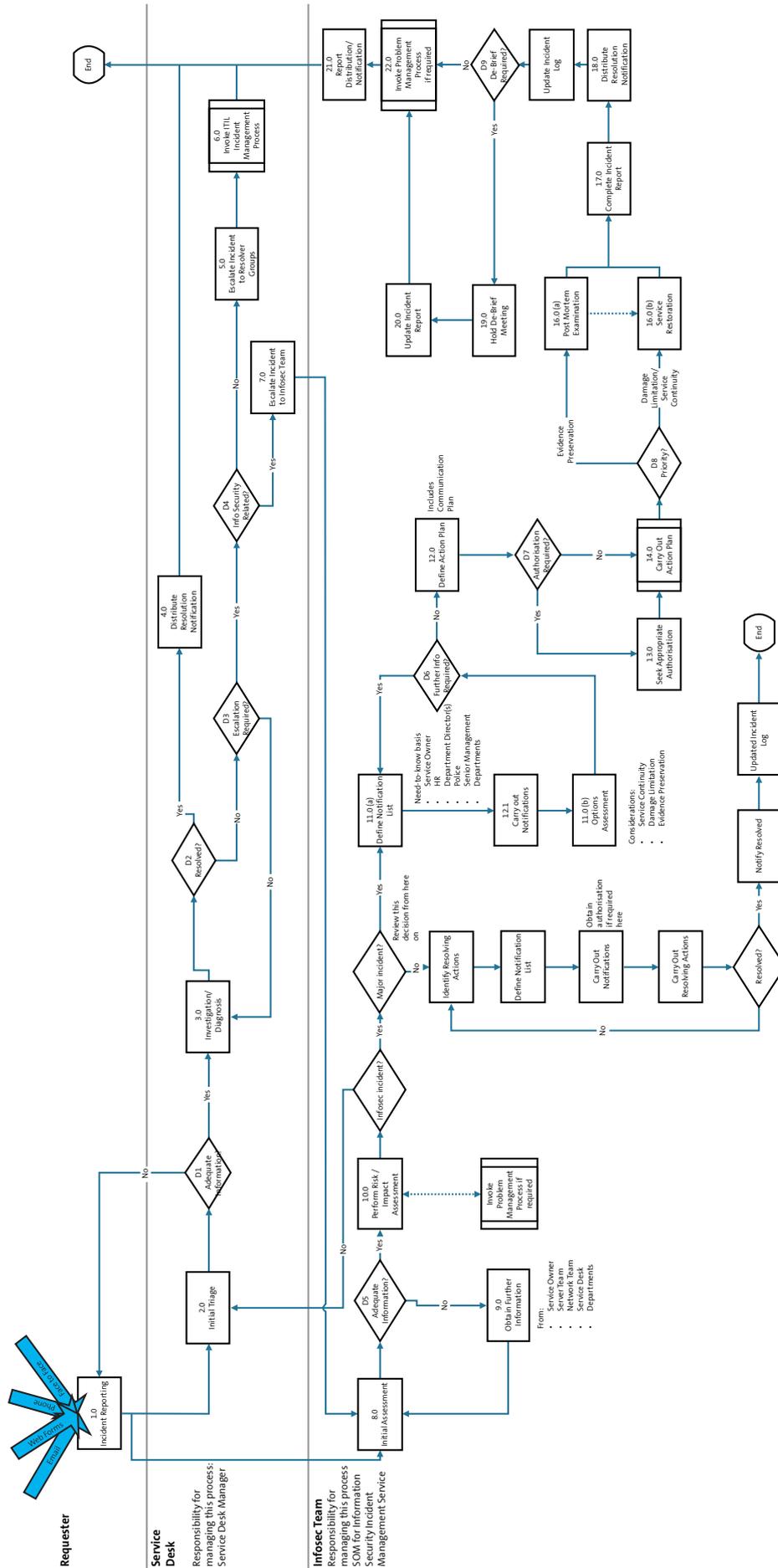
**Class 2** incidents will be escalated immediately to the Director of IT Risk Management and Head, Head of Compliance and, where personal data is potentially involved, the Data Protection Officer. The ISIRT will still usually be responsible for the initial investigations into the nature and extent of exposure of any personal information but the Data Protection Officer will likely be involved in all communications.

