

Roles and responsibilities

for

contingency planning

Version 1

September 2021

1. D. Jaliya

IT19991290

Executive summary

This document defines the responsibilities and competencies frequently associated with Contingency, Business Continuity, Business Resumption, and IT Disaster Recovery Planning roles in Tellida Pvt Ltd, based on ISO/IEC 27000-series standards and other references.

Contents

*Section Page*

[1 Introduction 3](#_Toc204745074)

[1.1 Background, concepts and key terms 3](#_Toc204745075)

[1.2 Scope and applicability of this document 4](#_Toc204745076)

[1.3 Using this document – an important *caveat* 4](#_Toc204745077)

[2 Contingency Planning (CP) rôles and responsibilities 5](#_Toc204745078)

[2.1 CP Manager 5](#_Toc204745079)

[2.2 CP Compliance Manager 5](#_Toc204745080)

[2.3 CP Office 6](#_Toc204745081)

[3 Business Continuity Planning (BCP) and Business Resumption Planning (BRP) rôles and responsibilities 7](#_Toc204745082)

[3.1 BCP Manager 7](#_Toc204745083)

[3.2 BRP Manager 7](#_Toc204745084)

[3.3 BCP/BRP office 8](#_Toc204745085)

[4 IT Disaster Recovery Planning (DRP) rôles and responsibilities 9](#_Toc204745086)

[4.1 IT DRP Manager 9](#_Toc204745087)

[4.2 IT DR Compliance Manager 9](#_Toc204745088)

[4.3 IT DRP Test and Exercise Coordinator 10](#_Toc204745089)

[4.4 IT DRP Development & Technical Assessment Manager 11](#_Toc204745090)

[4.5 IT DR Office 11](#_Toc204745091)

[5 Other CP-related rôles and responsibilities 12](#_Toc204745092)

[5.1 Incident Management rôles 12](#_Toc204745093)

[5.2 Crisis Management rôles 12](#_Toc204745094)

[5.3 Incident and Crisis Management deputies, succession planning and job rotation 13](#_Toc204745095)

[5.4 Information Asset Owners (IAOs) 13](#_Toc204745096)

[5.5 Custodians 13](#_Toc204745097)

[5.6 BC Operations functions 14](#_Toc204745098)

[5.7 IT DR Operations functions 14](#_Toc204745099)

[6 References and further reading 14](#_Toc204745100)

[7 Feedback on this document 15](#_Toc204745101)

[8 Acknowledgement 15](#_Toc204745102)

[9 Copyright notice and disclaimer 15](#_Toc204745103)

# Introduction

## Background, concepts and key terms

Because all risks cannot be completely removed in actuality, the essential premise of Contingency Planning (CP) is that residual hazards will always exist. Incidents will occur despite the organization's best efforts to avoid, prevent, or reduce them. Even the greatest information security procedures designed to safeguard the confidentiality, integrity, and availability of information assets may be bypassed or overwhelmed in specific scenarios, due to a mix of unfavorable events, unanticipated threats, and vulnerabilities.

CP is described in this paper as the sum of activities, controls, processes, plans, and other items related to catastrophic catastrophes and disasters. It is the act of planning for large occurrences and disasters, forming adaptable plans, and marshaling appropriate resources to be used in the event, whatever that event may be. The word 'contingency' means that the activities and resources needed in the aftermath of big incidents or disasters will be contingent (dependent) on the particular nature of the incidents or disasters that occur. In this sense, CP entails anticipating the unexpected and making plans for the unknown.

The primary goal of CP is to reduce the negative repercussions and effects of accidents and disasters. This document distinguishes a number of more particular concepts and activities within the field of CP, which serve as the foundation for the roles listed below.

