

# **ISO** **27001** **security**

## **Rôles and responsibilities** **for** **contingency planning**

Version 1

July 2008

Dr Gary Hinson PhD CISSP, CISM, CISA, MBA,  
CEO of IsecT Ltd.

And

Larry Kowalski, CISSP, ITIL  
Cybersecurity DR Program Office, IRS

### **Executive summary**

Drawing on ISO/IEC 27000-series standards and other references, this document describes the responsibilities and competencies commonly associated with Contingency, Business Continuity, Business Resumption and IT Disaster Recovery Planning rôles in large public or private sector organizations. While the rôles are often combined and simplified in smaller organizations, broadly similar principles generally apply.

## Contents

Section	Page
<b>1 Introduction</b> .....	<b>3</b>
1.1 Background, concepts and key terms .....	3
1.2 Scope and applicability of this document .....	4
1.3 Using this document – an important <i>caveat</i> .....	4
<b>2 Contingency Planning (CP) rôles and responsibilities</b> .....	<b>5</b>
2.1 CP Manager .....	5
2.2 CP Compliance Manager .....	5
2.3 CP Office .....	6
<b>3 Business Continuity Planning (BCP) and Business Resumption Planning (BRP) rôles and responsibilities</b> .....	<b>7</b>
3.1 BCP Manager.....	7
3.2 BRP Manager.....	7
3.3 BCP/BRP office .....	8
<b>4 IT Disaster Recovery Planning (DRP) rôles and responsibilities</b> .....	<b>9</b>
4.1 IT DRP Manager .....	9
4.2 IT DR Compliance Manager.....	9
4.3 IT DRP Test and Exercise Coordinator .....	10
4.4 IT DRP Development & Technical Assessment Manager .....	11
4.5 IT DR Office.....	11
<b>5 Other CP-related rôles and responsibilities</b> .....	<b>12</b>
5.1 Incident Management rôles.....	12
5.2 Crisis Management rôles.....	12
5.3 Incident and Crisis Management deputies, succession planning and job rotation .....	13
5.4 Information Asset Owners (IAOs).....	13
5.5 Custodians .....	13
5.6 BC Operations functions .....	14
5.7 IT DR Operations functions .....	14
<b>6 References and further reading</b> .....	<b>14</b>
<b>7 Feedback on this document</b> .....	<b>15</b>
<b>8 Acknowledgement</b> .....	<b>15</b>
<b>9 Copyright notice and disclaimer</b> .....	<b>15</b>

# 1 Introduction

## 1.1 Background, concepts and key terms

The fundamental basis of **Contingency Planning (CP)** is that, since all risks cannot be totally eliminated in practice, residual risks always remain. Despite the organization's very best efforts to avoid, prevent or mitigate them, incidents will still occur. Particular situations, combinations of adverse events or unanticipated threats and vulnerabilities may conspire to bypass or overwhelm even the best information security controls designed to ensure confidentiality, integrity and availability of information assets.

In the context of this document, CP is defined as the totality of activities, controls, processes, plans *etc.* relating to major incidents and disasters. It is the act of preparing for major incidents and disasters, formulating flexible plans and marshaling suitable resources that will come into play in the event, whatever actually eventuates. The very word 'contingency' implies that the activities and resources that will be required following major incidents or disasters are contingent (depend) on the exact nature of the incidents and disasters that actually unfold. In this sense, CP involves preparing for the unexpected and planning for the unknown.

The basic purpose of CP is to minimize the adverse consequences or impacts of incidents and disasters. Within the field of CP, a number of more specific terms and activities are distinguished in this document and form the basis of rôles identified below:

