

B Business continuity management and planning

This document is part of the *UCISA Information Security Toolkit* providing guidance on the policies and processes needed to implement an organisational information security policy. To use the Toolkit effectively it should be read alongside the Toolkit *Introduction* and the *How to use* guide and then used to develop appropriate information security elements for inclusion in your organisation's policies.

1. Introduction

The Business Continuity Management and Planning Policy sets out the process for assessing and addressing risks to business continuity and defines the responsibilities for preparing and implementing business continuity plans (BCPs).

Usually there will be a number of systems, each with different continuity requirements depending on the level of criticality to the organisation. The risk assessment process to classify systems should be formal but need not use any particular method and should categorise the impact of the system being unavailable as being of high, medium or low criticality. Appropriate business continuity plans for each system or classification can then be produced.

2. BS 7799 definitions and numbering

Business continuity management and planning is covered by section 14 of the standards document.

14.1 Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Controls

14.1.1 Including information security in the business continuity management process

A managed process should be developed and maintained for business continuity throughout the organisation that addresses the information security requirements needed for the organisation's business continuity.

14.1.2 Business continuity and risk assessment

Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.

14.1.3 Developing and implementing continuity plans including information security

Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

14.1.4 Business continuity planning framework

A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

14.1.5 Testing, maintaining and re-assessing business continuity plans

Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.

3. Interrelationship between policies in this document and related BS 7799 references

In this Toolkit, each subsection addresses a number of the business continuity management controls from the standard. All of the controls in section 14 of the standard are covered.

| Toolkit subsection | Control(s) |
|-------------------------------------|--|
| Initiating the BCP project | 14.1.1 Including information security in the business continuity management process 14.1.4 Business continuity planning framework |
| Assessing the BCP security risk | 14.1.2 Business continuity and risk assessment 14.1.4 Business continuity planning framework |
| Developing the BCP | 14.1.3 Developing and implementing continuity plans including information security 14.1.4 Business continuity planning framework |
| Testing the BCP | 14.1.4 Business continuity planning framework 14.1.5 Testing, maintaining and reassessing business continuity plans |
| Training and staff awareness on BCP | 14.1.4 Business continuity planning framework 14.1.5 Testing, maintaining and reassessing business continuity plans |
| Maintaining and updating the BCP | 14.1.4 Business continuity planning framework 14.1.5 Testing, maintaining and reassessing business continuity plans |

4. Guidelines for use

The purpose of business continuity planning is to prepare for interruptions to business activities.

Business continuity plans protect critical business processes from major failures or disasters affecting information systems. These plans (which include elements of disaster recovery) must be developed and maintained across the organisation and this requires a management process.

Business continuity planning involves identifying and reducing the risks from deliberate or accidental threats to vital services. Plans are developed to enable business operations to be maintained following the failure of, or damage to, vital services or facilities. The objective of these plans is to ensure that the organisation's essential services and facilities are restored as quickly as possible following such a failure.

The planning process should look at the entire infrastructure required to keep all critical business processes and support services running. This may include: staffing requirements, transport facilities, electrical supply, telephone services, etc.

The following six subsections identify each element which must be considered when developing a policy for business continuity planning and offer suggested policy statements. The final subsection then gives an example policy along with some notes on its use.

5. Initiating the BCP project

i. Suggested Policy Statement

"Management are required to initiate a business continuity plan."

Explanatory notes

The BCP project needs to be initiated, formally approved and supported by the Board or governing body of the organisation.

Information security issues to be considered when implementing your policy include the following:

- Lack of Senior Management Team commitment to formal BCP development is likely to result in an inadequate process.