* **Availability Management and Continuity Planning** practices include steps to maintain critical business operations and supporting IT infrastructure operational in the face of crises 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)** Includes procedures to guarantee that, to the extent practicable, IT systems, networks, and associated infrastructure and processes that enable key business operations remain operational in the event of a disaster. Fault-tolerant, robust, or high-availability system/network designs and configurations, built-in redundancy and automated failover of supporting IT systems, capacity and performance management, and so on are all part of this..
* **Recovery and Resumption Planning** refers to the process of recovering or resuming business and IT operations following catastrophes and disasters, usually from alternate locations and with backup equipment.:
  + **Business Resumption Planning (BRP)** ntails making plans to resume or restore key and important business processes to a state that is as close to normal as possible after disasters or major incidents that overwhelm the resilience capabilities mentioned above. Relocating personnel to alternate office sites, manual fallback processing, temporary relaxation of divisions of responsibility and delegated authorities, and so on are all examples of this.;
  + **IT Disaster Recovery Planning (IT DRP)** involves preparing for the recovery of critical IT systems and services in the event that the resilience arrangements are overwhelmed; examples include manually restoring IT systems and data on alternate/standby equipment from backups or archives, utilizing emergency communications facilities, and so on..
* **Incident and Crisis Management** activities are focused on managing incident and disaster scenarios “live”, as they occur:
  + **Incident Management (IM)** is a set of actions and processes for assessing and responding to various types of information security occurrences. The majority of IM activities are performed on a regular basis in the course of business, dealing with a variety of minor issues. Best practice proactive IM processes include 'corporate learning' by continuously updating processes, systems, and controls, as well as improving resilience and recovery activities in response to actual incidents and disasters, as well as near misses; Crisis
  + **Crisis Management (CM)** entails emergency management activities associated with the management of major incidents and crises, primarily relating to health and safety aspects. Preliminary evaluation of the situation, communication with emergency services and management, and (in the case of serious incidents) invocation of applicable BRP and IT DR plans are all common tasks during the crisis phase. An important aspect of CM is quickly developing a professional crisis management group/team to supervise and control ongoing recovery actions..

It is critical to recognize the importance of planning and preparation in all CP-related tasks. While many of us expect to be able to cope with and get through crisis situations on the fly, CP attempts to develop appropriate plans and store needed resources ahead of time to make the situation more manageable and less disruptive on the day. Furthermore, while it is prudent to prepare thoroughly for commonplace incidents (such as power or telecommunications outages), true CP also includes an element of planning for completely unexpected events, such as pre-determining the crisis management structure and processes to assess and respond to any incident more efficiently than if no such preparations had been made.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.

## Scope and applicability of this document

The roles and responsibilities outlined in this article are particularly for large organizations, such as private-sector corporations or government departments. Large enterprises have both the resources and the availability requirements to warrant dedicating full-time personnel to CP activities. Small to medium-sized businesses usually execute substantially comparable activities with fewer people, many of whom may work part-time on specific aspects of CP and may or may not be as qualified. Micro enterprises with a limited number of employees, on the other hand, may delegate all CP tasks to a single employee, ideally with a deputy or fallback.

The descriptions of important actions and competences in this document may be used to build job descriptions, vacancy announcements, and other documents for CP-related roles with careful consideration by management and adaptation to suit the specific requirements. In practice, organizations that most closely match the scope description above have most likely defined a number of CP-related roles, but may not have taken into account the full range of activities described here, implying that job descriptions and other documents may need to be reviewed and updated. Other organizations may benefit from reviewing their governance structures and job descriptions, particularly any significant gaps in coverage, as they are less likely to have such a comprehensive approach to CP.

## Using this document – an important *caveat*

This paper is offered solely for the purpose of education and discussion. The roles and responsibilities described in the rest of this document are generic. Without significant change and customization, the document is unlikely to meet the needs of Tellida Pvt Ltd..

# Contingency Planning (CP) rôles and responsibilities

## CP Manager

While most CP-related tasks are handled by the individual subsidiary roles described below, a senior manager is usually required to supervise, direct, and regulate the CP operations as a whole.