- **Availability Management and Continuity Planning** practices involve resilience measures designed to keep essential business processes and the supporting IT infrastructure running despite incidents and (limited) disasters:
  - **Business Continuity Planning (BCP)** involves measures to ensure, as far as possible, that critical business processes continue to operate satisfactorily despite a wide range of incidents. This includes aspects such as running parallel activities at disparate locations, using deputies and understudies, having alternative suppliers *etc.*;
  - **IT Continuity Planning (ITCP)** involves measures to ensure that, as far as possible, IT systems, networks and associated infrastructure and processes supporting critical business processes remain in operation despite disasters. This includes aspects such as fault tolerant, resilient or high availability system/network designs and configurations, built-in redundancy and automated failover of the supporting IT systems, capacity and performance management *etc.*
- **Recovery and Resumption Planning** relates to recovering or resuming business and IT operations following incidents and disasters, typically from alternative locations, using fallback equipment *etc.*:
  - **Business Resumption Planning (BRP)** involves planning to resume or restore critical and important business processes to something approaching normality following disasters or major incident that overwhelm the resilience capabilities noted above. This includes activities such as relocating employees to alternative office locations, manual fallback processing, temporary relaxation of divisions of responsibility and delegated authorities *etc.*;
  - **IT Disaster Recovery Planning (IT DRP)** involves planning for the recovery of critical IT systems and services in a fallback situation following a disaster that overwhelms the resilience arrangements; examples include manually restoring IT systems and data on alternate/standby equipment from backups or archives, utilizing emergency communications facilities *etc.*
- **Incident and Crisis Management** activities are focused on managing incident and disaster scenarios "live", as they occur:

- **Incident Management (IM)** involves activities and processes designed to evaluate and respond to information security-related incidents of all sorts. Most IM activities are routinely exercised in the normal course of business, dealing with all manner of minor incidents. Best practice proactive IM processes incorporate ‘corporate learning’ through continuously updating the processes, systems and controls, and improving resilience and recovery activities in response to actual incidents and disasters plus near misses;
- **Crisis Management (CM)** involves emergency management activities associated with the management of major incidents and crises, primarily relating to health and safety aspects. Key activities in the crisis phase typically include preliminary assessment of the situation, liaison with emergency services and management, and (in the case of serious incidents) invocation of relevant BRP and IT DR plans. Quickly forming a competent crisis management group/team to manage and control ongoing recovery activities is an important element of CM.

It is important to appreciate that planning and preparation are key to all CP-related activities. While many of us anticipate being able to deal with and get through crisis situations to some extent on-the-fly, CP aims to prepare suitable plans and stockpile essential resources in advance of any crisis to make the situation more manageable and less disruptive on the day. Furthermore, while it is sensible to prepare thoroughly for commonplace incidents (such as interruptions to power or telecommunications services), true CP includes an element of preparing for totally unanticipated events, for example pre-determining the crisis management structure and processes to assess and react appropriately to any incident more efficiently than if no such preparations had been made.

## 1.2 Scope and applicability of this document

The specific rôles and responsibilities identified in this document apply primarily to large organizations such as multinationals in the private sector or large government departments. Large organizations have both the resources and the availability requirements to justify the allocation of dedicated full-time professionals to the associated CP tasks. Small to medium-sized enterprises typically perform broadly similar functions using fewer individuals, many of whom may work part-time on particular elements of CP and may or may not be as highly qualified. In the extreme, micro businesses with just a small handful of employees may assign all CP responsibilities to a single employee, albeit ideally with a deputy or fallback.

With due consideration by management and adaptation to suit the specific requirements, the descriptions of key activities and competencies in this document may be used to develop job descriptions, vacancy notices *etc.* for CP-related rôles. In practice, organizations that most closely match the scope description above have probably already defined a number of CP-related rôles but may not have taken account of the full range of activities described here, meaning that some review and updating of job descriptions *etc.* may be in order. Other organizations are less likely to have such a comprehensive approach to CP and may also benefit from reviewing their governance structures and job descriptions, looking particularly at any significant gaps in coverage.

## 1.3 Using this document – an important caveat

This document is provided purely for information and discussion purposes. The rôles and competencies explained in the remainder of this document are generic. The document is unlikely to fulfill any specific organization’s requirements without some adaptation and customization which may be extensive. **Readers are encouraged to make use of the references and further reading listed towards the end, and/or to call upon qualified and competent employees or consultants with expertise in CP to flesh out the details.** Please read the [copyright notice and disclaimer](#) for more.