Class 2 incidents, including their handling, eventual impact and lessons learned, will be reviewed at ISAG meetings.

**Class 1** incidents will be escalated immediately to the whole crisis/escalation team. The CIO, Head of Compliance and Director of IT Risk Management will be responsible for coordinating the response to such incidents, ensuring sufficient resources are allocated to dealing with the incident and for keeping senior stakeholders (such as the Registrar) fully informed.

Class 1 incidents, including their handling, eventual impact and lessons learned, will be reviewed at Information Security Working Group meetings.

# Information Security Service: Information Security Incident Management Process – UCL



## Investigations and Data Access Policies – University of York, case study

An investigation policy can expect to be the most scrutinised documents in a whole policy suite. Investigations and Data Access policies will be used in circumstances ranging from access to documents of a member of staff off sick, to internal disciplinary procedures, to police requests for data and even requests for surveillance under warrant from the Home Secretary. As such, even more care and wide consultation are necessary than with other policies.

Different institutions will have different processes and expectations of privacy at work. At York, staff have always been permitted to use their work email accounts for personal use, we do not do web filtering and do not pro-actively look at web logs for misuse. This culture of personal use and privacy affected the final policy in many ways, and was an explicit part of the initial discussions. Other institutions may take a very different line: FE institutions will usually have web filtering and altering for example.

These differences in emphasis mean that it is very unlikely that any general document will work, and a policy tailored to the institution will be necessary.

At the University of York our previous policy was very old and no longer fit for purpose. The title itself was a problem: “Policy for Investigation of Incidents under the Regulation of Investigatory Powers Act” seemed to imply that the policy only applied RIPA requests, and not for anything else, when we used it not just for other legal requests but also for internal investigations.

The policy had other serious issues as well:

- It did not mandate record keeping
- It did not prescribe what to do if illegal material might be found
- It made promises we could not keep about what might happen in court cases
- There was no clear demarcation between who could authorise a request and who could do the work. A Head of Department could both initiate and authorise an investigation
- It pre-dated the use of cloud services. It was possible to read it so that cloud services came into scope, but it was also possible to argue that they did not. With the University of York adopting Google Apps this became an urgent problem.

It was very obvious that the old policy did not just need a minor update, so we started again from scratch.

We came up with a set of sample issues and scenarios based on real cases over the past few years, and thought about how the old policy had made life difficult. This generated a list of areas we needed to fix. Next we looked at how within the University should authorise requests. We were surprised at the difference in views here: some departments thought that line managers (at any grade) should be able to authorise access, others wanted it limited to very senior staff and it was important to get agreement on this fundamental principle before other work was done.

We also listed our constraints and assumptions. This helped us to consider specific parts of the policy against criteria and was helpful when “lost in the detail”. For example:

- The policy had to align with other policies such as social media policy
- We needed to consult with unions etc.
- None of our staff are trained to evidence standards and the University had no wish to establish a forensics facility
- We assumed that users would be informed about access unless there was a specific reason not to do so
- We wanted the scope of the data accessed to be drawn as tightly as possible
- To protect privacy, we do not normally give direct access to an account (either via sharing the password or delegation), instead we pass on the data.

Our final policy has been in place for a year, and works for us. It protects University members’ privacy by requiring sign off at a senior level (Head of Department for internal requests, the Registrar for external legal ones) and ensuring separation of request and authorisation but still allows us to quickly give access to data in situations where it is urgent.

### Links to policy

Policy

[http://www.york.ac.uk/media/abouttheuniversity/supportservices/informationdirectoratedocuments/policies/ITInvestigationsandDataAccessPolicy\\_Oct2013.pdf](http://www.york.ac.uk/media/abouttheuniversity/supportservices/informationdirectoratedocuments/policies/ITInvestigationsandDataAccessPolicy_Oct2013.pdf)

Method Statement

<http://www.york.ac.uk/media/abouttheuniversity/supportservices/informationdirectoratedocuments/policies/MethodStatement-InvestigationsandDataAccess.pdf>

Proforma (Word document) on the web page

<http://www.york.ac.uk/about/departments/support-and-admin/information-directorate/information-policy/>

## Data breach – case study

The University of Morpeth is a research intensive pre-92 University.

At 11.59 on a Friday night, CSIRT staff at the University of Morpeth were alerted via email that students had discovered a way to access a restricted system and could view personal information of moderate confidentiality by exploiting a mis-configuration in a development system.