### Key activities:

* Liaison with and coordination of 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 CP requirements
* Identify financial and progress deficiencies, as well as unmanaged risks, that undermine the success of CP efforts, and engage with management to identify and resolve these concerns;
* Take a strategic enterprise-wide view of CP, defining broad CP strategies and policies that complement and support other ordinary business strategies, risk and security management objectives, IT disaster recovery policies, and so on.
* Establish appropriate management, control, direction, and monitoring arrangements to oversee 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).

### 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.

## CP Compliance Manager

The CP Compliance Manager assists the CP Manager in achieving and demonstrating compliance with CP policies, strategies, and standards, among other things.

### Key activities:

* Manage routine CP management reporting, incorporating pertinent information from BIAs, plans, events, catastrophes, exercises, and so on, as well as the broader context from legal, regulatory, and standards authorities.
* Create and assist in the delivery of CP training and awareness activities;
* Assist with BIA and test/exercise planning, as well as the determination of any associated compliance requirements.

### Competencies:

* Detailed knowledge of CP, preferably demonstrated by applicable qualifications and experience;
* Detailed understanding of CP's corporate policies, legislation, and regulations;
* Knowledge of the Certification and Accreditation (C&A) process and requirements [where applicable];
* Working understanding of essential business processes and respective priorities;
* Capable of communicating and explaining CP policies in operational terms, as well as identifying CP training and awareness needs and cost-effective training and awareness approaches;
* Capable of developing, measuring, and reporting appropriate CP metrics;
* Business writing, presentation, and associated communication abilities are required.

## CP Office

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, in addition to the Incident Manager, Crisis Coordinator, BCP Manager, BRP Manager, IT DRP manager, and others.

### Key activities:

* Assist in the establishment of a CP "center of excellence" - a focal point within the company that provides internal consultancy support and direction on CP issues with the assistance of BC/BR managers and other experts;
* Create inventories of important processes, supporting IT systems, and so on.
* Schedule and coordinate meetings between CP managers and IAOs and other businesspeople.
* Guide and assist the development of relatively consistent, comprehensive, and high-quality contingency plans across the enterprise, particularly for essential business processes and the supporting/enabling functions that go with them.
* Contribute to the creation of CP-related rules, standards, procedures, and recommendations.
* Perform or assist others in identifying and managing CP project-related risks;
* Assist with the development of budget requests/proposals, business cases, and other documents for various CP operations.
* Monitor and generate management reports on CP-related plans, plan progress, budgets, risks, and opportunities.
* Assist in the coordination and/or delivery of CP-related awareness, training, and educational programs, exercises/tests, and so on; Assist in the implementation of CP plans, handle operational concerns, communicate clearly and effectively, and so on during a crisis.

### Competencies:

* Working knowledge of CP, BC, BR, IT DRP, and other business applications; ability to form and maintain constructive working relationships with other business people;
* General administrative abilities, as well as some experience with project management, metrics/management reporting, and so on;
* An eye for detail, as well as the diligence, persistence, and efficiency required to perform assigned tasks correctly and within realistic timescales; the ability to communicate calmly, effectively, and authoritatively, particularly in a crisis.

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

## BCP Manager

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

### Key activities:

* Manage the overall BCP process;
* Provide BCP advice and assistance to IAOs, BRP/IT DRP managers, and others.
* Assess and prioritize business processes in terms of resilience/availability.
* Determine/specify resilience requirements, taking into account the interdependence of processes and IT system support factors, and build BC plans.
* Contribute to the justification of any further investment required in BC arrangements by assisting in the preparation of investment plans, business cases, budget proposals, and so on.
* Ensure that BC plans are consistently prepared to a high level of quality, correctness, completeness, and detail, often by developing appropriate templates.

