|  |  |
| --- | --- |
| Roles and Responsibilities  for  Contingency Planning | Pradhap R /It22337108  Cyber Security - Year 3, Semester 2 |

Executive summary

These roles in large publicly or privately sector organizations are described in this document, which draws on ISO/IEC 27000-series guidelines and other references to describe the common responsibilities and competencies associated with backup plan, business continuity, business resume, and IT disaster recovery planning roles. Smaller companies may have fewer roles due to a lack of resources, but the underlying concepts remain the same.

# Introduction

## Background, concepts and key terms

CP is built on the premise that because no risk can be completely removed in reality, there will always be some residual risk. Accidents will happen, no matter how hard the organization tries to prevent them. Even the strongest information security measures intended to guarantee confidentiality, integrity, and availability of information assets may be bypassed or overwhelmed by a mix of unfavorable events, unexpected threats, and vulnerabilities.

For the purposes of this paper, CP refers to everything that goes into a significant event or catastrophe, including activities, controls, procedures, plans, and so on. Preparation for big events and disasters, including developing flexible strategies and assembling appropriate resources, will be critical no matter what happens. According to this definition, contingency plans assume that the actions and resources needed to respond to significant events or disasters will be determined by how such incidents or disasters develop. CP, therefore, is about being ready for everything, including the unexpected.

CP's primary goal is to lessen the negative effects and repercussions of events and catastrophes as much as possible. A number of CP-specific terminology and actions are highlighted in this paper, which serve as the foundation for the roles described below.

Availability Management and Continuity Planning In order to keep the critical business operations and supporting IT infrastructure operating in the face of events and (limited) disasters, practices include resilience measures.

* + Business Continuity Planning- Measures are taken to guarantee that key business processes, notwithstanding various events, continue to function properly as far as feasible as part of (BCP). These characteristics include, but are not limited to, the use of deputies and understudies, as well as having alternate vendors and suppliers.
  + IT Continuity Planning- In order to keep IT systems, networks, and related infrastructure and procedures supporting key business activities running as long as possible in the face of catastrophes, (ITCP) takes steps to guarantee that they do not go down. Included are things like designing and configuring fault-tolerant, robust, or high-availability system/network setups, adding redundancy, and automating IT system failover.

Recuperation and Resume It's important to plan for recovering or restarting business and IT activities after catastrophes, usually from other locations and with backup equipment.

* Business Resumption Planning- When catastrophes or significant incidents overwhelm a company's resilience, business recovery planning (BRP) is necessary. This includes making plans to restart or restore essential and crucial business operations to near-normality. Relocating workers to alternate office locations, using manual fallback processing, and temporarily easing off on the delegation of authority are all examples of this kind of activity.
* IT Disaster Recovery Planning- In the aftermath of a catastrophe that overwhelms the resilience preparations, (IT DRP) includes preparing for the recovery of key IT systems and services using alternate/standby equipment from backups or archives, using emergency communications facilities, etc.

Incident and Crisis Management There is an emphasis on incident and catastrophe management "on the fly," as they occur

* There are various activities and processes involved in Incident Management (IM), all designed to evaluate and respond to various types of information security-related incidents. The majority of IM operations are carried out in the course of business as usual, dealing with a wide range of insignificant issues. As part of best practice proactive IM, processes include "corporate learning" through the continuous update of processes, systems, and controls, as well as improving resilience and recovery activities in response to actual incidents and disaster plus near misses.
* Crisis Management (CM) includes emergency management activities associated with the management of major incidents and crises, primarily relating to health and safety aspects. Critical activities during the crisis phase include assessing the situation and communicating with emergency services and management, as well as invoking BRP and IT DR plans when necessary (especially in the event of a serious incident). CM relies heavily on quickly assembling a capable crisis management group or team to oversee and manage ongoing recovery efforts.

All CP-related actions need careful planning and preparation, and this must be understood. Even though many of us expect to be able to cope with and get through crisis circumstances on the fly, CP intends to create appropriate preparations and store necessary resources in advance of any crisis to make the situation more manageable and less disruptive on the day. CP also includes preparing for unanticipated events, such as pre-determining the crisis management structure and processes in order to assess and respond to any incident more efficiently than if no such preparations had been made, even though commonplace incidents (such as power or telecommunications service interruptions) should be thoroughly prepared for.