Scope of business continuity planning

For each system, it will be necessary to assess the longest period for which the system could be unavailable without serious detriment to the organisation. This will indicate the criticality of that system. For example:

| High Criticality Systems | Medium Criticality Systems | Low Criticality Systems |
|--|--|--|
| Business can continue using manual processes for up to two working days: a replacement for a failed system must be in place within two days. Relevant departmental plans accommodate a failure of up to two days. Estates, purchasing and insurance strategies/plans incorporate their role in information systems continuity. | Business can continue using manual processes for up to one week: a replacement for a failed system must be in place within one week. Relevant departmental plans accommodate a failure of up to one week. Estates, purchasing and insurance strategies/plans incorporate their role in information systems continuity. | Business can continue using manual processes for up to twelve weeks: a replacement for a failed system must be in place within twelve weeks. Relevant departmental plans accommodate a failure of up to 12 weeks. Estates, purchasing and insurance strategies/plans incorporate their role in information systems continuity. |

6. Assessing the BCP security risk

ii. Suggested Policy Statement

“Management are required to undertake a formal risk assessment in order to determine the requirements for a business continuity plan.”

Explanatory notes

Risk assessment, as part of business continuity planning, analyses the nature of such unexpected occurrences, their potential impact, and the likelihood of these occurrences becoming serious incidents.

Information security issues to be considered when implementing your policy include the following:

- Even where a formal BCP project has been initiated, if the allocated financial and human resources are insufficient, the resultant plan is likely to provide limited protection.
- Underestimating the short and medium term impact of a security incident can result in an inappropriate level of response towards building a suitable BCP.

Risk assessment for business continuity planning

Risk assessment should be undertaken for all systems which form part of the organisation’s infrastructure.

The outcome of the risk assessment should be the classification of the systems according to their criticality to business processes. The criticality level will be determined according to the impact of the failure of the system.

Systems where a failure would result in little loss of service or where only a small number of people would be affected will have low criticality whereas systems where failure would be catastrophic or would affect many people will have high criticality.

For most organisations it will be sufficient to classify systems as having high, medium or low criticality. Fewer or more categories may be used if necessary.

| High Criticality Systems | Medium Criticality Systems | Low Criticality Systems |
|--|--|---|
| All systems have been assessed against known risks. All feasible steps to militate against risks have been implemented. | All systems have been assessed against known risks. Steps to militate against the most likely risks have been identified and implemented where appropriate. | A sample of systems have been assessed against the risks most likely to occur. Simple steps have been taken to militate against obvious risks. |

7. Developing the BCP

iii. Suggested Policy Statement

“Management are required to develop a business continuity plan which covers all essential and critical business activities.”

Explanatory notes

The business continuity plan is a project plan which is likely to be complex and detailed.

Irrespective of the nature of your particular organisation, it should probably contain a series of critical actions to be taken in the event of a failure or disaster which should culminate in a return to normal operations.

Information security issues to be considered when implementing your policy include the following:

- When the need arises to trigger the BCP, but:
 - it does not exist, or
 - is untested, or
 - is non-viable, or
 - fails when activated.
- The organisation’s operations may not be able to recover – ever.

Business continuity planning framework

A single framework of corporate plans should be maintained to ensure that all levels of plan are consistent, and to identify priorities for testing and maintenance.

Business continuity plans should be modular and task oriented. Each plan should clearly specify the conditions for its activation, as well as the individuals responsible for executing each component of the plan. New plans need to be consistent with established emergency procedures and existing fallback arrangements, core computer services, telecommunications and accommodation.

Different levels of plan may be required as each level might have a different focus and/or involve different recovery teams.

Each plan should have four main components:

- Emergency procedures – describing the immediate action to be taken following a major incident that jeopardises business operations.
- Fallback procedures – describing the action to be taken to move essential business activities or support services to temporary locations.
- Resumption procedures – describing the action to be taken to return the business to the normal full operation, usually at the original site.
- Test schedule – which states how the plan should be tested.

Each level of plan, and each individual plan, should have a specific custodian. Copies of each of the above business continuity plans should be held off site.

| High Criticality Systems | Medium Criticality Systems | Low Criticality Systems |
|---|--|---|
| Continuity plans cover: Recovery procedures for most likely scenarios. Any temporary arrangements. Disaster recovery contracts. Replacement equipment arrangements. Relocation arrangements. | Continuity plans cover: Recovery procedures for most likely scenarios. Any temporary arrangements. | There is a documented recovery process. |

8. Testing the BCP

iv. Suggested Policy Statement

“The business continuity plan is to be periodically tested to ensure that the management and staff understand how it is to be executed.”

