Information Services IT Security Policies

B. Business continuity management and planning

Table of Contents

1. Introduction ......................................................................................................................... 2
2. Initiating the BCP project ................................................................................................. 3
3. Assessing the BCP security risk ......................................................................................... 4
4. Developing the BCP ............................................................................................................ 4
5. Testing the BCP .................................................................................................................. 5
6. Training and staff awareness on BCP ............................................................................... 6
7. Maintaining and updating the BCP ..................................................................................... 6
8. Glossary ................................................................................................................................ 7
1. Introduction

Business continuity planning (BCP) can be defined as the Institute's ability to maintain or restore its business and academic services when some circumstance threatens or disrupts normal operations. This can be achieved by identifying and reducing the risks from deliberate or accidental threats to vital services. Disaster recovery plans are also 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.

1.1 BCP roles and responsibilities

Senior management in DIT have a responsibility to provide resources and support for the development of BCP in the Institute. A lack of commitment to the formal development of BCP is likely to result in an inadequate process.

The Chief Information Officer (CIO) will have authority to develop, implement and enforce information security policy. The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of Information Services. In order to fulfil this goal, each business process must have a nominated owner who should be assigned responsibility for conducting Business Impact Assessment (BIA) for their areas, to determine the acceptable interruption periods and to identify risks to their processes. The responsibility for implementing business continuity measures may be delegated as agreed with Information Services – though accountability should remain with the nominated owner of the business process.

Where appropriate, the Public Affairs Office will have responsibility for communicating with the wider community and with the media.

Other functional areas who may have responsibilities under this policy include but are not limited to Human Resources and the Buildings Office.

1.2 Background to this document

This policy and other associated IT security policies form part of the Institute’s IS organisational security policies. The Institute has adopted the UCISA Information Security Toolkit as the framework for its Information security policies. The toolkit draws heavily on the British Standard BS 7799 which was also the main source of the international standard ISO 27002.

The tool kit comprises sixteen sections, of which this corresponds to Section B. The Institute will have a policy for each section adapted to its needs. Each policy will also refer to associated procedures and guidance notes that are relevant to the policy.

1.3 Intended audience

This document is intended to be read by those Institute staff involved in business continuity planning.
2. **Initiating the BCP project**

2.1 **Process for project approvals**

The resources (staff and equipment) required to implement BCP can be significant so a proposal to do so should be treated as a formal project that requires the approval and support of the Directorate for the Institute. Approval can only be given following a recommendation from the Institute’s IT governance body, the Information Services Steering Committee who will prioritise all project proposals according to statutory requirements and also, the risk to the Institute from not proceeding. Further information on the ISSC and the projects approval process is available from the Information Services Programme Management Office.

2.2 **Conducting a Business Impact Assessment**

Upon approval of a BCP project, one of the first actions should be to catalogue current IT systems, the business processes that they support and the owner for each business process. Each process should undergo a BIA to establish the longest period a function could be unavailable without a significant impact to the Institute. This will indicate the criticality of those processes and should give consideration to the following points:

- **Recovery time objective:** How long before a process can go operational again following an interruption?
- **Recovery point objective:** What would be an acceptable loss of data (which can be measured in hours or days)?
- **Seasonal activities:** Is a process critical at all times of the year round or for particular periods (e.g. exams)?
- **Cost to the Institute:** The cost of a process failure should be calculated and can be expressed in either monetary terms (e.g. revenue loss) or non-monetary terms (e.g. loss of reputation)

At the end of this exercise, it should be possible to rank business processes by their criticality and to group them accordingly. This is illustrated in the following table:

<table>
<thead>
<tr>
<th></th>
<th>High criticality processes</th>
<th>Medium criticality processes</th>
<th>Low criticality processes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recovery time objective</strong></td>
<td>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</td>
<td>Business can continue using manual processes for up to one week: a replacement for a failed system must be in place within one week</td>
<td>Business can continue using manual processes for up to twelve weeks: a replacement for a failed system must be in place within twelve weeks</td>
</tr>
<tr>
<td><strong>Recovery point objective</strong></td>
<td>Data recorded up to four hours before failure must be recovered</td>
<td>Data recorded up to one day before failure must be recovered</td>
<td>Data recorded up to one week before failure must be recovered</td>
</tr>
</tbody>
</table>
3. Assessing the BCP security risk

3.1 Risk assessment for business continuity planning

A formal risk assessment must be undertaken for all critical business processes. This requires identification of all the resources that a process depends on and can benefit from the creation of catalogues of regulations, standards, personnel, external suppliers and IT systems as a means of “seeding” the risk assessment. The assessment must consider all threats including those that are man-made and natural and should capture the following details:

- Description of risk
- Probability of risk occurring
- Impact of risk execution (quantitative and qualitative)
- Mitigating actions
- Action owner

Where appropriate, the risk assessment should be linked to the Institute’s risk register as an enterprise approach to risk mitigation is more cost-effective than a siloed approach. It will also facilitate the reuse of existing risk assessment tools such as the one listed below.

