IT Service Continuity Framework (ITSCF)

By

ITA

(Information Technology Authority)

هيئة تقنية المعلومات
سلطنة عمان
Information Technology Authority
Sultanate of Oman

Document control:

Attributes	Value
Document title:	IT Service Continuity Framework (ITSCF)
Document Owner:	Governance and Standards Division, ITA
Document Type:	Official
Document Approval:	CEO office, ITA
Document Circulation:	All Ministries and Government Agencies

Version control:

Version	Author	Date	Comments	Approved by
Final draft 1.02	Governance and Standard Division, ITA	12 Feb 2018		
Final draft 1.03	Governance and Standard Division, ITA	29 April 2018	Revision and update	
Final draft 1.04	Governance and Standard Division, ITA	4th June 2018	Revision and update	CEO office, ITA

Contents

This page is intentionally left blank.

Introduction

Information Technology (IT) represents a significant investment as well as a significant enabler of the eOman vision, requiring effective governance and planning. Pursuant to, Royal Decree 52/2006, Information Technology Authority (ITA) is responsible for implementation of the Digital Oman Strategy and to develop Policies, frameworks, standards and guidelines for government agencies.

Today Information technology (IT) has become a vital part of any business, which are elements of the critical infrastructures in all organizational sectors, whether public or private. The propagation of the Internet and other electronic service and networking devices/services, and today's capabilities of Infrastructure and applications, has also meant that organizations have become ever more dependent on trustworthy, safe and secure IT infrastructures.

Information systems are vital elements in most business processes because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

ITA has developed an Information Technology Service Continuity Framework (ITSCF) to address the need for having a contingency plan for the IT sector within government entities. The framework can be used by any government entity and it should be aligned with their own Business Continuity initiative. The framework comprise of eight (8) management practices in order to fulfill the need of having a Continuity arrangements within IT domain.

What is IT Continuity Management?

Service Continuity Management is a reactive and proactive process. It involves contingency planning for recovery in case an unforeseen disaster or event were to seriously affect or destroy IT service. It also involves risk analysis and the implementation of countermeasures to minimize the likelihood of such an event happening in the first place.

As the title of the process suggests, Service Continuity Management is about maintaining continuity of service – that is to say not just the continuation of equipment. It therefore follows that we must consider all components of the service, not just the hardware and software. Similarly, the risks are not confined to the dramatic and remote-sounding examples of fire, flood and terrorist attack. There are many more commonplace possibilities such as a severed cable under a road, a leaking central-heating system, destructive software virus, transport difficulties affecting staff and loss of system password.

Why use IT Continuity Management?

The difference between IT Continuity Management and 'disaster recovery' is that Service Continuity Management includes a proactive element to reduce risk, whereas 'disaster

recovery' is usually just the reactive part. Other benefits of IT Continuity Management include the following.

• The focus on service, rather than equipment, aligns the process with the overall school and IT strategy, not just the technical support strategy.

• Having a contingency plan reduces the impact on governmental activities of a medium to long-term IT outage.

• Good service continuity management can help to reduce the cost of insurance.

• It allows technical support to understand the importance and priority of each IT service within the entity, which is beneficial day to day, not just in the event of a disaster. Do not think 'it won't happen to me'. Service Continuity Management is not just for dramatic disasters – workaday accidents do happen!

The Business Value of IT Service Continuity Framework (ITSCF)

Due to the high probability of calamities happening worldwide there is crucial, need of arrangements to be made by any business/organization to survive or at least continue providing their core services in such unfortunate event. So Continuity arrangements are of high value for any business/organization, there are certain factors, which are playing an important part in Continuity domain or considered to be main drivers for Continuity arrangements, these are but not limited to:

• **Regulatory requirements**

In some industries, a recovery capability is becoming a mandatory requirement such as health, defense, and financial industries

• **Business relationship**

The requirement to work closely with the business to develop and maintain a continuity capability fosters a much closer working relationship between IT and the business areas

• **Positive marketing of contingency capabilities**

Being able to demonstrate effective ITCM capabilities enables an organization to provide high service levels to clients and customers and thus win business

• **Organizational credibility**

There is a responsibility on the directors of organizations to protect the shareholders' interest and those of their clients

• **Competitive advantage**

Service organizations are increasingly being asked by business partners, customers and stakeholders to demonstrate their contingency facilities and may not be invited to tender for business unless they can demonstrate appropriate recovery capabilities.