## Scope and applicability of this document

# For big organizations like multinational corporations or government agencies, the roles and duties described in this text are particularly relevant. Organizations with a lot of resources have the availability needs, which allows them to allocate full-time staff members to the CP activities involved. The tasks performed by small and medium-sized businesses are often comparable since they have fewer employees that work part-time on certain CP components and are either less qualified or more competent. Smaller companies may be able to delegate all of the CP duties to one person, but it is preferable to have a deputy or backup.

# The definitions of essential tasks and skills in this paper may be used to create job descriptions, vacancy announcements, etc. for CP-related roles with appropriate consideration by management and modification to fit the particular needs. Companies that best fit the scope definition above may have previously established certain roles linked to customer service, but they may not have taken into consideration the entire range of tasks mentioned below, requiring a re-evaluation of job descriptions and other documents. Organizations with a less complete approach to corporate citizenship may benefit from reexamining their governance structures and job descriptions, paying special attention to any major coverage holes.

# Contingency Planning (CP) roles and responsibilities

## CP Manager

Most CP-related tasks are handled by the following subsidiary functions, although a senior manager is usually required to oversee, lead, and supervise all CP-related activities.

### **Key activities.**

• Liaise with and coordinate various internal and external stakeholders (such as senior management, key customers, suppliers and business partners, employee representatives, and third-party service/equipment suppliers) to clarify CP requirements and capabilities, utilizing rational Business Impact Analysis (BIA) processes to ‘normalize' and prioritize CP requirements on behalf of the organization.

• Work with management to identify financial and progress shortages, as well as uncontrolled risks, that jeopardize the effectiveness of CP operations, and address and resolve these problems.

• Develop broad CP plans and policies that complement and support other regular business goals, risk and security management objectives, IT disaster recovery policies, and so forth.

• Establish appropriate management, control, direction, and monitoring procedures to oversee CP operations (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).

### **Competencies.**

* Working knowledge of project management, IT DCP/DRP, and other related topics
* Expert understanding of CP
* Detailed knowledge of the organization's management structure, business strategy, and other related topics.
* Demonstrated capacity to lead
* Able to speak calmly, efficiently, and authoritatively, even in a crisis

## CP Compliance Manager

The CP Compliance Manager assists the CP Manager in attaining and proving CP policies, strategies, and standards compliance.

### **Key activities**.

* Oversee regular CP management reporting, including data from BIAs, plans, events, catastrophes, exercises, and other sources, as well as the larger context provided by legal, regulatory, and standards organizations
* Assist with BIA and test/exercise planning, identifying any related compliance needs
* Develop and assist administer CP training and awareness initiatives (e.g. legal obligations to conduct a certain number and type of exercise each year).

### **Competencies.**

* Detailed understanding of CP, preferably shown by appropriate credentials and experience
* Detailed knowledge of company policies, rules, and regulations regulating CP.
* Detailed knowledge of the Certification and Accreditation (C&A) process and requirements
* Ability to articulate and explain CP policies in operational terms, as well as identify CP training and awareness needs and cost-effective training and awareness methods.
* Ability to develop, measure, and report appropriate CP metrics. • Business writing, presenting, and related communications skills

## CP Office

In large organizations, the CP Manager 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, in addition to the Incident Manager, Crisis Coordinator, BCP Manager, BRP Manager, IT DRP Manager, and others.

### **Key activities.**

* Assist in the creation of a CP "center of excellence" - a focal point inside the company that provides internal consulting and guidance on CP issues with the assistance of BC/BR managers and other specialists.
* Create inventories of key processes, supporting IT systems, and so forth.
* Schedule and coordinate meetings between CP managers and IAOs and other businesspeople.

Assist in the development of fairly consistent, comprehensive, and high-quality contingency plans throughout the organization, especially for key business operations and supporting/enabling functions.

* Assist in the development of CP policies, standards, procedures, and guidelines.
* Perform or assist others in identifying and managing risks associated with the CP project.
* Assist in the development of budget requests/proposals, business cases, and other CP-related documents.
* Keep track of CP-related plans, progress, budgets, risks, and opportunities, and produce management reports.
* Assist in the planning and/or delivery of CP-related awareness, training, and educational programs, exercises/tests, and other activities.
* Assist with the implementation of CP plans, operational problems, and clear and effective communication during a crisis.

.