<table>
<thead>
<tr>
<th>Risk occurrence</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probable</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Likely</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Reasonably likely</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Unlikely</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Improbable</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Where the risk assessment should be linked to the Institute’s risk register as an enterprise approach to risk mitigation is more cost-effective than a siloed approach. It will also facilitate the reuse of existing risk assessment tools such as the one listed below.

4. Developing the BCP

4.1 Mitigation of known risks

Disaster recovery is a subset of Business Continuity as it deals with the recovery of a process following a failure. Therefore, it is highly desirable that all identified risks be assessed against their mitigating actions, particularly where there are interdependencies, so that an agreed approach be applied to eliminate or reduce the likelihood of the risk occurring or to lessen the impact of its execution.

It is important to ensure that the allocated financial and human resources are sufficient to address the risks prioritised for mitigation. Where this is not feasible then such risks must remain in the risk register and be addressed as part of disaster recovery.
4.2 Business continuity planning framework

For all remaining risks, a BCP is required for each critical business process. This should 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. There must be an overall framework of plans to ensure consistency and to assist in the prioritisation of testing and maintenance.

Each plan should clearly specify the conditions for its activation, as well as the individuals responsible for executing each component of the plan. A plan should comprise of four main components as follows:

- **Emergency procedures**: These describe the immediate action to be taken following a major incident that jeopardises business operations. These should be consistent with established Institute procedures for handling emergencies.
- **Fallback procedures**: The action to be taken to move essential business activities or support services to temporary locations.
- **Resumption procedures**: What actions should be taken to return the business to the normal full operation, usually at the original site.
- **Test schedule**: How the plan should be tested

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

5. Testing the BCP

5.1 Developing a formal test programme

Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective, and that staff understand how they are to be executed in a time of crisis. Otherwise, there is no demonstrated ability to recover in the event of a major failure. The criticality of each process will help determine the frequency for testing each plan.

In preparing for the test, there should be a clear understanding of what the objectives of the exercise are, i.e. to discover problems that might occur during a real disaster situation. Care should be taken to avoid running tests that are designed to reassure management that all issues are addressed thereby creating a false sense of security. Therefore, the test exercise should be documented and provide details on the following:

- Objectives of the test
- Testing schedule
- Specific test steps
- Roles and responsibilities for the test
- Report from the previous test
5.2 Conducting the test

There are a number of approaches for conducting tests and these are listed below in order of increasing complexity and realism.

- **Checklist**: Preliminary step to real test, distribute plan for review by business unit managers
- **Structured walk through**: Business unit managers walk through the test plan with each step marked as performed
- **Simulation**: All personnel with BCP responsibilities meet, go through a practice session
- **Parallel**: Full test of recovery plan in backup site using all personnel. Does not affect availability of main systems
- **Full-interruption**: Disaster is replicated to the point of ceasing normal operations

5.3 Addressing weaknesses in the BCP

Upon conclusion of the testing, there should be a review of the exercise before the test team is disbanded. There must then be a process to ensure that any flaws identified during the exercise are logged and that somebody is given responsibility for implementing corrective actions.

6. Training and staff awareness on BCP

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

- The plan does not fail as a result of staff not being sufficiently familiar with its contents
- The relevance of BCP is understood by staff to prevent apathy and disinterest colouring people’s opinions

7. Maintaining and updating the BCP

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. Each plan owner should be responsible for identifying and applying changes to the plan which should be reviewed at least annually.

It is also recommend that the BIA for each process be reviewed on a regular basis to ensure BCP remains in alignment with the strategic goals of the Institute. This could mean that some systems now have tighter recovery objectives while others have a reduced priority.
<table>
<thead>
<tr>
<th>Standard</th>
<th>Objective no.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS 7799 / ISO 27002</td>
<td>14.1.1</td>
<td>Including information security in the business continuity management process</td>
</tr>
<tr>
<td>BS 7799 / ISO 27002</td>
<td>14.1.12</td>
<td>Business continuity and risk assessment</td>
</tr>
<tr>
<td>BS 7799 / ISO 27002</td>
<td>14.1.3</td>
<td>Developing and implementing continuity plans including information security</td>
</tr>
<tr>
<td>BS 7799 / ISO 27002</td>
<td>14.1.4</td>
<td>Business continuity planning framework</td>
</tr>
<tr>
<td>BS 7799 / ISO 27002</td>
<td>14.1.5</td>
<td>Testing, maintaining and re-assessing business continuity plans</td>
</tr>
</tbody>
</table>

8. **Glossary**

- **BCP**  Business continuity planning
- **BIA**  Business Impact Assessment