The competencies below refer to three ‘levels’ of knowledge and expertise in various topics, namely: **expert knowledge** (the level of knowledge expected of an expert in the field with at least ten years’ work experience and relevant qualifications); **detailed knowledge** (between expert but

and working knowledge, perhaps supported by relevant qualifications); and **working knowledge** (expected of someone with at least one or two years' work experience in the field).

## 2 Contingency Planning (CP) rôles and responsibilities

### 2.1 CP Manager

While most CP-related activities fall to the individual subsidiary functions listed below, there is generally a need for a senior manager to manage, direct and control the CP activities as a whole.

#### 2.1.1 Key activities:

- Liaise between and coordinating various internal and external stakeholders (such as senior management, key customers, suppliers and business partners, employee representatives and third party service/equipment suppliers) to elucidate the CP requirements and capabilities, using rational Business Impact Analysis (BIA) processes to 'normalize' and prioritize CP requirements on behalf of the organization as a whole, and form the big picture of CP requirements in relation to normal operational and strategic activities;
- Identify shortfalls in funding and progress, or unmanaged risks that threaten the success of CP activities, and working with management to address and resolve these issues;
- Take a strategic enterprise-wide view of CP, developing broad strategies and policies for CP that complement and support other routine business strategies, risk and security management objectives, IT DR policies *etc.*;
- Implement suitable management, control, directive and monitoring arrangements to govern the CP activities (with a large CP team, this is likely to include interviewing and appointing a number of managers, coordinators, team leaders *etc.* to lead the various CP activities).

#### 2.1.2 Competencies:

- Expert knowledge of CP;
- Detailed knowledge of the organization's management structure, business strategies *etc.*;
- Working knowledge of project management, IT DCP/DRP *etc.*;
- Demonstrated leadership ability;
- Able to communicate calmly, effectively and authoritatively, including in a crisis.

### 2.2 CP Compliance Manager

The CP Compliance Manager supports the CP Manager in both achieving and demonstrating compliance with CP policies, strategies, standards *etc.*

#### 2.2.1 Key activities:

- Manage routine CP management reporting, drawing relevant information from BIAs, plans, incidents, disasters, exercises *etc.* plus the wider context from legal, regulatory and standards bodies (*e.g.* legislative changes);
- Develop and help deliver CP training and awareness activities;
- Assist with BIA and test/exercise planning, determining any associated compliance requirements (*e.g.* legal obligations to conduct a certain number and type of exercise each year).

### 2.2.2 Competencies:

- Detailed knowledge of CP, ideally evidenced by relevant qualifications and experience;
- Detailed knowledge of corporate policies, laws and regulations governing CP;
- Detailed knowledge of Certification and Accreditation (C&A) process and requirements [where relevant];
- Working knowledge of critical business processes and relative priorities;
- Able to articulate and explain CP policies in operational terms, and identify CP training and awareness needs plus cost effective training and awareness methods;
- Able to develop, measure and report suitable CP metrics;
- Business writing, presenting and related communications skills.

## 2.3 CP Office

As well as the Incident Manager, Crisis Coordinator, BCP Manager, BRP Manager, IT DRP manager and others, the CP Manager in large organizations may be supported by a dedicated CP Management Office and/or subsidiary functions providing project management support to other CP-related functions such as BCP and IT DRP.

### 2.3.1 Key activities:

- Help build a 'center of excellence' for CP - a focal point in the organization offering internal consultancy support and direction on CP matters with help from BC/BR managers and other experts;
- Design and build inventories of critical processes, supporting IT systems *etc.*;
- Schedule and arrange meetings for CP managers with IAOs and other business people;
- Guide and support the creation of reasonably consistent, comprehensive and high quality contingency plans throughout the enterprise, particularly in respect of critical business processes and the associated supporting/enabling functions;
- Assist with the drafting of CP-related policies, standards, procedures and guidelines;
- Perform or support others in the identification and management of CP project-related risks;
- Assist with the creation of budget requests/proposals, business cases *etc.* for various CP activities;
- Monitor and prepare management reports on CP-related plans, progress to plans, budgets, risks and opportunities;
- Assist with the coordination and/or delivery of CP-related awareness, training and educational activities, exercises/tests *etc.*;
- Assist in a crisis to implement CP plans, address operational issues, communicate clearly and effectively *etc.*

### 2.3.2 Competencies:

- Working knowledge of CP, BC, BR, IT DRP *etc.*;
- Able to forge and maintain productive working relationships with other business people;
- General administrative skills, with some exposure to project management, metrics/management reporting *etc.*;
- An eye for detail, sufficiently diligent, persistent and efficient to complete assigned activities properly within realistic timeframes;

- Able to communicate calmly, effectively and authoritatively, including in a crisis.