### 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.

## BRP Manager

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

### Key activities:

* Manage the overall BRP process;
* On BRP issues, collaborate with IAOs, BCP, and IT DRP peers.
* Assess and prioritize business operations in terms of recovery;
* Determine recovery requirements, taking into account process interdependence and IT system support elements.
* Justify any further investment in BRP that is required.
* Make 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:

* Assist in the establishment of a 'center of excellence' for BC/BR - a focal point within the company that provides internal consultancy support and direction on BC/BR issues with the assistance of BC/BR managers and other experts;
* Keep inventories of important processes, supporting IT systems, and so on.
* Schedule and organize meetings with IAOs and other business persons for their management.
* Guide and support the development of reasonably consistent, comprehensive, and high-quality BC/BR plans across the company, with a focus on important business processes and the supporting/enabling services that go with them.
* Assist in the development of BC/BP policies, standards, procedures, and recommendations.
* Perform or assist others in identifying and managing BC/BR project-related risks;
* Assist in the development of budget requests/proposals, business cases, and other documents for various BC/BR tasks.
* Monitor and generate management reports on BC/BR-related plans, plan progress, budgets, risks, and opportunities.
* Contribute to the coordination and/or delivery of BC/BR-related awareness, training, and educational programs, exercises/tests, and so on.
* In a crisis, assist in the implementation of BC/BR plans, address operational concerns, communicate clearly and effectively, and so on.

### Competencies:

* Capable of establishing and maintaining fruitful working connections with other businesspeople;
* General administrative abilities, as well as some experience with project management, metrics/management reporting, and so on;
* An eye for detail, as well as the diligence, persistence, and efficiency required to execute specified tasks correctly and within reasonable timescales;
* Capable of communicating calmly, efficiently, and authoritatively, even amid a crisis.

# IT Disaster Recovery Planning (DRP) rôles and responsibilities

## IT DRP Manager

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

### Key activities:

* Coordination of stakeholder participation in disaster recovery planning and collaboration with IAOs to prioritize important business processes
* Manage the DR program's resources.
* Define the principles, rules, and procedures required to support or restore critical business functions following a catastrophic occurrence.
* Create programs for assessing the business impact, compliance, training, testing, and exercising, technical assessment, and plan formulation.
* Implement disaster recovery plans through disaster recovery arrangements such as regular data backups, secure data archival, backup restoration, secure on- and off-site backup media storage, and the provision of alternate IT processing facilities, networks, and so on.
* Examine the entire IT DRP program and IT preparedness in regard to BRP and broader CP needs.

### Competencies:

* Expert knowledge of IT DRP; in-depth knowledge of IT systems, networks, and applications that support essential business operations; in-depth knowledge of project management
* Knowledge of CP, BCP, and BRP;
* Working understanding of the critical business processes of the organization;
* Working understanding of certification and accreditation processes [in scenarios where IT disaster recovery plans must be independently examined and certified against enterprise-wide criteria and, in some cases, legal/regulatory requirements];
* Working understanding of procurement policies and processes is required.
* Capable of actively contributing to Business Impact Analysis (BIA);
* Capable of communicating calmly, efficiently, and authoritatively, even amid a crisis.

## IT DR Compliance Manager

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

### Key activities:

* Manage routine IT disaster recovery reporting, pulling pertinent information from BIAs, plans, events, disasters, exercises, and so on, as well as the broader context from legal, regulatory, and standards bodies (e.g., legislative changes);
* Assist in the delivery of IT disaster recovery training and awareness efforts.
* Assists with BIA and test/exercise planning, as well as determining any associated compliance requirements (for example, legal duties to conduct a particular number and type of exercises each year).

### Competencies:

* Detailed understanding of compliance practices; Detailed understanding of business policies, rules, and regulations regulating IT DRP;
* Detailed knowledge of IT disaster recovery planning as a subject, preferably demonstrated by applicable certifications and experience;
* Knowledge of the Certification and Accreditation (C&A) process and requirements [where applicable];
* Working understanding of essential business processes and respective priorities;
* Capable of articulating and explaining IT disaster recovery policies in operational terms
* Capable of assisting in the delivery of IT disaster recovery training and awareness;
* Business writing, presentation, and associated communication abilities are required.