### **Competencies.**

* Working understanding of CP, BC, BR, IT DRP, and other similar programs.
* Capable of establishing and maintaining effective working connections with others in the business world.
* Administrative abilities, including project management, metrics/management reporting, and so on.
* A keen eye for detail, as well as the diligence, persistence, and efficiency required to accomplish given tasks in a timely manner.
* Can speak calmly, effectively, and authoritatively in any situation, even a crisis.

# Business Continuity Planning (BCP) and Business Resumption Planning (BRP) roles and responsibilities

## BCP Manager

The main responsibility of the BCP Manager is to ensure that key business processes are sufficiently resilient to continue functioning successfully in the event of an emergency.

### **Key activities.**

* Oversee the BCP process as a whole.
* Provide BCP advice and assistance to IAOs, BRP/IT DRP managers, and others.
* Evaluate and prioritize business processes in terms of robustness and availability.
* Define and define resilience needs, taking into consideration interdependencies between processes and IT system support elements, and develop BC strategies.
* Assist in the preparation of investment plans, business cases, budget proposals, and other documents that will assist justify any extra investment needed in BC arrangements.
* Use appropriate templates to ensure that BC plans are produced to a consistent degree of quality, correctness, completeness, and detail.
* In-depth understanding of BCP.

### **Competencies.**

* Thorough understanding of BRP.
* Working understanding of the company's key business processes, procedures, and risk appetite, among other things.
* Familiarity with CP and IT DRP.
* Working understanding of the organization's financial management and investing procedures.
* Can speak calmly, effectively, and authoritatively in any situation, even a crisis.

## BRP Manager

The BRP Manager’s role emphasizes the timely restoration of business processes following a disaster.

### **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.

### **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.

## 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.]

### **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/BP-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.

### **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.

# IT Disaster Recovery Planning (DRP) roles and responsibilities

## IT DRP Manager

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

### **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.

### **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.

**IT DR Compliance Manager (4.2)**

The IT DR Compliance Manager assists the IT DRP Manager in achieving and demonstrating IT DR policy compliance.

**4.2.1 The main actions**

* Oversee routine IT DR reporting, incorporating data from BIAs, plans, incidents, disasters, exercises, and other sources, as well as the larger context provided by legal, regulatory, and standards bodies (e.g. legislative changes).
* Assist in the delivery of IT disaster recovery training and awareness events.
* Assists with BIA and test/exercise planning, as well as identifying any compliance needs (e.g. legal obligations to conduct a certain number and type exercise each year).

**4.2.2 Competencies.**

* Thorough understanding of compliance procedures.
* Thorough understanding of IT DRP business policies, rules, and regulations.
* Thorough understanding of IT disaster recovery planning as a discipline, ideally demonstrated by relevant qualifications and experience.
* Thorough understanding of the Certification and Accreditation (C&A) process and requirements [where applicable].
* Working understanding of key business processes and their respective importance.
* Capable of articulating and explaining IT disaster recovery policies in operational terms.
* Able to assist in the delivery of IT disaster recovery training and awareness.
* Business writing, presentation, and other relevant communication abilities.

**4.3 Test and Exercise Coordinator for the IT DRP**

The IT DRP Test and Exercise Coordinator assists the IT DRP Manager in designing and implementing IT DRP testing, awareness, training, and educational processes in accordance with legal, regulatory, and business requirements in order to ensure CP.

**4.3.1 The main activities**

* Design, plan/schedule, and organize IT DRP tests and exercises (mainly focused on educating personnel in IT DR-related processes and activities), assessing their efficacy, and supporting any improvement efforts that are deemed required to achieve the CP goals.
* Organize the materials needed for exams and activities.
* Coordinate all aspects of IT DRP tests and exercises, including planning, execution, and management reporting, with the IT DRP Manager, IT DR Office, different IT experts, information asset owners, BC and DR managers, and others. He/she gathers the necessary IT and other resources, as well as assesses the efficacy of IT DR tests and exercises and provides constructive comments.

**4.3.2 Competencies.**

* Thorough understanding of CP assurance requirements for demonstrating IT DRP components of CP, including laws, regulations, and business needs.
* Working understanding of CP and IT DRP information security procedures.
* Thorough understanding of key business processes and their respective importance.
* Familiarity with C&A procedures (where relevant).
* Able to create test/exercise plans, scenarios, and metrics for IT DRP.
* Capable of planning, managing, and delivering the IT DRP test/exercise program.
* Knowledge of how to create successful IT DR tests/exercises that offer the required degree of assurance while reducing needless testing expenses and risks.
* Capable of coordinating the actions of many stakeholders and participants in test/exercise situations.
* Analytical ability to compare and contrast the results of IT DR exercises and tests to expectations.