## 3 Business Continuity Planning (BCP) and Business Resumption Planning (BRP) rôles and responsibilities

### 3.1 BCP Manager

The BCP Manager's primary focus is on ensuring that critical business processes are sufficiently resilient to continue operating effectively despite incidents.

#### 3.1.1 Key activities:

- Manage the overall BCP process;
- Advise and assist IAOs, BRP/IT DRP managers and others with BCP matters;
- Assess and prioritize business processes from the resilience/availability perspective;
- Determine/specify resilience requirements, taking into account interdependencies between processes and IT systems support aspects, and prepare BC plans;
- Help justify any additional investment required in BC arrangements by helping to prepare investment proposals, business cases, budget proposals *etc.*;
- Ensure that BC plans are prepared to a consistent level of quality, accuracy, completeness and detail, typically by preparing suitable templates.

#### 3.1.2 Competencies:

- Expert knowledge of BCP;
- Detailed knowledge of BRP;
- Working knowledge of the organization's critical business processes, policies, risk appetite *etc.*;
- Working knowledge of CP and IT DRP;
- Working knowledge of the organization's investment/financial management practices.
- Able to communicate calmly, effectively and authoritatively, including in a crisis.

### 3.2 BRP Manager

The BRP Manager's rôle emphasizes the timely restoration of business processes following a disaster.

#### 3.2.1 Key activities:

- Manage the overall BRP process;
- Collaborate with IAOs, BCP and IT DRP colleagues on BRP matters;
- Assess and prioritize business processes from the recovery perspective;
- Determine recovery requirements, taking into account interdependencies between processes and IT systems support aspects;
- Justify any additional investment required in BRP;
- Prepare BR plans.

### 3.2.2 Competencies:

- Expert knowledge of BRP;
- Detailed knowledge of BCP;
- Working knowledge of the organization's critical business processes;
- Working knowledge of CP and IT DRP;
- Able to develop sound business cases;
- Able to communicate calmly, effectively and authoritatively, including in a crisis.

### 3.3 BCP/BRP office

Depending on the amount of work involved, the BCP and BRP Managers may need the support of an administrative staff. [Note: the BCP/DRP office may be part of the CP Office noted above.]

#### 3.3.1 Key activities:

- Help build a 'center of excellence' for BC/BR - a focal point in the organization offering internal consultancy support and direction on BC/BR matters with help from BC/BR managers and other experts;
- Maintain inventories of critical processes, supporting IT systems *etc.*;
- Schedule and arrange meetings for their managers with IAOs and other business people;
- Guide and support the creation of reasonably consistent, comprehensive and high quality BC/BR plans throughout the enterprise, particularly in respect of critical business processes and the associated supporting/enabling functions;
- Assist with the drafting of BC/BR-related policies, standards, procedures and guidelines;
- Perform or support others in the identification and management of BC/BR project-related risks;
- Assist with the creation of budget requests/proposals, business cases *etc.* for various BC/BR activities;
- Monitor and prepare management reports on BC/BR-related plans, progress to plans, budgets, risks and opportunities;
- Assist with the coordination and/or delivery of BC/BR-related awareness, training and educational activities, exercises/tests *etc.*;
- Assist in a crisis to implement BC/BR plans, address operational issues, communicate clearly and effectively *etc.*

#### 3.3.2 Competencies:

- Working knowledge of BC, BR, CP, IT DRP *etc.*;
- Able to forge and maintain productive working relationships with other business people;
- General administrative skills, with some exposure to project management, metrics/management reporting *etc.*;
- An eye for detail, sufficiently diligent, persistent and efficient to complete assigned activities properly within realistic timeframes;
- Able to communicate calmly, effectively and authoritatively, including in a crisis.