Scope

The scope of "IT Service Continuity Framework (ITSCF)" is limited to IT and not Business continuity moreover this framework is focused on IT, In case of a disaster/ disruption or in any calamity whether natural or man-made, this framework if adopted can serve the purpose, so that an organization can continue to deliver its critical ITs in such difficult situation.

Hence, this framework is focused on Continuity of IT, however it should be aligned with the organization's overall Business continuity management (BCM).

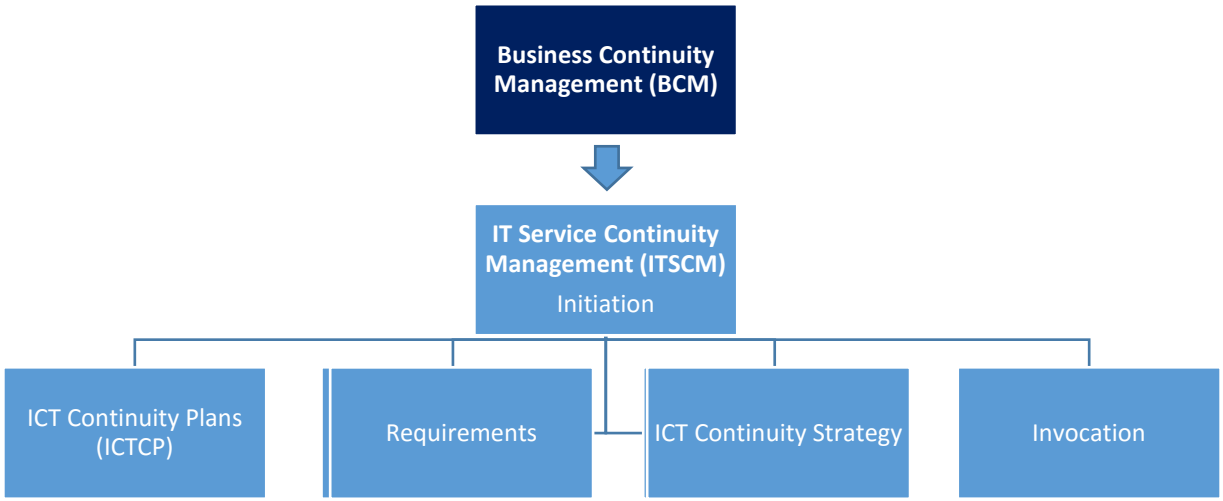

Fig: Alignment of ITCM with Business Continuity

In the figure above the IT Continuity management part is covered in the framework i.e. ITCP (IT Continuity Plan) will take inputs from 'Business Continuity Strategy' and 'Requirements', which lies in the Business Continuity Management (BCM) domain. Than all the stages of IT continuity will provide inputs/outputs as shown in the figure and are covered in this framework.

Target audience

The framework is intended for IT professionals who have basic knowledge and experience of Disaster recovery and Business Continuity management concepts. The document did not explain the terms and definitions, as they are self-explanatory and meant for practitioners who are working in Continuity domain and understand the concepts of Business and IT Continuity.

The framework is directed towards government entities i.e. Ministries and government authorities so that organizations in Oman government can utilize and take benefits from this framework. The framework give direction from the governance point of view, to set the direction and course for any organization (government entity) so that they can have basic outline or structure as a guide in achieving Continuity in case of any calamity.

As the framework (ITSCF) is devised from a governance perspective, it sets few management practices for senior management, which once established, maintained and followed properly

will certainly provide value to business. Therefore, this framework is intended for Oman public sector only, to be used as a reference or it will provide basic guidance to any government organization who want to initiate/establish IT Continuity Project in their organization.

Description of IT Service Continuity Framework

Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required ITs and maintain availability of information at a level acceptable to the enterprise.

Purpose Statement

Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.

The process supports the achievement of a set of primary IT-related goals:

IT-related Goal	Related Metrics
Managed IT-related business risk	• Percent of critical business processes, IT and IT-enabled business programs covered by risk assessment • Number of significant IT-related incidents that were not identified in risk assessment • Frequency of update of risk profile
Delivery of IT in line with business requirements	• Number of business disruptions due to IT incidents • Percent of business stakeholders satisfied that IT delivery meets agreed-on service levels • Percent of users satisfied with the quality of IT delivery
Availability of reliable and useful information for decision making	• Level of business user satisfaction with quality and timeliness (or availability) of management information • Number of business process incidents caused by non-availability of information • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor

Process Goals and Metrics

Process Goal	Related Metrics
1. Business-critical information is available to the business in line with minimum required service levels.	• Percent of ITs meeting uptime requirements • Percent of successful and timely restoration from backup or alternate media copies • Percent of backup media transferred and stored securely
2. Sufficient resilience is in place for critical services.	• Number of critical business systems not covered by the plan

3. Service continuity tests have verified the effectiveness of the plan.	• Number of exercises and tests that have achieved recovery objectives • Frequency of tests
4. An up-to-date continuity plan reflects current business requirements.	• Percent of agreed-on improvements to the plan that have been reflected in the plan • Percent of issues identified that have been subsequently addressed in the plan
5. Internal and external parties have been trained in the continuity plan.	• Percent of internal and external stakeholders that have received training • Percent of issues identified that have been subsequently addressed in the training materials

Initiation of IT Continuity

When implementing an ITSCF (IT Service Continuity Framework) programme for the first time in an organization, project management disciplines should be adopted, which define clear deliverables, budgets and timescales.

Once the ITSCF (IT Service Continuity Framework) programme has been established and the key elements are in place, further work programmes are likely to develop as the maintenance, testing, training and review cycle get under way and the BCP evolves.

Initiating the programme should include:

- Goals and objectives of strategic and operational activities of ITSCF (IT Service Continuity Framework)
- Identification of deliverables and outcomes
- Timescales and deadlines
- Constraints
- Budget and work effort control
- Resourcing capabilities

There are several project management methods, some of which have software support. The method selected should be appropriate to the size and complexity of the organization.

Assign ITCM (IT Continuity Management) responsibilities

The senior management team should appoint or nominate a person with appropriate seniority and authority to be accountable for IT Continuity Policy and implementation and appoint one or more individuals to deliver and maintain the IT Continuity programme.

Essentially, responsibility for the implementation and ongoing day-to-day management of the IT Continuity project is undertaken by two teams, the IT Continuity Management Team and the Business Continuity Steering Committee.

In addition to it, specific teams will be appointed to deal with incidents.

The team structures proposed in the following paragraphs to steer and deliver the IT Continuity Project, derived from some leading standards, better suit the need of larger organizations as in smaller organizations many roles and responsibilities may be bundled together and covered by fewer teams/people. This holds true also for the teams in charge of operations following an incident.

Management and structure

The IT Continuity Management Team will be led by the IT Continuity Manager, who will be responsible for the delivery of the IT Continuity Plan (ITCP), embedding Continuity within the organization and ongoing maintenance of the IT Continuity Plan (ITCP). Depending on the scope of the programme the IT Continuity Manager might be assisted by a IT Continuity Analyst. In large organizations, there may also be Continuity coordinators within each business unit, who are responsible for assisting with the gathering of the impact data and for writing and maintaining their own business unit recovery plans under the guidance of the IT Continuity Manager.

The IT Continuity Manager does not necessarily become a member of the Incident Management Team during an incident. Rather, this role is often used in a consultative capacity wing to its extensive knowledge of the organization.

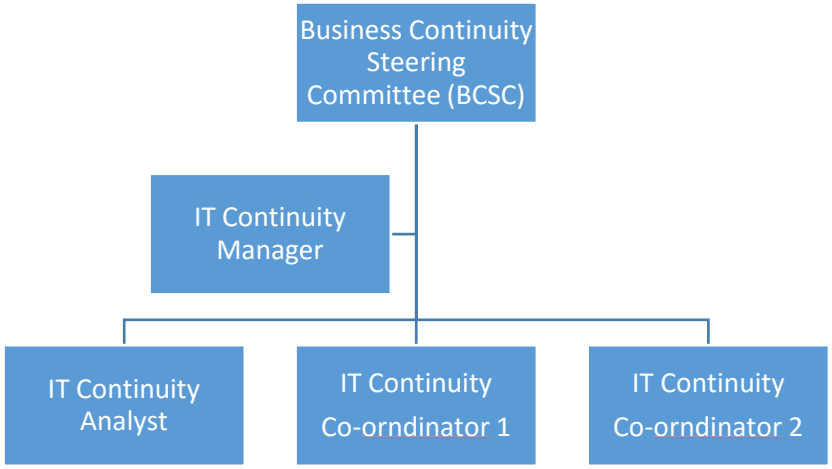

Fig: Hierarchy of organization structure for IT Continuity

ITSCF Key Management Practices:

In order to adopt the this framework, the management needs to follow or incorporate certain practices for an organization to achieve the continuity of its core services in times of disaster/calamities or any unfortunate incident, which may cause serious damage to an organization's reputation or critical business. The ITSCF management practices are as follows:

ITSCF-01 - Define the IT Continuity Policy, objectives and scope.