**4.4 Manager of IT DRP Development and Technical Assessment**

The IT DRP Development & Technical Assessment Manager provides assistance to the IT DRP Manager, IAOs, and others in developing sufficient IT DR plans and evaluating technical needs for successful recovery.

**4.4.1 The main actions**

* Assist IAOs through the IT system development life cycle to translate IT DR needs into DR plans by designing assessment tools.
* Assess the IT infrastructure's resilience and recovery capabilities, as well as the threats it poses.
* Compare IT DR plans to DR needs in Service Level Agreements (SLAs), contracts, and other explicit requirements (such as laws and regulations).
* Encourage the adoption of innovative technology and procedures to aid IT disaster recovery.

**4.4.2 Competencies.**

* In-depth understanding of IT DRP.
* Familiarity with key business procedures and priorities.
* Working understanding of Service Level Agreements (SLAs), contracts, and Memorandums of Understanding (MOUs).
* Working understanding of project management and the system development life cycle.
* Capable of creating and implementing realistic IT disaster recovery strategies.
* Able to evaluate the efficacy of proposed IT DR technologies, techniques, and approaches against BIA and other assessments' requirements.

**4.5 IT Disaster Recovery Office**

A staff may be required to assist the IT DR Managers, depending on the amount of work involved in maintaining IT DR plans and operations. [Note that the IT DR Office may be part of the CP Office mentioned above, although it is most often located inside the IT function, perhaps within the IT Project Management Office.]

**4.5.1 The main actions**

* Assist in the creation of an IT DR "center of excellence" - a focal point inside the company that provides internal consultation and guidance on IT DR issues with the assistance of IT DR managers and other specialists.
* Keep inventory of IT systems, services, and other items that support essential business operations.
* Schedule and organize meetings with IAOs and other businesspeople for their management.
* Assist in the development of fairly consistent, comprehensive, and high-quality IT disaster recovery plans throughout the business, especially for key IT systems and services.
* Assist in the creation of IT disaster recovery policies, processes, and guidelines.
* Perform or assist others in identifying and managing IT disaster recovery project risks.
* Assist with budget requests/proposals, business cases, and other IT DR-related tasks.
* Keep track of IT disaster recovery plans, progress, budgets, risks, and opportunities, and produce management reports.
* Assist with the planning and/or delivery of IT DR-related awareness, training, and educational programs, exercises/tests, and other activities.
* Assist in the implementation of IT disaster recovery plans, operational problems, and clear and efficient communication during a crisis.

**4.5.2 Competencies.**

* Working understanding of BC, BR, CP, IT DRP, and other similar systems.
* Capable of establishing and maintaining effective working connections with others in the business world.
* Administrative abilities, including project management, metrics/management reporting, and so on.
* A keen eye for detail, as well as the diligence, persistence, and efficiency required to accomplish given tasks in a timely manner.
* Can speak calmly, effectively, and authoritatively in any situation, even a crisis.

**5 Additional CP roles and duties**

In the case of IM, CM, BCP, BRP, and IT DRP, a number of additional business activities usually play supporting roles. While individuals may not realize their importance in contingency planning, they will be expected to help with recovery efforts after an event or disaster.

**5.1 Roles in Incident Management**

Dealing with small outages, various information security events, and near-misses are all examples of incident management in the workplace. Except in the event of more serious incidents, incident management procedures, roles, and duties lie beyond the scope of contingency planning. While regular incident management actions are likely to be well-practiced in the ordinary company, unusual occurrences (such as large physical or logical/T incidents) may need operations that are less known and well-practiced. Management should consider the potential that the typical incident manager or managers will not be accessible during or after a significant event.