## 4 IT Disaster Recovery Planning (DRP) rôles and responsibilities

### 4.1 IT DRP Manager

The IT DRP Manager has overall responsibilities for managing and directing IT DRP.

#### 4.1.1 Key activities:

- Coordinate stakeholder participation in DR planning and works with IAOs to prioritize critical business processes;
- Manage DR program resources;
- Define the principles, policies and procedures necessary to support or reconstitute essential business functions after a catastrophic event;
- Develop programs of business impact assessment, compliance, training, testing and exercising, technical assessment and plan development;
- Implement DR policies through DR arrangements such as regular data backups; secure data archival; backup restoration; secure on- and off-site storage of backup media; provision of alternative IT processing facilities, networks *etc.*;
- Evaluate the overall IT DRP program and state of readiness of IT in relation to BRP and broader CP requirements.

#### 4.1.2 Competencies:

- Expert knowledge of IT DRP;
- Detailed knowledge of the IT systems, networks and applications supporting critical business processes;
- Detailed knowledge of project management;
- Working knowledge of CP, BCP and BRP;
- Working knowledge of the organization's critical business processes;
- Working knowledge of certification and accreditation processes [in situations where IT DR plans have to be independently assessed and certified against enterprise-wide criteria and, in some cases, legal/regulatory obligations];
- Working knowledge of procurement policies and practices;
- Able to contribute proactively to Business Impact Analysis (BIA);
- Able to communicate calmly, effectively and authoritatively, including in a crisis.

### 4.2 IT DR Compliance Manager

The IT DR Compliance Manager helps the IT DRP Manager to achieve and demonstrate compliance with IT DR policies.

#### 4.2.1 Key activities:

- Manage routine IT DR reporting, drawing relevant information from BIAs, plans, incidents, disasters, exercises *etc.* plus the wider context from legal, regulatory and standards bodies (*e.g.* legislative changes);
- Assist with the delivery of IT DR training and awareness activities;

- Assists with BIA and test/exercise planning, determining any associated compliance requirements (e.g. legal obligations to conduct a certain number and type exercise each year);

#### 4.2.2 Competencies:

- Detailed knowledge of compliance practices;
- Detailed knowledge of corporate policies, laws and regulations governing IT DRP;
- Detailed knowledge of IT DR planning as a discipline, ideally evidenced by relevant qualifications and experience;
- Detailed knowledge of Certification and Accreditation (C&A) process and requirements [where relevant];
- Working knowledge of critical business processes and relative priorities;
- Able to articulate and explain IT DR policies in operational terms
- Able to help deliver IT DR training and awareness;
- Business writing, presenting and related communications skills.

### 4.3 IT DRP Test and Exercise Coordinator

The IT DRP Test and Exercise Coordinator assists the IT DRP Manager to design and conduct testing, awareness, training and educational processes associated with IT DRP in accordance with legal, regulatory and business requirements for assurance of CP.

#### 4.3.1 Key activities:

- Design, plan/schedule and coordinate IT DRP tests (primarily focused on testing correct operation of the DR technologies) and exercises (primarily focused on training people in IT DR-related procedures and activities), evaluating their effectiveness and promoting any improvement activities that are considered necessary to meet the CP objectives;
- Manage the resources required for tests and exercises;
- Liaise between the IT DRP Manager, IT DR Office, various IT professionals, information asset owners, BC and DR managers *etc.* on all matters related to IT DRP tests and exercises, including planning, execution and management reporting. He/she marshals IT and other resources required, and evaluates the effectiveness of IT DR tests and exercises, providing constructive feedback.

#### 4.3.2 Competencies:

- Detailed knowledge of laws, regulations and business requirements regarding CP assurance requirements for proving IT DRP elements of CP;
- Working knowledge of information security controls related to CP and IT DRP;
- Working knowledge of critical business processes and their relative priorities;
- Working knowledge of C&A processes (where relevant);
- Able to design IT DRP test/exercise plans, scenarios and metrics;
- Able to schedule, manage and deliver the IT DRP test/exercise program;
- Skill in designing effective IT DR tests/exercises that provide the desired level of assurance whilst minimizing unnecessary testing costs and risks;
- Able to coordinate activities of various stakeholders and participants in test/exercise scenarios;

- Analytical skill to evaluate the outcomes of IT DR exercises and tests against expectations.

