

## Lessons Learnt from Implementing BS 25999 Business Continuity Management Systems

### White Paper

---

#### Neil O'Connor, Activity

This White Paper discusses Activity's approach to the implementation of Business Continuity Management Systems, and identifies lessons learnt from engagements with a number of clients.

Introduction .....	1
BS 25999.....	1
Implementing BS 25999 .....	2
Key Lessons Learnt.....	4
For More Information .....	5
Biography of Author.....	5
About Activity.....	6

### **Introduction**

Activity has helped a number of clients implement Business Continuity Management Systems (BCMS), more recently using the model described in BS 25999 Business Continuity Management – Part 2 Specification since its publication in November 2007. This paper outlines our approach to implementing a BS 25999-compliant BCMS and notes some lessons learnt to date from the implementation of the standard.

### **BS 25999**

#### **The Standards**

BS 25999 is defined in two standards:

1. BS 25999-1:2006 Business Continuity Management – Part 1 Code of Practice. This document defines good practice Business Continuity Management (BCM) and provides advice and guidance on the implementation of a BCMS.

2. BS 25999-2:2007 Business Continuity Management – Part 2 Specification. This standard provides the specification for a BS 25999-compliant BCMS. Any compliance audit or independent certification of a BCMS against BS 25999 would be against this specification.

BS 25999 Part 1 provides general guidance and advice on the implementation of a BCMS, whereas BS 25999 Part 2 provides the specification that a BCMS must meet if it is to be independently certified.

## The Model

BS 25999 adopts the Plan – Do – Check – Act (PDCA) model implemented by the major management systems (Quality, Environment, Security etc) documented as International and British Standards.

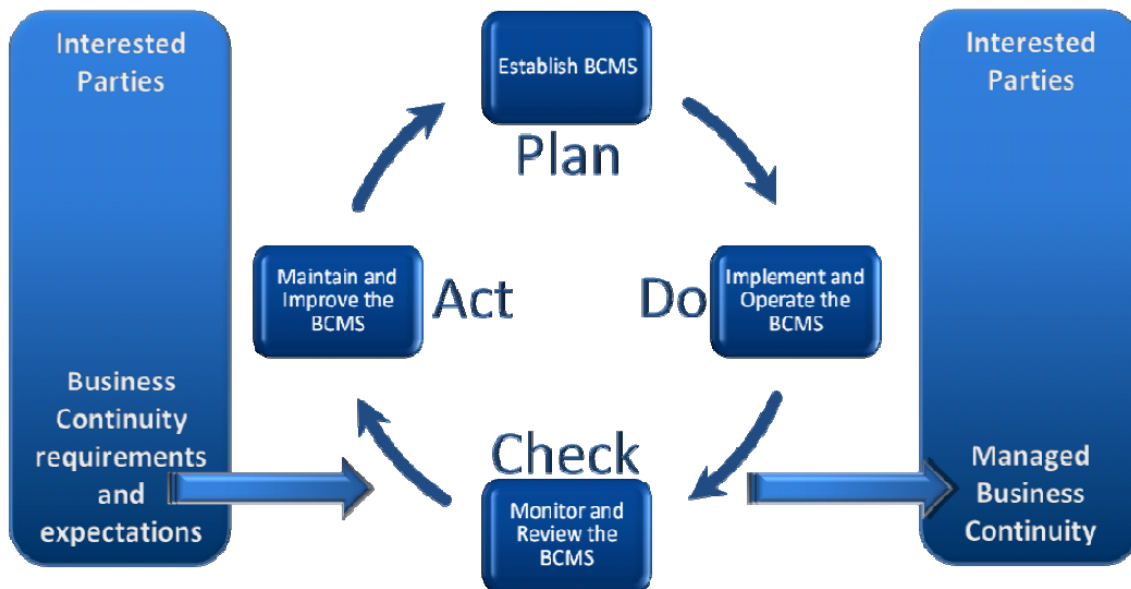


Figure 1 BS25999 Plan – Do –Check – Act Model

This is the classic BCMS process model that should be implemented for the ongoing management and improvement of the BCMS. However, in order to establish a BCMS and this PDCA model, there are several initial steps that an organisation must take.

## Implementing BS 25999

The approach to implementing BS 25999 is summarised in Figure 2. The steps required to implement BS 25999 are:

### 1 Business Continuity Policy and Scope

Define the scope of the BCMS and document and agree the organisation’s policy to Business Continuity Management, and the responsibilities within the organisation.

