SERVICES CONTINUITY PLANNING

PURPOSE

Organisations create a services continuity plan (SCP) to coordinate the recovery of their services in the event of a short-term (emergency) or long-term disruption. An SCP contains all of the information necessary to recover business service and operational functions, should a natural disaster or other disruptive event cause a serious interruption of services.

An SCP not only targets business operations, but also ensures the safety of employees and visitors, and mitigates (if not altogether eliminates) the damage that disasters or disruptions can cause.

It is important to practice and document preparations prior to a disaster or serious interruption so that you are prepared when a threat does emerge. It's also essential to document the plan efficiently in order to guarantee a speedy recovery of services and the continuity of all critical business functions. Any changes to the plan should be fully communicated to the rest of the department, team, or business.

A SCP, when written correctly, should be a comprehensive plan of action, unique to your organisation, that provides guidance on how to deal with a disruption, emergency, or disaster. To help you gain a better sense of the key components included in a SCP, here is an example table of contents that lists each section of the document:

- Business name (usually appears on the title page and includes the date of BCP completion)
- Context and scope
- Policy information
- Emergency management and response
- Business impact analysis
- Recovery strategies (with step-by-step instructions)
- Relevant appendices (plan-enabling information)

Keep in mind that every business is different — therefore, no two SCPs look the same. Tailor your services continuity plan to your organisation, and make sure the document captures all the information necessary to maintain your service operations. Having everything you need to know in the event of an emergency is the most important part of service continuity planning.

CONTEXT

Disaster Recovery and Business Continuity

Disaster recovery and business continuity planning are clearly interlinked due to the potential for a natural disasters (e.g. earthquakes, volcanic eruptions, serious flooding, extreme weather - cyclones etc.) to cause business interruption.

However, business or services interruption can also result from other serious interruptive events (e.g. loss of key personnel, fire, energy disruption, communication disruption, civil emergency etc.), which may or may not be the result of natural disasters.

Therefore it is sensible to focus on the risk or threat of occurrence of these serious interruptive events (SIE) rather than what may have caused them.

Risk-based Planning

The potential for the occurrence of SIE poses a risk for the organisation and accordingly service continuity planning should be linked with, or be a subset of, the organisation's risk management planning.

Effective risk management requires the prioritisation of risks to ensure that organisational resources are focussed on mitigating the risk events that are most likely to have a major organisational impact. Similarly, it make sense in service continuity planning to apply risk management principles in focussing our attention on those SIE that could potentially have the greatest impact on services continuity.

Accordingly, it is logical to frame this policy within our Risk Management Policy and assess potential SIE according to their likelihood of occurrence and the severity of their impact on service continuity. This rating can inform our level of investment in developing potential recovery strategies – i.e. mitigating the potential risks for the occurrence of SIE.

PLANNING FRAMEWORK

The following planning framework adopts a risk-based approach to developing a services continuity plan.

1. Context & Scope Definition	2. Services Impact Analysis	3. Recovery Strategies	4. Testing & Revising
You begin by describing the business/services context and the likely service -interruption threats. Then you determine the scope of the plan – identifying the services that are regarded as essential and	During this phase, you assess the potential factors (significant interruptive events – SIE) that could harm your service operation and you create a risk-based services impact analysis (SIA). Review the SIA with Board of Trustees, staff and other key stakeholders to ensure visibility	For each of the SIE rated as a medium, high or very high risk of occurrence, determine a plausible recovery strategy based on the needs of the business and the SIA, and document and implement that strategy	Create a test plan and subsequent exercises that can be performed by the business to ensure that the business continuity plan works successfully. Update the SCP as needed based on the tests and exercises

CONTEXT & SCOPE

The first step in Services Continuity Planning (SCP) is to define the context and scope of the plan.

The **SCP context** definition should present a general description the organisation and its services that enable a high level understanding of its general vulnerability to significant interruptive events.

This description could include:

- **Operational context** – understanding the business:
    - service(s) centres: virtual/physical-location;
    - services: a brief profile of the services provided;
    - people: organisational governance and staffing; consultant/collaborator dependencies;
    - clients: a summary profile of client base;
    - facilities and systems: physical and technology dependencies
- **Interruption threats** – essentially a high level risk analysis
    - locational vulnerability to natural disasters;
    - history/previous experience of interruption events as relevant
    - primary areas of service continuity concern – brief summary of high risk areas;
    - general mitigating factors – operational potential to cope with high risk threats; and
    - relevant history/previous experience of interruptive events.

Defining **SCP scope** involves clearly and succinctly describing:

- the **objective**(s) of the plan;
- the **range of services** that will be included noting:
    - those services that are regarded as critical – essential,
    - the key resource factors for the delivery of each service
    - the recovery status to be achieved for each service – necessary to desirable;
    - the time period tolerance for the service to be unavailable and why;

With context and scope defined, the next step is to complete the services impact analysis

SERVICES IMPACT ANALYSIS

The first step in the continuity planning process is to understand the potential for our services to be substantially disrupted by a significant interruptive event (SIE).

Such events may include, for example, loss of key personnel (resignation, ill health etc.), fire, energy disruption (loss of electricity, gas etc.), communications disruption (internet loss, website down, system corruption etc.), civil emergency events (police, security etc.).