#### 4.4 IT DRP Development & Technical Assessment Manager

The IT DRP Development & Technical Assessment Manager assists the IT DRP Manager, IAOs *etc.*, providing guidance in the creation of adequate IT DR plans and assessing technical requirements for effective recovery.

##### 4.4.1 Key activities:

- Design assessment tools to determine the appropriate level of recovery services;
- Translate IT DR requirements into DR plans by assisting IAOs through the IT system development life cycle;
- Evaluate resilience and recovery capabilities and risks inherent in the IT infrastructure;
- Correlate DR requirements in Service Level Agreements (SLAs), contracts and other express requirements (*e.g.* laws and regulations) against IT DR plans;
- Promote the use of new technologies and processes in support of IT DR.

##### 4.4.2 Competencies:

- Expert knowledge of IT DRP;
- Working knowledge of critical business processes and priorities;
- Working knowledge of SLAs, contracts and Memoranda of Understanding (MOUs);
- Working knowledge of the system development life cycle and project management;
- Able to design and develop realistic IT DR plans;
- Able to assess the effectiveness of proposed IT DR technologies, methods and approaches against requirements determined by BIA and other assessments.

#### 4.5 IT DR Office

Depending on the amount of work involved in managing IT DR plans and activities, a staff may be necessary to support the IT DR Managers. [Note: the IT DR Office may be part of the CP Office noted earlier, but is more usually sited within the IT function, perhaps within the IT Project Management Office.]

##### 4.5.1 Key activities:

- Help build a 'center of excellence' for IT DR - a focal point in the organization offering internal consultancy support and direction on IT DR matters with help from IT DR managers and other experts;
- Maintain inventories of IT systems, services *etc.* supporting critical business processes;
- Schedule and arrange meetings for their managers with IAOs and other business people;
- Guide and support the creation of reasonably consistent, comprehensive and high quality IT DR plans throughout the enterprise, particularly in respect of critical IT systems and services;
- Assist with the drafting of IT DR-related policies, standards, procedures and guidelines;
- Perform or support others in the identification and management of IT DR project-related risks;
- Assist with the creation of budget requests/proposals, business cases *etc.* for various IT DR activities;

- Monitor and prepare management reports on IT DR-related plans, progress to plans, budgets, risks and opportunities;
- Assist with the coordination and/or delivery of IT DR-related awareness, training and educational activities, exercises/tests *etc.*;
- Assist in a crisis to implement IT DR plans, address operational issues, communicate clearly and effectively *etc.*

#### 4.5.2 Competencies:

- Working knowledge of BC, BR, CP, IT DRP *etc.*;
- Able to forge and maintain productive working relationships with other business people;
- General administrative skills, with some exposure to project management, metrics/management reporting *etc.*;
- An eye for detail, sufficiently diligent, persistent and efficient to complete assigned activities properly within realistic timeframes;
- Able to communicate calmly, effectively and authoritatively, including in a crisis.

## 5 Other CP-related rôles and responsibilities

A number of other business functions typically play supporting rôles in respect of IM, CM, BCP, BRP and IT DRP. While they may not necessarily appreciate their relevance to contingency management, following an incident or crisis they will be expected to assist with the recovery activities.

### 5.1 Incident Management rôles

Incident management is a normal part of routine business operations, for example dealing with minor outages, other information security incidents and near-misses. Incident management processes, rôles and responsibilities therefore mostly fall outside the sphere of contingency planning, except in the case of more severe incidents. Whereas routine incident management activities are likely to be quite well practiced in the average corporation, exceptional events (such as major physical or logical/T incidents) may require different activities that are unlikely to be as familiar and well-rehearsed. In particular, management must give some thought to the possibility that the usual incident manager/s may not be available during or following a major incident.