Explanatory notes

Testing your organisation’s business continuity plan (BCP) assesses its viability, and ensures that your staff are conversant with the proposals.

Information security issues to be considered when implementing your policy include the following:

- Where the BCP testing does not reproduce authentic conditions, the value of such testing is limited.
- A failure to analyse the BCP test plan results is likely detract from the value of the test.

Testing business continuity plans

Business continuity plans must be tested.

A test schedule should be drawn up for each business continuity plan. The schedule should indicate how and when each element of the plan should be tested.

A phased approach to testing is recommended, based on frequent tests of individual components of the plan. Feedback from the tests should be used to update the plans. This ensures that the plan is kept alive and up to date throughout the year. It also reduces the dependency on (less frequent) all-out tests of the full plan.

There is a documented recovery process.

| High Criticality Systems | Medium Criticality Systems | Low Criticality Systems |
|---|--|--|
| Continuity plans are tested on a sample of systems each year. | Continuity plans are tested on a sample of systems after any major system changes. | Continuity plans are tested on a sample of systems after any major system changes. |

9. Training and staff awareness on BCP

v. Suggested Policy Statement

“All staff must be made aware of the business continuity plan and their own respective roles.”

Explanatory notes

If a business continuity plan is to be executed successfully, all personnel must not only be aware that the plan exists, but also know its contents, together with the duties and responsibilities of each party.

Information security issues to be considered when implementing your policy include the following:

- Even a BCP that is tested can fail if personnel are not sufficiently familiar with its contents.
- When BCP becomes divorced from people’s perception of realistic risk, a sense of apathy can reduce their desire for participation in BCP activities.

10. Maintaining and updating the BCP

vi. Suggested Policy Statement

“The business continuity plan is to be kept up to date and retested periodically.”

Explanatory notes

The maintaining and updating of the business continuity plan (BCP) is critical if its successful execution is to be relied upon.

Information security issues to be considered when implementing your policy include the following:

- Where the updates to the BCP have not probed the implications and underlying assumptions resulting from changes, the execution of the BCP may be flawed.
- Where the BCP is not being updated periodically, its fitness for purpose may become questionable very quickly.

Updating business continuity plans

Business continuity plans must be updated regularly. Business continuity plans quickly become out of date because of changes in the business or organisation. Management of the plans is essential to protect the investment in developing the initial plan, otherwise the effectiveness of the plan may be degraded.

The owner should be responsible for identifying and applying changes to the plan. Individual changes should be applied periodically. The complete plan should be reviewed at least annually.

| High Criticality Systems | Medium Criticality Systems | Low Criticality Systems |
|---|---|---|
| Continuity plans are reviewed annually. | Continuity plans are reviewed annually. | Continuity plans are reviewed periodically. |

Specimen Information Security Elements of a Business Continuity Policy

The organisation management team will initiate a project to assess business continuity requirements and to identify appropriate areas for further action.

A formal risk assessment exercise will be conducted to classify all systems according to their level of criticality to the organisation and to determine where business continuity planning is needed.

A business continuity plan will be developed for each system or activity. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates.

All business continuity plans will be periodically tested. The frequency of testing will be as defined for the appropriate criticality level and will include tests to verify whether management and staff are able to put the plan into operation.

All relevant staff will receive appropriate training to be able to carry out their roles with respect to business continuity plans.

Each business continuity plan will be reviewed, and if necessary updated. The frequency of reviews will be as defined for the appropriate criticality level.

These specimen policy elements are intended only as a guide and should be adapted for individual organisations.

The implementation of a business continuity planning policy will also require the development of processes and procedures. Documentary evidence of these will be required to satisfy an external party, such as an auditor, that the policy has been fully implemented. These documents may include:

- Up to date business continuity plans for systems and activities.
- Records of the testing regime.
- Risk assessment records.