Once the potential SIE's have been identified you need to prepare a detailed Service Impact Analysis, which:

- details the **nature** of the potential interruptive event;

- assesses its **likelihood** of occurrence (Rare, Unlikely, Possible, Likely, Almost Certain);
- describes the **probable impacts** that such an event would have on the delivery of services;
- rates the **impact consequences** as Insignificant, Minor, Moderate, Major or Severe; and
- **rates the overall risk** of the SIE actually occurring as Very Low, Low, Medium, High and Very High (using the Risk Management Framework[1] ratings).

Consistent with MSTTT Risk Management policy, the services continuity plan must address all SIE rated as MEDIUM to VERY HIGH as follows:

MEDIUM	Tolerable	*A recovery strategy is required but may be acceptable if high costs or action impractical*
HIGH	Intolerable	*A recovery strategy MUST be implemented – scope of action subject to cost-benefit*
VERY HIGH	Unacceptable	*A recovery strategy MUST be implemented irrespective of costs*

Example SIA format[2]:

Services Impact Analysis				
Significant Interruptive Event	Likelihood	Probable Impact	Impact Severity	Risk Rating
Loss of key personnel – resignation, ill health/disability etc.	Possible	Inability to sustain essential support services for regular & vulnerable clients with consequential impacts	Major	HIGH
Major premises fire requiring reconstruction, closure and/or relocation	Possible	Loss of facilities, records, technologies etc. Restricted or no access for staff or clients	Moderate	MEDIUM
Serious breach of information systems security	Possible	Potential loss of confidential client records – reputational and service integrity issues	Major	HIGH
Etc.				

[1] *Refer MSTTT Risk Management Policy*

[2] *Typically this analysis would be recorded in an Excel spreadsheet*

EMERGENCY MANAGEMENT

Short-term interruptive events such as a fire or a civil emergency or a temporary loss of power etc. that only present a limited and manageable temporary interruption to services can be distinguished from major, long-term interruptive events as **emergencies**. These events also require a clear and concise management plan and should be included in the service continuity planning process with the resultant recovery and/or interruption-management plans identified in a separate section of the SCP.

RECOVERY STRATEGIES

Once the SIA is complete, the next process is to design recovery strategies to mitigate the potential impact for each SIE with the focus. During this phase, you will explore many of the SCP response options including, by way of example, the following:

- **Facilities**: Exploring the opportunities, and the necessity, for post disruption facilities (and equipment) including relocation to alternate and/or temporary-shared facilities, potential for non-facility based service provision, working from home etc and the associated transition arrangements;
- **Critical Services**: Finding ways to sustain the essential services as defined in the SCP scope;
- **Data**: Understanding how to recover, restore and/or access the data that is necessary to sustain essential services;.
- **Backlog**: Making allowance for the recovery of service backlogs that were stalled during the SIE;
- **Communication:** Determining the way in which employees, customers and third-party entities will communicate during the emergency;
- **Technology:** Understanding the processes involved in recovering/restoring the of technology systems and processes that are necessary to enable services;
- **Time:** Appreciating the maximum amount of services downtime time that can be sustained before there are severe effects on clients; and
- **Workarounds**: Exploring the potential for manual workarounds and alternative service delivery options that could assure the failure of planned recovery options.

Example Recovery Strategies format:

SIE Recovery Strategies					
SIE	Probable Impact				
Loss of key personnel – resignation, ill health/disability etc.	Inability to sustain essential support services for regular & vulnerable clients with consequential impacts				
Recovery Strategies	Impact Zone	Recovery Time	Estimated Cost Impacts	Resp. Person	Tested
Implement staff position covers as per succession-cover plan	People	Two weeks	Cost: $3,000 per cover per week	Name	Date

Implement XYZ collaborative service support arrangement	People	48 hours	Revenue loss: $5,000 per service per week	Name	Date
SIE	Probable Impact				
Major premises fire requiring reconstruction, closure and/or relocation	Loss of facilities, records, systems, technologies, etc. Restricted or no access for staff or clients to centre				
Recovery Strategies	Impact Zone	Recovery Time	Resource-cost Impacts	Resp. Person	Tested
Implement virtual office & outreach workers strategy	Facilities	One week	Cost: $500 per staff per week	Name	Date
Implement technology recovery strategy – hardware, systems, files	Tech.	One week	Cost: $2000 per laptop $5,000 system restore contract	Name	Date
Etc.					

Enabling Documentation

Another significant feature of your SCP is the enabling documentation - specific information you may need to reference once you put the plan into place. This information, which is usually located in the appendices, will vary based on the particulars of your SCP, but may include the following:

- Employee contact list identifying recovery critical roles
- Recovery priorities for critical business functions
- Alternate site recovery resource requirements (could also include alternate site transportation and accommodation information)
- Agreements with service partners or other service providers that will provide service-recovery support
- Emergency services locations
- Critical records
- Vendor and third-party list
- Relevant computer system recovery and support documentation
- Impact and risk assessments
- Recovery task lists
- Recommended office recovery plan
- Business policy or handbook

Quality Assurance

The final step is to implement and test the SCP in full. It is important to conduct training activities throughout the organisation to ensure that everyone is familiar with the plan and knows how to respond to a significant interruptive event. This training can take the form of an orientation or education, walk-through drills, functional drills, or full-scale run-throughs. These exercises will ensure that the preparedness and response strategies you've developed in the SCP actually work when put to the test.