



UCISA-Infrastructure Group Case Study

King's College London – Infrastructure Analysis and Resilience Review

1. Introduction

Information Services and Systems (ISS) at King's College London has recently restructured a significant part of its IT services (integrating business and academic IT systems), and recruited several new members of staff to the IT Systems Management Team. In addition, ISS has secured a significant amount of funding from the College for upgrading and improving its ailing legacy IT infrastructure. In this context, it has been timely to conduct a high-level review of systems and services, with a particular focus on resilience and business continuity. A high level methodology designed to provide a point-in-time assessment and measurement of the resilience risk across the IT systems, and the impact of infrastructure unavailability has been designed and implemented. This has been highly successful in assisting with development of a shared understanding of the existing infrastructure within the Team, transparent decision-making and prioritisation, and communication with the College's management team.

2. Description of the work

2.1 Infrastructure Analysis methodology

The objectives of developing the Infrastructure Analysis methodology were:

- To quickly develop a shared understanding of the existing IT systems and infrastructure across the IT Management Team
- To assess and measure the risk of failure of these systems (resilience)
- To assess and measure the impact on the College of the unavailability of the systems, and improve the shared understanding of this across the IT department.
- To assist with decision-making and prioritisation
- To assess the in-house knowledge and breadth of support skills
- To assist with communication of these findings to College senior management and hence secure resource to reduce resilience risk

In order to meet these objectives a light-touch high-level methodology has been designed, with the intention of being able to measure the resilience and impact of unavailability of each system.

At a weekly meeting for each system, a comparative score (out of 10) was assigned to each of the criteria overleaf:

- Resilience Risk
 - Complexity of the service infrastructure
 - Age of hardware
 - Age of software (distance from current implementation to latest point release)
 - Supportability (reliance on key staff, market availability of skills and support, third party support etc)
 - Single points of failure
 - Estimated disaster recover time
 - Current capacity/performance
 - Environmental vulnerability (power, location of equipment, risk of tampering etc)

- Institutional impact of unavailability of the system/service
 - Client/user ranking (high for VIP users)
 - Level of business function affected
 - Number of IT services affected
 - Number of clients/users affected
 - Impact of unavailability on institutional image/brand

2.2 Infrastructure Analysis meetings

In order to implement the methodology, weekly (hour-long) meetings of a team comprised of senior IT managers and technical specialists, led by the Chief Technology Officer, were conducted. Using existing documentation where available, diagrammatic representation of the systems and assessments were made of the following systems/services according to the above criteria:

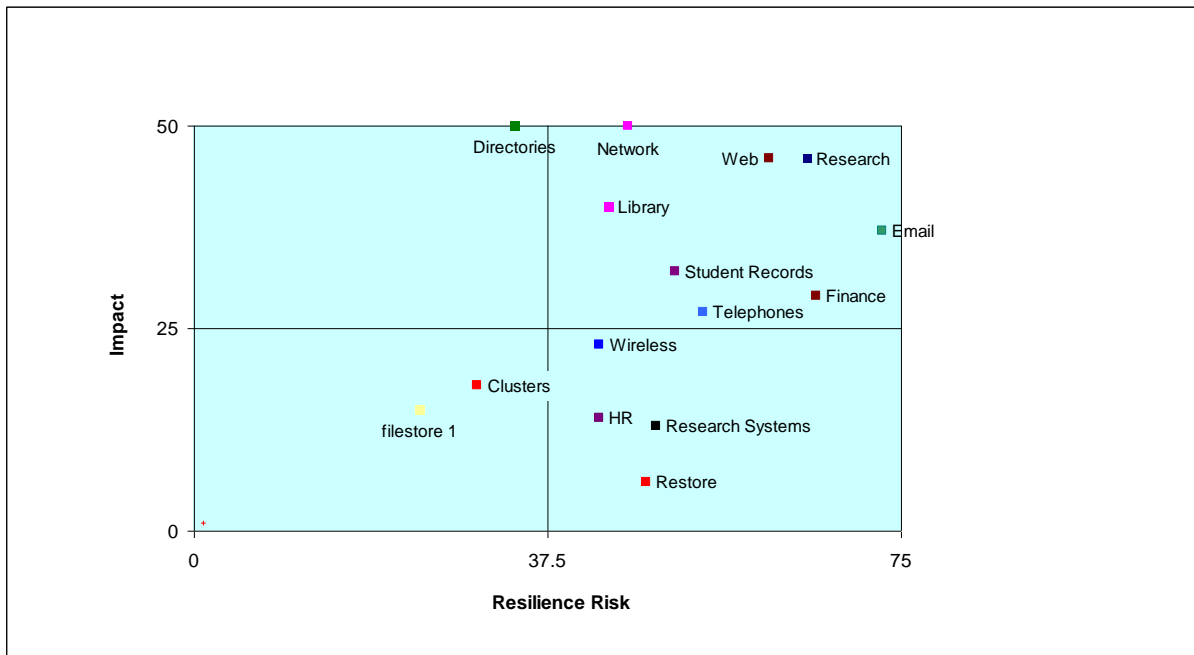
- Email systems
- Web systems
- Student Records systems
- Finance/payroll systems
- HR systems
- Library systems
- Research systems
- Backup/restore systems
- E-learning systems
- Student cluster workstation infrastructure
- Network infrastructure
- Wireless infrastructure
- Directories/Authentication systems
- Networked filestore systems
- Telephony systems

An example scoring spreadsheet is detailed in Appendix A.