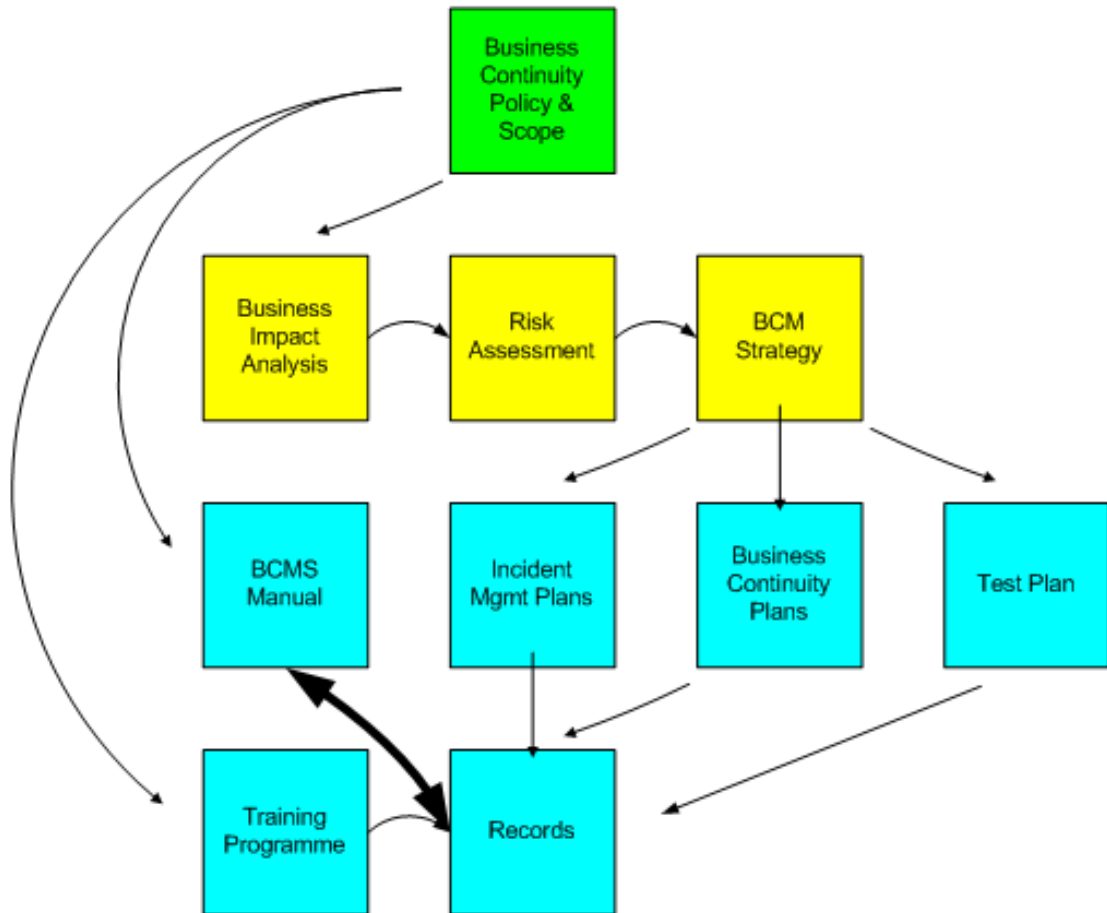


Figure 2. Implementing a BCMS

## 2 Business Impact Analysis

Determining the information and systems required by the organisation, how the business would be affected by their unavailability, and potential alternative ways of working.

## 3 Risk Analysis

Understanding the likelihood of the loss of critical information and systems.

## 4 BCM Strategy

Documenting the organisation's strategy for BCM in terms of:

- Risk mitigation strategies;
- Recovery Objectives;
- Recovery strategies (e.g. DR sites, data centre duplication etc.).

## **5 BCM Manual**

Detailing the responsibilities, processes and procedures required to implement the BCMS PDCA model, thereby ensuring the ongoing measurement and improvement of the BCMS.

## **6 Incident Management/Business Continuity Plans**

The exact requirements for these will vary from organisation to organisation, but will typically include a Crisis Management Plan and Communications plan for the whole organisation, Disaster Recovery Plans for key IT systems and services and Business Continuity Plans for one or more parts of the organisation.

## **7 Test Plan**

The overall plan for how the BCM plans are to be exercised, measured, and improved.

## **8 Training Programme**

Documented training requirements and how these are to be addressed.

## **9 Records**

The records to be maintained documenting the operation of the BCMS will be defined in the BCMS Manual. These are the key evidence of the implementation of the BCMS and are crucial for external independent audit.

## **10 Supporting Measures**

In addition to the above BCMS requirements, BS 25999 requires the following supporting measures which must be implemented:

- Document control
- Records management
- Internal audit

## ***Key Lessons Learnt***

Having implemented BS 25999 for a variety of organisations, we have identified a number of common key lessons for successful implementation.

### **Understand the Business Requirement**

It is important to understand and agree the business requirement for business continuity at an early stage, otherwise considerable effort can be spent developing BCM Strategies etc. that are later revised as the business need is re-defined.

## **Time & Effort from Across the Business**

Implementing an effective BCMS requires time and effort from all parts of an organisation, both to understand the business need for continuity and to develop meaningful impact analyses, risk assessments and continuity plans.