### 5.2 Crisis Management rôles

As with incident management, crisis management may be seen as an extension of normal operational activities. Under normal circumstances, a number of individuals are normally appointed and trained to fulfill rôles such as:

- Building Evacuation Manager/Crisis Coordinator;
- Fire Warden;
- First Aider;
- Physical/Site Security Guard *etc.*
- Damage Assessor or Damage Assessment Team Leader.

The organization should ensure that such individuals are sufficiently well prepared to act appropriately under exceptional circumstances following a major incident, and that there are sufficient trained and prepared individuals to cope reasonably well with exceptional incidents (this

may be taken to imply the need for basic crisis management training for all employees, ranging from typical building evacuation procedures to fire fighting and first aid where appropriate).

### 5.3 Incident and Crisis Management deputies, succession planning and job rotation

In addition to the primary incident and crisis managers, suitable deputies should ideally be appointed and trained to take the lead if the primary manager/s is/are unavailable (whether involved in the incident or otherwise engaged *e.g.* off sick, on holiday or simply overloaded). Succession planning is recommended for all key rôles in the organization but has special significance in relation to serious incidents. Some organizations for example operate a deliberate policy of job rotation to expose multiple employees to such critical rôles, sharing knowledge and spreading competencies.

### 5.4 Information Asset Owners (IAOs)

“Owners” of critical information assets including vital business processes *etc.* have a rôle in specifying availability (both resilience and recovery) requirements as a result of following the BIA process, and funding the associated controls. While strictly speaking the body corporate may be the legal owner of all corporate assets, Information Asset Owners (IAOs) within the organization are normally held personally accountable by management and other stakeholders for adequate protection of the information assets under their remit. This often includes information assets belonging to third parties but placed in the care of the organization (*e.g.* personal data relating to customers).

Using the organization’s BIA process, IAOs focus on the BC aspects of CP, typically relying on Custodians and IT DR specialists to elaborate and supply the corresponding IT DR elements. They plan and coordinate BC activities, specify business objectives for availability (normally in terms of resiliency, Recovery Point Objectives, Recovery Time Objectives *etc.*), allocate resources for BC and perhaps IT DR activities, and evaluate the results of DR tests against their requirements.

IAO competencies include:

- Deep knowledge of critical business processes under their remit, and a reasonable understanding of their prioritization in relation to other business processes
- Working knowledge of IT systems and other resources supporting their critical business processes;
- General understanding of CP, including resilience and IT DR as complementary aspects of CP;
- General knowledge of IT DR test procedures and exercises necessary to provide sufficient assurance that the resilience and IT DR arrangements satisfy the organization’s availability requirements;
- Working knowledge of the IT systems development life cycle (such that IT DRP arrangements remain closely aligned with BC requirements as IT systems change);
- Ability to perform BIA, normally in conjunction with expert advisors drawn from the BC/DRP teams, Risk Management, Information Security Management *etc.*

### 5.5 Custodians

Following BIA, responsibilities relating to the operation and protection/security of information assets supporting critical business processes are normally delegated to Custodians, typically within IT Department for IT systems and networks.

While Custodians are not formally accountable for providing and proving the adequacy of IT DRP and other contingency arrangements, they do have a professional duty to identify and resolve issues in their domain of expertise and/or bring residual risks to the attention of management,

including IAOs, BC Managers *etc.* This is especially important in the case of complex technical IT DRP configurations where IT people who are familiar with the technologies are more likely to notice technical issues, dependencies *etc.* that would render the arrangements ineffective in a genuine DR scenario.

## 5.6 BC Operations functions

These are the people who operate maintained or restored business processes in contingency situations following incidents and disasters. They are most likely to be ordinary employees but some may be operating in unfamiliar areas, for example covering for other employees who are unable to work normally through injury, incapacity or other non-availability.

Such people have responsibilities to get actively involved in relevant BC and/or IT DRP exercises, identify non-technical issues, dependencies *etc.* that would render the arrangements ineffective in a genuine DR scenario, and bring these to the attention of the relevant managers.