The message was picked up first thing on the Saturday morning, but due to a miscommunication between members of the team, the bug wasn't fixed until the Monday morning. Shortly after 9am on Monday the bug was fixed.

Because students had spotted the issue, the student press was in touch immediately, with other local media following later that day. University senior management were alerted while key technical staff set to work analysing the log files to understand the extent of the breach.

The University had not “war-gamed” an incident like this and the many decisions that have to be taken. For example, should a spokesperson be provided for TV/radio, or should all media enquiries just receive a prepared statement? Making such decisions required heavy levels of involvement from senior staff, working under considerable pressure. The University opted not to provide a case study for local radio and other requests, but kept this decision under close review as the incident progressed.

Fortunately, full logging was available and the University was able to determine every unauthorised access and which information was viewed. This proved to be key in managing the incident, with the certainty given by detailed logging helping to manage fears.

A key learning point is that any analysis needs to be communicated carefully: an initial estimate of the number of people affected was produced on the fly in a meeting by a member of the technical team. Within 90 minutes, and without double checking, that number was released in an official press release. Fortunately for everyone concerned, when double checked the next day, the number was correct.

Since the University now had a full list of the individuals affected, the nature of the data released and, in many cases, knowledge of who accessed the data, the decision was made to telephone everyone affected. Initial plans within IT had been to issue email alerts: the decision to telephone everyone affected by the breach proved a very good one. People contacted were surprised to be directly contacted, grateful for the chance to be reassured and get details on what happened.

To make this work, two key things were done. 1) All phone calls were done by two members of staff working in tandem and 2) a full script was written in advance covering opening lines, responses to questions, details of the insurance offered etc. The need for a script was contested by some staff, but its use in avoiding mistakes when making the 20th phone call of the day soon became apparent.

The combination of a formal response, transparency about the extent of the breach, personal communications and offers of suitable insurance seemed to work, with interest in the incident dropping rapidly after the first two days. There have been no reports of any loss or harm to individuals as a result of the incident.

In the aftermath of the breach, the Information Commissioner's Office was notified and a plan put in place to prevent a repeat including governance changes, staff training and changes to development practice.

### Key points:

- Having an incident plan in advance, covering IT, Communications and University Senior Management with clear lines of escalation, out-of-hours contact details for key stakeholders and agreed criteria for actions e.g. when something is serious enough to place on the University's front page, can save a lot of time
- Develop a communication plan in advance
- Logs are vital, but manage the release of information internally as well as externally. Caveats around data get lost very rapidly.
- Personal communication with victims, if at all possible, is highly appreciated.
- Even with detailed communications to the media, some media organisations will get the facts very wrong. One on-line trade site reported a level of users affected two orders of magnitude too high! Such mistakes are had to correct and develop a life of their own. Getting the correct facts out as early as possible is the best defence.



# Resources for Chapter 12 – Continual improvement

There are no resources for this chapter



# Resources for Chapter 13 – Policies

## RESOURCES

- [Template for a generic policy](#)

## Template for a generic policy

**Header:** date, version, classification, policy name and version

**Footer:** page number (X of Y), organisation name

**Policy title:** unique reference

**Policy contact:** the role to contact if the reader has questions or comments. Not a person's name.

**Policy owner:** if different to policy contact. Role, not name.

### History

| Date | Version number                           | Author        | Approved by   | Comments   |
|------|--|---------------|---------------|--|
|      | Have a consistent approach to versioning | Name and role | Name and role | Initial version                                      |
|      |  |               |               | What changes were made and why<br>Was this a review? |

### Review plan

When will this document be reviewed? Either every X years, or after event Y, e.g. changes to related requirements, or to related documents.

### Introduction

Answer these questions about the document:

- Where did it come from- history and context?
- What problem(s) is it intended to solve?
- What benefit(s) is it intended to create?

Keep it short and pithy. This is your opportunity to explain to people why they should bother to read on.

### Scope

- Who needs to know what's in this document?
- What roles/physical areas/groups does it apply to?
- When?

### Related documents

This allows you to find out what effect there will be on other documents if you change this one, and vice versa.