ITSCF-02 - Maintain an IT Continuity strategy.

ITSCF-03 - Develop and implement an IT continuity response.

ITSCF-04 - Exercise, test and review the ITCP (IT Continuity Plan).

ITSCF-05 - Review, maintain and improve the Continuity plan (ITCP).

ITSCF-06 - Conduct Continuity plan (ITCP) training

ITSCF-07 - Manage backup arrangements

ITSCF-08 - Conduct post-resumption review

For each of the above IT continuity management practice there are certain inputs, outputs and activities defined. So that if senior management in any government entity define, implement, follow and maintain these management practices than they are in a better position to react efficiently and effectively to any unfortunate/ unforeseen event or disaster which may interrupt their capability to provide IT services.

Inputs/Outputs and Activities:

<table>
<tr><th colspan="5">Inputs/Outputs and Activities</th></tr>
<tr><td>Management Practice</td><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="4">ITSCF-01 Define the IT Continuity Policy, objectives and scope.

Define IT Continuity Policy and scope aligned with enterprise and stakeholder objectives</td><th>From</th><th>Description</th><th>Description</th><th>To</th></tr>
<tr><td rowspan="3">Business goals, Objectives, Business continuity Management documents</td><td rowspan="3">Business related goals and objectives, SLAs, Agreements</td><td>Policy and objectives for IT continuity</td><td>ITCM team</td></tr>
<tr><td>Disruptive incident scenarios</td><td>ITCM team</td></tr>
<tr><td>Assessments of current continuity capabilities and gaps</td><td>ITCM team</td></tr>
<tr><td colspan="5">Activities</td></tr>
<tr><td colspan="5">1. Identify internal and outsourced business processes and service activities that are critical to the enterprise operations or necessary to meet legal and/ or contractual obligations.</td></tr>
<tr><td colspan="5">2. Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.</td></tr>
<tr><td colspan="5">3. Define and document the agreed-on minimum policy objectives and scope for business continuity and embed the need for continuity planning in the enterprise culture.</td></tr>
<tr><td colspan="5">4. Identify essential supporting business processes and related ITs.</td></tr>
</table>

<table>
<tr><th>Management Practice</th><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="4">ITSCF-02 - Maintain an IT Continuity strategy.

Evaluate IT Continuity Management options and choose a cost-effective and viable continuity strategy that will ensure enterprise recovery and continuity in the face of a disaster or other major incident or disruption.</td><th>From</th><th>Description</th><th>Description</th><th>To</th></tr>
<tr><td rowspan="3">• Business strategy

• Enterprise Risk Management</td><td rowspan="3">• Risk-related root causes
• Risk impact communications</td><td>Business Impact Analysis</td><td>BIA document</td></tr>
<tr><td>Continuity requirements</td><td>ITCM team</td></tr>
<tr><td>Approved strategic options</td><td>IT continuity documents needs to be updated accordingly</td></tr>
<tr><td colspan="5">Activities</td></tr>
<tr><td colspan="5">1. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.</td></tr>
<tr><td colspan="5">2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.</td></tr>
<tr><td colspan="5">3. Establish the minimum time required to recover a business process and supporting IT based on an acceptable length of business interruption and maximum tolerable outage.</td></tr>
<tr><td colspan="5">4. Assess the likelihood of threats that could cause loss of business continuity and identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.</td></tr>
<tr><td colspan="5">5. Analyze continuity requirements to identify the possible strategic business and technical options.</td></tr>
<tr><td colspan="5">6. Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.</td></tr>
<tr><td colspan="5">7. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.</td></tr>
<tr><td colspan="5">8. Obtain executive business approval for selected strategic options.</td></tr>
</table>

<table>
<tr><th>Management Practice</th><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="2">ITSCF-03 - Develop and implement an IT continuity response.