## 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.

### Key activities:

* Design, plan/schedule, and coordinate IT DRP tests (primarily focused on testing the correct operation of DR technologies) and exercises (primarily focused on training people in IT DR-related procedures and activities), evaluating their effectiveness and promoting any improvement activities deemed necessary to meet CP objectives.
* Organize the resources needed for tests and exercises.
* Liaise with the IT DRP Manager, IT DR Office, various IT experts, information asset owners, BC and DR managers, and others on all aspects of IT DRP tests and exercises, such as planning, execution, and management reporting. He/she coordinates IT and other resources as needed, and assesses the efficacy of IT DR tests and exercises, providing constructive input.

### Competencies:

* Detailed understanding of laws, regulations, and business requirements pertaining to CP assurance criteria for proving IT DRP elements of CP;
* Working knowledge of CP and IT DRP information security controls;
* Working understanding of essential business processes and their relative importance;
* Working knowledge of C&A processes (where applicable);
* Capable of creating IT DRP test/exercise plans, scenarios, and metrics;
* Capable of planning, managing, and delivering the IT DRP test/exercise program;
* Ability to create successful IT disaster recovery tests/exercises that offer the needed degree of confidence while eliminating extraneous testing expenses and hazards;
* Capable of coordinating the activity of multiple stakeholders and participants in test/exercise scenarios;
* Analytical ability to compare the results of IT DR exercises and tests to expectations.

## 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.

### Key activities:

* Create assessment tools that help you identify the right level of recovery assistance for you.
* Assist IAOs across the IT system development life cycle in translating IT DR needs into DR plans.
* Evaluate the IT infrastructure's resilience and recovery capabilities, as well as the dangers it poses.
* Correlate DR requirements in Service Level Agreements (SLAs), contracts, and other specified obligations (such as laws and regulations) to IT DR strategies.
* Encourage the use of innovative technology and techniques to aid in IT disaster recovery.

### Competencies:

* IT DRP expert knowledge; working understanding of important business processes and priorities
* Working knowledge of service level agreements (SLAs), contracts, and Memorandums of Understanding (MOUs);
* Knowledge of the system development life cycle and project management is required.
* Capable of designing and developing realistic IT disaster recovery plans;
* Capable of evaluating the effectiveness of proposed IT DR technologies, methods, and approaches against BIA and other assessments' requirements.

## 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.]

### Key activities:

* Assist in the creation of an IT DR "center of excellence" - a focal point within the business that provides internal consultancy support and direction on IT DR issues with the assistance of IT DR managers and other professionals;
* Maintain inventories of IT systems, services, and other items that support important business processes;
* Schedule and organize meetings with IAOs and other business persons for their management.
* Guide and support the development of reasonably consistent, comprehensive, and high-quality IT disaster recovery plans across the company, particularly for essential IT systems and services.
* Assist in the creation of IT disaster recovery policies, standards, processes, and guidelines.
* Perform or assist others in identifying and managing IT DR project-related risks;
* Assist with the development of funding requests/proposals, business cases, and other documents for various IT DR initiatives.
* Monitor and generate management reports on IT disaster recovery plans, plan progress, budgets, risks, and opportunities.
* Assist in the coordination and/or delivery of IT disaster recovery-related awareness, training, and educational programs, exercises/tests, and so on.
* Assist in the implementation of IT disaster recovery plans, address operational issues, communicate clearly and efficiently, and so on during a crisis.

### Competencies:

* Working knowledge of BC, BR, CP, IT DRP, and other business processes; ability to form and maintain constructive working relationships with different business people
* General administrative abilities, as well as some experience with project management, metrics/management reporting, and so on;
* An eye for detail, as well as the diligence, persistence, and efficiency required to perform assigned tasks correctly and within realistic timescales; the ability to communicate calmly, effectively, and authoritatively, particularly in a crisis.

# Other CP-related rôles and responsibilities

IM, CM, BCP, BRP, and IT DRP are often supported by a variety of additional business processes. While individuals may not recognize their importance in contingency planning, they will be expected to assist with recovery efforts following an incident or crisis.

