

- ▶ Gather data and draft the plan.
- ▶ Iterate it with stakeholders and interested parties as appropriate and get it signed off by the relevant authority (e.g., CIO/Steering Group).

There are at least two fundamentally different ways to develop a BCP: procedure-driven planning and decision-driven planning.

9.2.1.1 Procedure-Driven Planning

Create a set of procedures, which are adhered to during invocation and recovery. These procedures usually comprise a detailed, step-by-step approach against a timeline. The underlying assumption is that, whatever the disruption, the same procedures and processes will result in an effective recovery. These plans work well for repetitive, routine activities where priorities do not change much. In a technology environment they are essential to ensure the sequence of recovery is followed and that each activity is covered.

A procedurally-based BCP typically assumes a worst case scenario with a fairly simple outcome – e.g., loss of site, facilities, technology, or supply. However, where the organization's activities are less predictable, there could be multiple disruption scenarios with significantly different worst case outcomes, and a procedurally based BCP may be less appropriate. Some of the signs are:

- ▶ Highly dynamic, rapid business growth or contraction.
- ▶ Short product lifecycles and quick obsolescence of products.
- ▶ Frequently changing priorities.
- ▶ Project-based activities where the organization has a few important projects, especially projects with short timeframes.
- ▶ Many different products, services, projects.
- ▶ A few high value, irregular customers.
- ▶ A seasonal or volatile workload and perhaps rapidly changing customer base.

A procedure-driven BCP would need multiple procedures to respond to these possible permutations – and, even then, might fail to cover the actual situation. It would be complex, confusing, and could lead to inappropriate actions depending on the real incident and its progress. In this case, a procedure-based plan would be trying to hit a series of constantly moving targets. It would also be a nightmare to maintain, since priorities and information are constantly changing. In such cases, a decision-driven BCP may be more appropriate.

9.2.1.2 Decision-Driven Planning

A decision-driven BCP will provide a number of checkpoints at which decisions have to be made and usually provide options for actions and decisions depending on what is actually happening and the potential impact. This identifies trigger points and asks questions, supplying possible courses of action from which to select. Although some of these actions may be supported by procedures, they are more likely to be supported by checklists. The types of questions that may be asked are:

- ▶ What is our current biggest project?
- ▶ Can it still be delivered on time?
- ▶ What is the impact of late delivery?

In effect, a decision-based BCP will perform a real-time BIA, assess action choices (typically from a list of prompts) and reallocate or apply (usually pre-identified) resources based on this BIA. While the procedures for doing this can be broadly sketched out at a high level, they are far less detailed than in the procedure-based BCP.

Determine which people are critical to running the business, supporting the recovery, and supporting customers.

9.2.13 Areas to Consider in Planning

Whether you decide on a procedure-based or decision-driven BCP, the resultant plan will cover a number of important areas. It will:

- ▶ Consider teleworking and establish a policy on teleworking for BC team members and other staff. Define and include secure remote access arrangements.
- ▶ Have an introduction that:
 - Identifies the scope of the plan.
 - Explicitly declares the assumptions on which the plan is based.
 - Defines disaster or disruption (i.e., your name for the situation in which you will invoke the BCP).
 - Identifies any known weaknesses in the plan together with any actions to rectify them, the “owner” of each action, and deadline to do so.
 - Contains incident checklists with triggers, escalation procedures, and corresponding actions.
 - Shows the escalation process from an incident occurring to declaring a disaster.
 - Covers alert, invocation, and stand down procedures.
 - Explains how to use the plan.
- ▶ Identify and establish management and departmental (business and support units) teams and their roles.
- ▶ Identify critical personnel.
- ▶ Determine which people are critical to running the business, supporting the recovery, and supporting customers.
- ▶ Ensure that they can access key systems and information whenever they need to. Ensure they have trained deputies (including the CEO!).
- ▶ Provide them with adequate support at all times.
- ▶ Identify team leaders and alternates, and team members and their alternates.
- ▶ Identify and prioritize tasks, actions, and functions to be undertaken for recovery.
- ▶ Assign roles and responsibilities of team leaders and team members.
- ▶ Ensure the same team leader or team member have no other conflicting, concurrent responsibilities.
- ▶ Identify alternative locations (standby locations) from which to work.

- ▶ Spell out what to say to the media and to whom the media should be referred.
- ▶ Provide contact details and essential information for internal and external contacts. These should include, as appropriate, regulators, critical suppliers (including utility companies and telcos), contractors, lawyers, bankers, real estate agents, consultants, municipal and community authorities, the post office, emergency services, police, fire, hospitals, insurers, and salvage companies. Also list suppliers whom you may not use now, but whom you might want to use in an emergency – logistic companies, couriers, movers, security firms, employment or temporary staffing agencies, etc.
- ▶ Identify and document critical equipment. Apart from IT (servers, PCs, laptops, tablets, and other devices plus software including version details), critical equipment could include fax machines, photocopiers, the company seal, and check signing equipment. Ensure the BCP covers replacement equipment or alternative places where it can be obtained or used. If you rely on BYOD (Bring Your Own Devices) ensure alternate devices are available.
- ▶ Identify vital documents and materials, including backups, and specify how to access them.
- ▶ Provide information about your standby location(s) – address, telephone number, and contact details, alert, invocation, and occupation procedures, transport arrangements, security arrangements, etc.
- ▶ Identify resource requirements, say how and by whom they will be provided, and establish the timescale for their provision. Plan ahead to allow for increased capacity in production, bandwidth, and computing capability.
- ▶ Consider the need for more user licenses for software, VPN, and Internet connections. Include alternative communication methods in the event that normal fixed line or mobile telephony is unavailable.
- ▶ Establish reporting processes and requirements.
- ▶ Contain confidentiality status, version control, and document configuration management to ensure all BCPs in circulation are the latest version of those BCPs.
- ▶ Since an incident may be followed by inquiries, claims, counter-claims, and compliance or regulatory implications, it is essential that the plan provides for an audit trail to be maintained of actions undertaken in recovery, why and when they were taken, and by whom.
- ▶ Take care to have sufficient document version control to ensure that only the current version can be accessed in a disaster.