## **Internal Communication**

Two aspects of communication are key to success:

1. Communicating the progress of the BCMS project in order to gain and maintain engagement; and
2. The BCM Communications Plan is probably the most important document in any real crisis. Time spent getting this right is worth the effort.

## **The Documentation Should Match the Organisation**

No two organisations are the same. This is particularly true of BCM where the structure of the documentation needs to match the organisational structure and the business requirements for BCM.

## **Testing**

Exercising BC Plans is the most cost-effective way to ensure that they meet the organisation's needs, to gain engagement from all parts of the organisation, and to improve the plans in order to make them fit or purpose. Time spent testing is not time wasted.

## ***For More Information***

For more information contact:

Activity  
25 Hercules Way  
Aeropark  
Farnborough  
Hampshire  
GU14 6UU  
Tel 01252 377321  
Fax 01252 377670  
Email [info@activityim.com](mailto:info@activityim.com)  
Web [www.activityim.com](http://www.activityim.com)

## ***Biography of Author***

Neil O'Connor is Managing Director of Activity, which he founded in 2004 in response to the demand for independent security advice. With twenty years experience in information

Lessons Learnt from Implementing BS 25999 Business Continuity Management Systems

security, Neil started out in secure systems development and project management for secure Government projects.

For fifteen years Neil was an information security consultant advising clients such as the Ministry of Defence, Foreign & Commonwealth Office, NHS and a number of commercial clients. He fast became an expert in the management of information security and the implementation of ISO 27001.

In 1995 Neil began working for BT before establishing Claritas, an information security consultancy. It was sold to Diagonal plc in 2001, forming part of Diagonal Security, for whom Neil was Technical Director until 2004.

Neil has qualifications including an MA (Oxon) in Physics, and a diploma in management studies. He is a member of the CESG Listed Advisor Scheme (CLAS), and is an ISO 27001 auditor.

In his spare time Neil enjoys flying, photography, walking, and sailing.

## **About Activity**

Established in 2004, Activity is an independent specialist information security consultancy that helps commercial and public sector organisations protect their data networks, business information and online assets. Activity provides advice on best practice information security and business continuity strategies to a wide range of organisations from mid-sized companies to world leading enterprises, government institutions and public sector services. Activity's clients include the Ministry of Defence, Cabinet Office, Metropolitan Police Service, Atos Origin UK, Rolls-Royce.

## **Accreditations**

Activity is a member of the Council of Registered Ethical Security Testers (CREST) and the BSI Associate Consultant Programme. Many of its consultants are members of CESG CLAS scheme for security consultancy advice and are PRINCE2 qualified. All of Activity's services are independently certified to comply with the international standards for quality (ISO 9001) and information security management (ISO 27001).

## **Services**

### **Information Security Consultancy**

Assignments delivered by Activity include the development of security architectures; advice on the requirements for connection to the Government Secure Intranet (GSI); security risk and analysis and the development of security policies (including HMG-compliant policies).

### **Business Continuity Management**

Activity provides independent advice on crisis management, business continuity management and disaster recovery. Activity's business continuity services are BS 25999

Lessons Learnt from Implementing BS 25999 Business Continuity Management Systems

compliant and include business continuity document review and audit, business impact and analysis, the development of business continuity strategies, business continuity planning and testing, disaster recovery planning and testing.

## **ISO 27001**

Activity provides advice on ISO 27001 compliance, the international standard for Information Security Management Systems implementation, and enables organisations to achieve compliance with or certification against this standard. Activity helped Atos Origin UK gain ISO 27001 compliance in 2006, one of the largest companies to gain certification against the new international standard.

## **Information System Audit**

Activity provides a comprehensive service to review security risks, procedures and system implementation against legislative, regulatory and business requirements, to confirm that controls are effective and appropriate. This service covers all aspects of an IS Audit including:

- IT Governance & Compliance
- Risk Assessment
- IT Controls
- Business Continuity & Disaster Recovery
- Physical Environment
- Personnel and HR Procedures

## **Security Testing**

Activity provide a full range of security testing services that assess the technical threats to an organisation's networks and applications, from Network Penetration Tests and Host Configuration Assessments to Web Application Security Assessments and full Enterprise Application Security Reviews. Activity's structured and repeatable methodologies build on those provided by the CESG CHECK Scheme, OSSTM and OWASP.

## **End-to-End Security Review**

Activity deliver a technical security auditing programme that covers all aspects of the security enforcing components of an application encompassing physical, technical and procedural perspectives. The review may include an assessment of security design specifications, system documentation, implementation strategies, integration and operational management. It typically includes a combination of documentation reviews, interviews with key stakeholders, configuration reviews and a proactive technical assessment and analysis of the system itself.

Other security testing services provided by Activity include:

- Wireless security assessment
- Social engineering

Lessons Learnt from Implementing BS 25999 Business Continuity Management Systems

## Glossary

BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Planning