The scores assigned to the individual criteria were aggregated to provide a final score for risk and impact for each system, and these totals were then plotted on axes to provide a visual comparison. In addition, notes were made where appropriate detailing why decisions were made to allocate particular scores.

2.3 Outcomes and Analysis Results

An example outcomes graph is shown below (some results have been changed for confidentiality which may distort the impact findings):



This clearly enabled identification of those systems most at risk and those which were of high criticality to the institution, relative to other systems and has enabled focussed resource allocation in these areas. The graphical presentation is easily understood by non-technical stakeholders and has resulted in a shared understanding of risk points and priorities at senior level within the College.

Analysis of the figures also enabled the calculation of an overall resilience risk figure, which has been helpful in measurable goal setting. ISS identified an overall 65% resilience risk which we have undertaken to reduce to 40% within one year. In addition, more granular goals have been set in specific areas.

The spreadsheet also allowed for calculation of the highest risk categories. At King's these were identified as Supportability and Environmental Risk. Programmes are now underway to mitigate risks in these areas, primarily by reducing the range of hardware and operating systems supported and addressing issues with facilities in data centres.

By-product benefits of the process have been in the area of staff engagement and transparency. IT Senior Management were initially cautious about the reaction of technical staff to the exercise but feedback has been that they were keen to share the burden of responsibility regarding systems resilience and pleased to have the opportunity to engage with colleagues. In turn management have been able to share the results with all IT staff as an indication of why we are focussing resources and

change programmes in particular areas.

2.4 Further workstreams and spin-off activities

The success of the methodology has inspired staff in ISS and the College to adopt a similar approach to assessment of systems and services. In particular, a high-level assessment of the College's Business Systems is now being conducted by a range of staff from across the business units using a similar process. Business systems are being assessed for "fit-for purpose" (via a range of criteria) and plotted against the extent to which they provide support for the College's strategic objectives. In this way, prioritisation of resources can again be facilitated in a transparent fashion with buy-in from across the institution.

There is also an exercise underway to assess systems' security risk against the impact criteria.

3. Conclusion

The infrastructure analysis methodology has been highly successful in developing a shared understanding of systems risk and impact of unavailability within IT Systems, ISS and the College. It has enabled transparent allocation of resources to areas of priority, setting of measurable goals and targets and communication of IT risks and issues at all levels. The benefits of the exercise have been recognised by various stakeholders, from the College's senior management through to IT staff, and several spin-off processes are underway.

4. Contact

For further information please contact Lynne Tucker:

Lynne Tucker
Chief Technology Officer

Information Services and Systems
King's College London
Room 4.27, 4th Floor
Waterloo Bridge Wing
Franklin Wilkins Building
150 Stamford Street
London SE1 9NN

Email: Lynne.Tucker@kcl.ac.uk

Tel: 0207 848 4443

Fax: 0207 848 4457

Appendix A

RESILIENCE	Description	System A	System B	System C
Complexity	Degree of complexity based on the number of items and interconnects required to provide service	10	6	4
Hardware age	Age of hardware	7	5	6
Software age	Factor based on number of items > 2 versions older than current release	6	5	8
Supportability	Supportability factor based on in house capability (key person dependencies), reliance on 3rd party and contractual arrangements	9	5	9
Single points of failure	Factor based on number of single points of failure	6	7	10
DR time	Factor based on time to implement full DR plan	9	3	8
Capacity/Performance	Utilised capacity at tightest bottle neck	10	5	7
Environmental	Factor based on risk to virus attack, user breakage, physical damage, power failure etc	8	10	9
TOTAL		65	46	61

IMPACT				
Client Ranking	highest level of staff/student affected. E.g.: 1= student, 10=VIP	10	10	10
Business Function	level of College Business function affected. E.g.: loss of College website = 10. Loss of student printing services = 1	10	10	10
IT Services	ranking for type and number of IT services unavailable or affected. E.g.: loss of network infrastructure = 10, loss of individual system (e.g. printing)= 1.	6	10	6
Number of Clients	number of clients affected. 1= less than 50, 2=50-99, 3=100-299, 4=300-499, 5=500-999, 6=1,000-1,999, 7=2,000-4,999, 9=5,000-9,999, 10=10,000 or over	10	10	10
Brand/Image factor	rating for the potential effect on the College's external image	10	10	10
TOTAL		46	50	46