**5.2 Roles in Crisis Management**

Crisis management, like incident management, may be seen as an extension of routine operations. Normally, a number of people are selected and trained to perform roles such as:

* Building Evacuation Manager/Crisis Coordinator.
* Fire Warden.
* First Aider.
* Physical/Site Security Guard, and so on.
* Damage Assessor or Leader of the Damage Assessment Team

The organization should ensure that such individuals are sufficiently well prepared to act appropriately in exceptional circumstances after a major incident, and that there are enough trained and prepared individuals to handle such incidents reasonably well (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, Job Rotation, and Succession Planning**

In addition to the main incident and crisis managers, competent deputies should preferably be selected and trained to take over in the event that the primary manager(s) are unavailable (whether involved in the incident or otherwise engaged e.g. off sick, on holiday or simply overloaded). For all essential roles in the company, succession planning is advised, but it is especially important in the case of severe events. Some companies, for example, have a purposeful job rotation strategy in place to expose various workers to key roles, share information, and disseminate skills.

**5.4 Owners of Information Assets**

As a consequence of the BIA process, “owners” of important information assets, such as essential business processes, have a role in defining availability (both resilience and recovery) needs and financing the related controls. While the body corporate is technically the legal owner of all corporate assets, management and other stakeholders often hold Information Asset Owners (IAOs) inside the company personally responsible for the appropriate security of the information assets within their jurisdiction. This often involves third-party information assets that have been entrusted to the organization's protection (e.g. personal data relating to customers).

IAOs concentrate on the BC components of CP using the organization's BIA process, usually depending on Custodians and IT DR experts to develop and provide the appropriate IT DR elements. They plan and coordinate BC operations, define business availability goals (often in terms of resilience, Recovery Point Objectives, Recovery Time Objectives, and so on), assign resources for BC and perhaps IT DR activities, and compare the outcomes of DR tests to their requirements.

The competences of the IAO include the following.

* A thorough grasp of the key business processes that fall within their purview, as well as their priority in respect to other business processes.
* Working understanding of the information technology systems and other resources that support their key business operations.
* A general knowledge of continuity planning, including resilience and IT disaster recovery as complementing elements of continuity planning.
* A general understanding of IT DR test methods and exercises is required to ensure that the resilience and IT DR solutions meet the organization's availability needs.
* Working understanding of the IT development life cycle (such that IT DRP arrangements remain closely aligned with BC requirements as IT systems change).
* Ability to conduct BIAs, usually in collaboration with professional advisers from the BC/DRP teams, Risk Management, and Information Security Management, among other things.

**5.5 Custodians**

Following BIA, Custodians, usually inside the IT Department for IT systems and networks, are typically assigned duties for the operation and protection/security of information assets supporting key business operations.

While Custodians are not formally responsible for providing and proving the adequacy of IT DRPs and other contingency plans, they do have a professional responsibility to identify and resolve issues in their area of expertise, as well as to bring residual risks to the attention of management, including IAOs, BC Managers, and others. This is particularly true in the case of sophisticated technical IT DRP setups, where IT professionals who are acquainted with the technologies are more likely to see technical problems, dependencies, and other concerns that would make the arrangements useless in a true DR situation.

**5.6 BC Functions of Operations**

These are the individuals in charge of maintaining or restoring company operations in the aftermath of events and disasters. They are most usually regular workers, although some may be working in unusual situations, such as covering for other employees who are unable to work due to injury, disability, or other reasons.

Such individuals are responsible for actively participating in relevant BC and/or IT DRP exercises, identifying non-technical problems, dependencies, and other factors that might make the arrangements ineffective in a true DR situation, and reporting them to the appropriate management.

**5.7 IT Disaster Recovery Operations**

These are the individuals that handle IT recovery duties including setting up standby/recovery systems, recovering backups from offline media, validating recovered data, and releasing systems for production usage. They are most often regular IT workers, network/system managers, operators, and so on, although they may be working in unusual areas, such as covering for other IT professionals who are unable to work due to injury, incapacity, or other reasons.

Many operational tasks are covered by the IT DR roles, including system/application administration, database administration, network and telecommunications, procurement, server replenishment, and IT Help/Service Desk, among others. Employees in such roles.

* Put the IT disaster recovery strategies in place, both in practice and in real-life situations.
* Test and evaluate the efficacy of IT DR procedures in real-world scenarios, giving feedback and lessons gained to improve the plans.
* Competencies in IT DR Ops include the following.
* Working understanding of key business operations, recovery priorities, and supporting IT systems, as well as other relevant information.
* Able to identify weaknesses in DR processes and suggest realistic remedies, for example as a result of DR tests or exercises, for IT systems and procedures for which they have recovery responsibilities, as well as specific/expert knowledge of the associated hardware platforms, operating systems, middleware, application software, configurations, and so on.
* are distributed under the same conditions as this.