Documents which refer to this policy:

Documents which this policy refers to:

### Related requirements

Contracts, laws and other internal or external requirements which have shaped this policy. So if they change, you know to review this policy- and if you change this policy, you know what other documents to check with, so that you don't accidentally breach contract etc.

### Stakeholders

Optional: roles which need to be involved in revisions of this document.

### Definitions

Key definitions can go here, or this section can reference a Glossary where all of the definitions live.

### Policy statements

List of policy statements. No lengthy explanations, no sanctions, no detailed technical statements. This document should not need to be changed every time a new version of Internet Explorer comes out.

Divide into subsections if appropriate.

Separate mandatory items from optional items to allow people to see at a glance what they have to do, as opposed to what they can ignore.

Anything mandatory uses the words must, will and/or shall.

Optional items use the words might, should, could, may.

Review statements for coverage, overlap, consistency and ambiguity.

### **Sanctions**

What happens if this policy is not followed? Either describe how this is to be addressed, or reference a single sanctions document (possibly in the HR area). If non-compliance is acceptable, this is not a policy but guidance - rename it.



## Project Team

The UCISA Information Security Management Toolkit project team consisted of a lead author, a group of five contributing universities, and colleagues from Jisc Technologies.

UCISA would like to thank Jisc for their support to the project through their release of expert Jisc Technologies staff to author and review content.

## Lead author

Bridget Kenyon, Head of Information Security, University College London

## Cardiff University

Gareth Jenkins, Business Change Manager, Information Security Framework Programme  
Ruth Robertson, Deputy Director Governance and Compliance

## Jisc Technologies

Andrew Cormack, Chief Security Advisor  
James Davis, Information Security Manager

## Loughborough University

Matthew Cook, Head of Infrastructure and Middleware  
Niraj Kacha, Senior IT Services Specialist  
Graeme Fowler, Senior IT Services Specialist

## University of Oxford

Jonathan Ashton, Information Security Officer, IT Services  
Professor Paul Jeffreys, Director of IT Risk Management, IT Services  
Sarah Lawson, Head of IT and Information Security, National Perinatal Epidemiology Unit

## University College London

Daniela Cooper, Information Security Officer  
Dr. Granville Moore, Senior Research Associate, Information Security Research Group  
Dr. Simon Parkin, Senior Research Associate, Information Security Research Group  
Professor Angela Sasse, Head, Information Security Research Group

## University of York

Dr. Arthur Clune, Head of Systems, IT Services  
Kay Mills-Hicks, Information Policy Consultant

The project was managed by Anna Mathews, UCISA Head of Policy and Projects, with oversight from Mark Cockshoot, Chair of the UCISA Infrastructure Group and Alan Radley, Elected Member of the UCISA Executive Committee. Peter Tinson, UCISA Executive Director, provided additional support.

UCISA is very grateful for the assistance received from colleagues across the sector. In particular, we would like to thank the following individuals who provided information or acted as critical friends whilst the Toolkit was being drafted:

Jon Bagshaw, Senior Computer Officer, University of Bradford  
Tony Brookes, University Information Assurance Officer, University Of Derby  
Nigel Bailey, IT Business Assurance Manager, King's College London  
Mike Barwise, Information Risk Management Consultant, Integrated InfoSec  
Matt Ball, Business Analyst, University of Leicester and PCI DSS Sig Chair  
Dr. Michael Fraser, Director, Infrastructure Services, IT Services, University of Oxford  
Owen Freel, Project Manager, Universities and Colleges Shared Services  
Barbara Frost, Information Security Manager, University of Manchester

Brian Gilmore, Director of IT Infrastructure, University of Edinburgh  
William Hammonds, Policy Researcher, Universities UK  
Quentin North, Assistant Director, IT Services, University of Brighton  
Gary Nye, ICT Planning Manager, University of Bedfordshire  
Christa Price, Senior Information Security Officer, University of Salford  
Peter Rigby, Senior Policy Manager, Efficiency and Reform, Research Councils UK  
Bruce Rodger, Head of Infrastructure Services, University of Strathclyde  
Harris Salapasidis, IT Security Manager, University of the Arts London  
Robbie Walker, Security Architect, University of Portsmouth

The external reviewer for the Toolkit was Tim Phillips.

We would also like to thank members of the UCISA Networking Group, the UCISA Infrastructure Group and the UCISA Executive Committee for their comments and suggestions.