Develop an IT continuity plan (ITCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the enterprise to continue its critical activities.</td><th>From</th><th>Description</th><th>Description</th><th>To</th></tr>
<tr><td>• Business Strategy

• IT Strategy

• Admin Dept. / Health & Safety management system/ Dept.</td><td>• Alignment with Business Strategy and IT Strategy

• Any agreements (OLAs)</td><td>Incident response actions and communications

IT Continuity Plan (ITCP)</td><td>Incident response document

IT Continuity Policy document</td></tr>
<tr><td colspan="5">Activities</td></tr>
<tr><td colspan="5">1. Define the incident response actions and communications to be taken in the event of disruption. Define related roles and responsibilities, including accountability for policy and implementation.</td></tr>
<tr><td colspan="5">2. Develop and maintain operational ITCP containing the procedures to be followed to enable continued operation of critical business processes and/or temporary processing arrangements, including links to plans of outsourced service providers.</td></tr>
<tr><td colspan="5">3. Ensure that key suppliers and outsource partners have effective continuity plans in place. Obtain audited evidence as required.</td></tr>
<tr><td colspan="5">4. Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity.</td></tr>
<tr><td colspan="5">5. Define and document the resources required to support the continuity and recovery procedures, considering people, facilities and IT infrastructure.</td></tr>
<tr><td colspan="5">6. Define and document the information backup requirements required to support the plans, including plans and paper documents as well as data files, and consider the need for security and off-site storage.</td></tr>
<tr><td colspan="5">7. Determine required skills for individuals involved in executing the plan and procedures.</td></tr>
<tr><td colspan="5">8. Distribute the plans and supporting documentation securely to appropriately authorize interested parties and make sure they are accessible under all disaster scenarios.</td></tr>
</table>

<table>
<tr><th>Management Practice</th><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="4">ITSCF-04 - Exercise, test and review the ITCP (IT Continuity Plan).

Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.</td><th>From</th><th>Description</th><th>Description</th><th>To</th></tr>
<tr><td rowspan="3">• Business Continuity Plan (BCP)

• IT Continuity Plan (ITCP)</td><td rowspan="3">Alignment with BCP developed by BCM (Business Continuity Management) and with ITCP</td><td>Test objectives</td><td>ITCM team</td></tr>
<tr><td>Test exercises</td><td>ITCM team</td></tr>
<tr><td>Test results and recommendations</td><td>ITCM team</td></tr>
<tr><td colspan="5">Activities</td></tr>
<tr><td colspan="5">1. Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the ITCP in meeting business risk.</td></tr>
<tr><td colspan="5">2. Define and agree on with stakeholders exercises that are realistic, validate continuity procedures, and include roles, responsibilities, and data retention arrangements that cause minimum disruption to business processes.</td></tr>
<tr><td colspan="5">3. Assign roles and responsibilities for performing continuity plan exercises and tests.</td></tr>
<tr><td colspan="5">4. Schedule exercises and test activities as defined in the continuity plan.</td></tr>
<tr><td colspan="5">5. Conduct a post-exercise debriefing and analysis to consider the achievement.</td></tr>
<tr><td colspan="5">6. Develop recommendations for improving the current continuity plan based on the results of the review.</td></tr>
</table>

<table>
<tr><th>Management Practice</th><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="4">ITSCF-05 - Review, maintain and improve the Continuity plan (ITCP).

Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plan in accordance with the change control process to ensure that the continuity plan is kept up to date and continually reflects actual business requirements.</td><td>From</td><td>Description</td><td>Description</td><td>To</td></tr>
<tr><td rowspan="3">• Business Continuity Plan (BCP)

• IT Continuity Plan (ITCP)</td><td rowspan="3">Any change in BCP or previous ITCP should be taken into consideration</td><td>Results of reviews of plans</td><td>ITCM team</td></tr>
<tr><td>Recommended changes to plans</td><td>ITCM team</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="5">Activities</td></tr>
<tr><td colspan="5">1. Review the continuity plan and capability on a regular basis against any assumptions made and current business operational and strategic objectives.</td></tr>
<tr><td colspan="5">2. Consider whether a revised business impact assessment may be required, depending on the nature of the change.</td></tr>
<tr><td colspan="5">3. Recommend and communicate changes in policy, plans, procedures, infrastructure, and roles and responsibilities for management approval and processing via the change management process.</td></tr>
<tr><td colspan="5">4. Review the continuity plan on a regular basis to consider the impact of new or major changes to: enterprise organization, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.</td></tr>
</table>

<table>
<tr><th>Management Practice</th><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="3">ITSCF-06 - Conduct Continuity plan (ITCP) training

Provide all concerned internal and external parties with regular training sessions regarding the procedures and their roles and responsibilities in case of disruption.</td><td>From</td><td>Description</td><td>Description</td><td>To</td></tr>
<tr><td rowspan="2">HR/ HRD/ Admin</td><td rowspan="2">List of personnel requiring training</td><td>Training requirements</td><td>Training needs analysis document (TNA)</td></tr>
<tr><td>Monitoring results of skills and competencies</td><td>Appraisals/ KPI as per IT Continuity team arrangement</td></tr>
<tr><td colspan="5">Activities</td></tr>
<tr><td colspan="5">1. Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.</td></tr>
<tr><td colspan="5">2. Develop competencies based on practical training including participation in exercises and tests.</td></tr>
<tr><td colspan="5">3. Monitor skills and competencies based on the exercise and test results.</td></tr>
</table>

<table>
<tr><th>Management Practice</th><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="4">ITSCF-07 Manage backup arrangements.