## Incident Management rôles

Incident management is a standard element of day-to-day corporate operations, such as dealing with minor outages, other information security incidents, and near-misses. Except in the case of more serious incidents, incident management processes, roles, and duties remain primarily beyond the scope of contingency planning. Whereas ordinary incident management actions are likely to be well-practiced in the average organization, unusual occurrences (such as major physical or logical/T incidents) may necessitate other activities that are unlikely to be as known and well-practiced. Management must consider the potential that the normal incident manager/s will not be available during or after a significant occurrence.

## Crisis Management rôles

Crisis management, like incident management, can be viewed as an extension of typical operational tasks. Under normal conditions, a variety of people are appointed and trained to fill roles 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 guarantee that such personnel are sufficiently well equipped to behave correctly under unusual conditions following a big incident, and that there are sufficient trained and prepared individuals to cope relatively effectively with exceptional situations.

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

In addition to the principal incident and crisis managers, appropriate deputies should preferably be chosen and trained to take the lead if the primary manager/s is/are unavailable (whether participating in the incident or elsewhere engaged e.g. off sick, on holiday or just overwhelmed). Succession planning is advised for all major rôles in the company but has specific relevance in connection to serious occurrences. Some businesses for example run an intentional strategy of job rotation to expose various people to such essential rôles, exchanging information and spreading capabilities.es.

## Information Asset Owners (IAOs)

“Owners” of important information assets including vital business processes etc. have a rôle in establishing availability (both resilience and recovery) needs as a consequence of following the BIA process, and paying the related controls. While legally speaking the body corporate may be the legal owner of all corporate assets, Information Asset Owners (IAOs) inside the company are typically held personally accountable by management and other stakeholders for proper protection of the information assets under their jurisdiction. This typically comprises information assets belonging to third parties but placed in the custody of the business (e.g. personal data pertaining to consumers).

Using the organization’s BIA process, IAOs focus on the BC components of CP, generally depending on Custodians and IT DR professionals to develop and deliver the relevant IT DR parts. They plan and organize BC operations, establish business objectives for availability (usually in terms of resilience, Recovery Point Objectives, Recovery Time Objectives etc.), assign resources for BC and potentially IT DR activities, and assess the outcomes of DR tests against their criteria.

IAO competencies include:

* Deep knowledge of important business operations within their jurisdiction, and a fair grasp of their priority in respect to other business processes
* Working understanding of IT systems and other resources supporting their essential business operations;
* General concept of CP, including resilience and IT DR as complimentary components of CP;
* General understanding of IT DR test methods and exercises essential to offer adequate confidence that the resilience and IT DR solutions fulfill the organization’s availability needs;
* Working understanding of the IT systems development life cycle (so that IT DRP arrangements stay tightly linked with BC needs when IT systems evolve);
* Ability to execute BIA, typically in cooperation with expert advisers chosen from the BC/DRP teams, Risk Management, Information Security Management etc.

## Custodians

Following BIA, duties pertaining to the operation and protection/security of information assets supporting key business activities are generally allocated to Custodians, typically inside 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 essential in the case of sophisticated technical IT DRP settings where IT professionals who are knowledgeable with the technologies are more likely to identify technical problems, dependencies etc. that would render the arrangements useless in a true DR situation..

## BC Operations functions

These are the personnel in charge of maintaining or restoring company processes in the aftermath of accidents and disasters. They are most usually regular employees, 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 render the arrangements ineffective in a true DR situation, and reporting them to the appropriate management.

## IT DR Operations functions

* These are the personnel 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 usually regular IT personnel, 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 activities 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 these roles: Implement IT DR plans in both testing and real-world incidents; Evaluate the efficacy of IT DR procedures in both tests and real-world incidents, giving feedback and lessons learned to improve the plans.

IT DR Ops competencies include:

* Knowledge of important business operations, recovery priorities, and supporting IT systems, among other things;
* Detailed understanding of disaster recovery plans and processes for IT systems and other systems for which they are responsible for recovery, as well as specific/expert knowledge of the hardware platforms, operating systems, middleware, application software, configurations, and so on;
* Capable of identifying flaws in DR procedures and proposing practical solutions, such as as a consequence of DR tests or exercises.