The **Business Continuity Toolkit** for this book provides specific guidance and models. We also consider use of software tools for BCP development below.

9.2.2 Plan Introduction

The Introduction to your plan should clearly define its scope. For instance:

- ▶ Is it an interim BCP, a standalone BCP, or an MCP?
- ▶ Is it a procedure-based BCP or a decision-driven BCP?
- ▶ Does it cover full crisis and reputation management or just physical disasters?

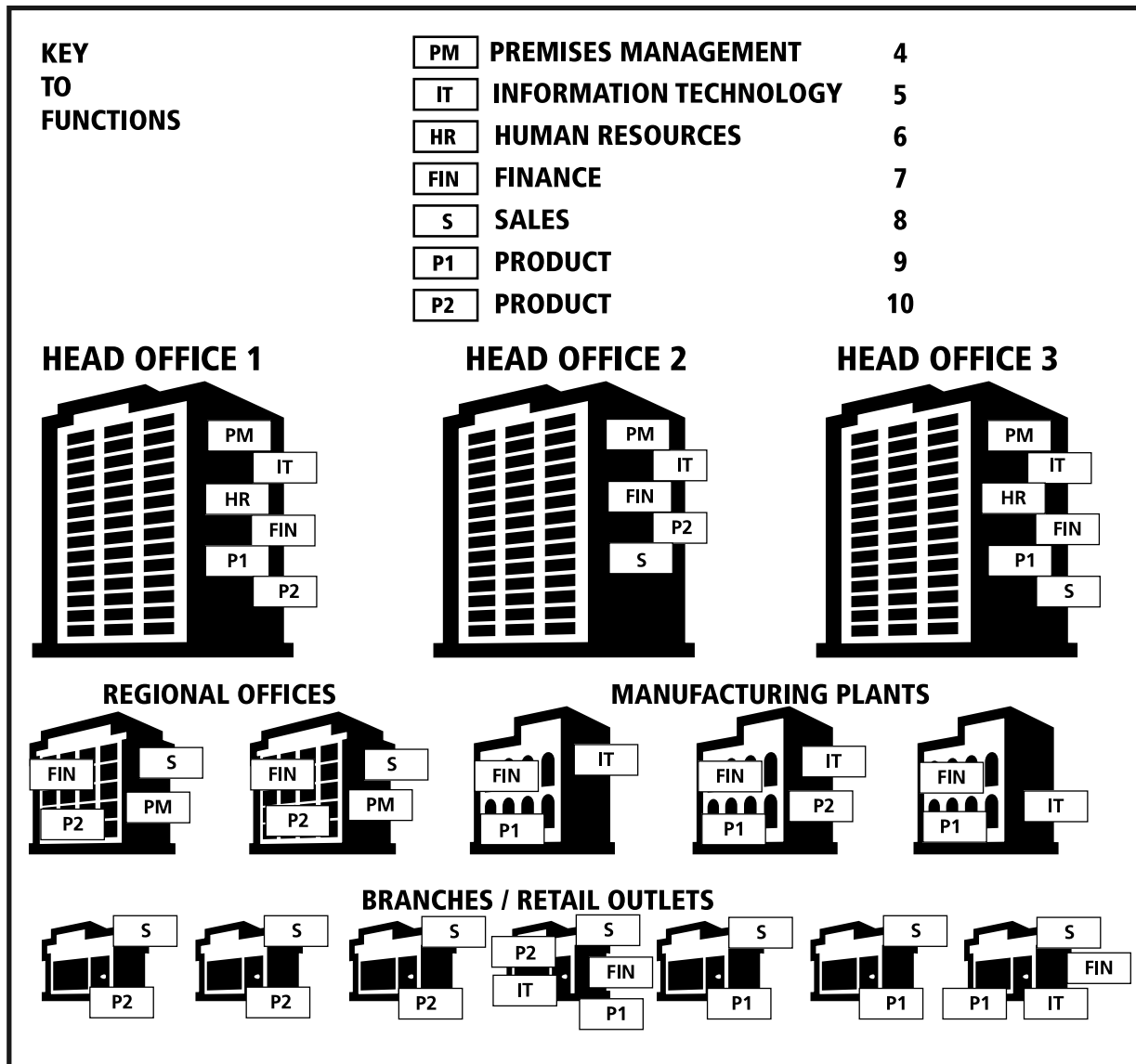


Figure 9-2. Example Organization and BC Plan Structure

- ▶ Section 2 would be the BC organization and EMT structure, roles, and action plan; recovery priorities; contacts; and vital materials.
- ▶ Section 3 would contain instructions for the BC manager.

All other sections would be completed only for the sites at which the functions specified at Figure 9-2 took place; where they did not take place, that section would be identified as having been deliberately omitted.

A site BC perspective could then be obtained by calling for each site's BCPs, while a functional perspective would result from, for instance, IT calling for all sites' BCPs, section 5 only. A product view for product 1 would be obtained by calling for the BCPs of all sites, section 9 only.