## 5.7 IT DR Operations functions

These are the people who perform IT recovery tasks such as configuring standby/recovery systems for use, restoring backups from offline media, verifying the restored data and releasing systems for production use. Again, they are most likely to be ordinary IT employees, network/system managers, operators *etc.* but may be operating in unfamiliar areas, for example covering for other IT employees who are unable to work normally through injury, incapacity or other non-availability.

The IT DR rôles encompass many operational functions *e.g.* system/application administration, database administration, network and telecommunications, procurement, server replenishment, IT Help/Service Desk *etc.* In such rôles, employees:

- Implement the IT DR plans, both in tests and in actual incidents;
- Evaluate the effectiveness of IT DR processes in tests and in actual events, providing feedback and lessons learned to update the plans.

IT DR Ops competencies include:

- Working knowledge of critical business processes, recovery priorities and supporting IT systems *etc.*;
- Detailed knowledge of DR plans and procedures for IT systems *etc.* for which they have recovery responsibilities, plus specific/expert knowledge of the associated hardware platforms, operating systems, middleware, application software, configurations *etc.*;
- Able to identify weaknesses in DR processes and suggest realistic remedies, for example as the result of DR tests or exercises.

## 6 References and further reading

Item	Relevance
BS 27999-1:2006 and BS 27999-2:2007	British Standard 25999 part 1, " <a href="#">Business Continuity Management Code of Practice</a> ", establishes the process, principles and terminology of business continuity management and provides a comprehensive set of best practice BCM controls covering the whole BCM lifecycle. BS 25999 part 2, " <a href="#">Business Continuity Management Specification</a> ", is a more formal BCM certification standard.

Item	Relevance
PAS 77:2006	Publicly Available Specification 77, " <a href="#">IT Service Continuity Management Code of Practice</a> ", provides guidance on ensuring continuity of vital IT services.
NIST SP 800-34:2002	NIST's Special Publication 800-34, " <a href="#">Contingency Planning Guide for Information Technology Systems</a> ", provides advice for interim measures to recover US government IT services following an emergency or system disruption.
ISO/IEC 27002:2005	The ISO/IEC standard " <a href="#">Information technology -- Security techniques -- Code of Practice for Information Security Management</a> " covers business continuity management in section 14.

## 7 Feedback on this document

You are encouraged to contribute to the continued development and refinement of this document by returning comments and improvement suggestions directly to its author ([Gary@isect.com](mailto:Gary@isect.com)) or discussing it through the ISO27k Implementers' Forum at [www.ISO27001security.com](http://www.ISO27001security.com).

While we cannot notify you if the document is updated, any such updates will normally be released through the ISO27k Toolkit page at [www.ISO27001security.com](http://www.ISO27001security.com). Please visit the website at least once a month and/or check the "What's new?" page for details of any updates.

## 8 Acknowledgement

This paper was based on an excellent DR training strategy document kindly supplied by Larry Kowalski of the US Internal Revenue Service's Cybersecurity DR Program Office. Gary Hinson reformatted and slightly extended the document for the purposes of the ISO27k Toolkit but remains extremely grateful for the generous intellectual input that prompted this work. Thanks Larry!

## 9 Copyright notice and disclaimer

As stated in the scope and applicability section above, this document is a generic example for discussion and consideration. **This document is very unlikely to be entirely sufficient or suitable for any specific organization without customization.** It is generic in nature, incorporating a selection of commonplace rôles and responsibilities relating to contingency planning in large organizations. Because it is generic, it cannot fully reflect every organization's requirements. We are not familiar with your specific circumstances and cannot offer tailored guidance to suit your particular needs. It is certainly not legal advice and is unlikely to reflect fully any legal or regulatory obligations on an organization to prepare suitable contingency arrangements.



This work is copyright © 2008, [ISO27k implementers' forum](#), some rights reserved. The authors have donated this document to the ISO27k Toolkit at [www.ISO27001security.com](http://www.ISO27001security.com). It is licensed under the [Creative Commons Attribution-NonCommercial-Share Alike 3.0 License](#).



You are welcome to reproduce, circulate, use and create derivative works from this *provided* that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the [ISO27k implementers' forum](#) at [www.ISO27001security.com](http://www.ISO27001security.com), and (c) any derivative works are shared under the same terms as this.