Maintain availability of business-critical information.</td><th>From</th><th>Description</th><th>Description</th><th>To</th></tr>
<tr><td rowspan="3">• Configuration Management Database (CMDB) OR any Service assets repository

• IT Infrastructure/Applications Dept./ team

• Third party involved for Backup arrangements</td><td rowspan="3">Data can be taken from any Database (CMDB) which stores enterprise Cis (Configuration items)</td><td>Test results of backup data</td><td>ITCM team</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="5">Activities</td></tr>
<tr><td colspan="5">1. Backup systems, applications, data and documentation according to a defined schedule, considering:
• Frequency (monthly, weekly, daily, etc.)
• Mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention)
• Type of backup (e.g., full vs. incremental)
• Type of media • Automated online backups
• Data types (e.g., voice, optical)
• Creation of logs
• Critical end-user computing data (e.g., spreadsheets)
• Physical and logical location of data sources
• Security and access rights • Encryption</td></tr>
<tr><td colspan="5">2. Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.</td></tr>
<tr><td colspan="5">3. Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.</td></tr>
<tr><td colspan="5">4. Roll out BCP awareness and training.</td></tr>
<tr><td colspan="5">5. Periodically test and refresh archived and backup data.</td></tr>
</table>

<table>
<tr><th>Management Practice</th><th colspan="2">Inputs</th><th colspan="2">Outputs</th></tr>
<tr><td rowspan="3">ITSCF-08 - Conduct post-resumption review

Assess the adequacy of the ITCP following the successful resumption of business processes and services after a disruption.</td><td>From</td><td>Description</td><td>Description</td><td>To</td></tr>
<tr><td rowspan="2">IT Continuity Plan (ITCP)</td><td rowspan="2">Validate the adherence to ITCP</td><td>Post-resumption review report</td><td>ITCM team</td></tr>
<tr><td>Approved changes to the plans</td><td>ITCM team</td></tr>
<tr><td colspan="5">Activities</td></tr>
<tr><td colspan="5">1. Assess adherence to the documented IT Continuity Plan (ITCP)</td></tr>
<tr><td colspan="5">2. Determine the effectiveness of the plan, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organizational structures and relationships.</td></tr>
<tr><td colspan="5">3. Identify weaknesses or omissions in the plan and capabilities and make recommendations for improvement.</td></tr>
<tr><td colspan="5">4. Obtain management approval for any changes to the plan and apply via the enterprise change control process.</td></tr>
</table>

Roles and responsibilities:

In order to adopt this IT Service Continuity Framework it is recommended that senior management should assign roles/responsibilities in a defined manner or align their existing roles according to the below chart, which will facilitate the adoption of framework without much difficulty.

In below chart roles are defined and each role has been assigned 'accountability' or 'responsibility' for the fulfillment of a management practice.

RACI chart						
Key Management Practice	IT Director/ Head of IT	Infrastructure/ Internal IT/ IT Support- Director/ Team Lead	Applications/ Software/ Information system- Director/ Team Lead	IT Security Officer	Enterprise Architect/ System analyst	IT Continuity Manager
ITSCF-01 Define the IT Continuity Policy, objectives and scope	A			C	I	R
ITSCF-02 Maintain an IT Continuity strategy	A	C	C	I	I	R
ITSCF-03 Develop and implement an IT continuity response	R		I	I	C	A
ITSCF-04 Exercise, test and review the ITCP (IT Continuity Plan)	R	I	I	C		A
ITSCF-05 Review, maintain and improve the Continuity plan (ITCP)	A			C	C	R
ITSCF-06 Conduct Continuity plan (ITCP) training	R	C	C	I		A
ITSCF-07 Manage backup arrangements		A	C	C		R
ITSCF-08 Conduct post-resumption review	C	R				A

Supporting information

A successful IT DR plan will provide a framework for responding to an IT asset DR incident. Hence, the plan should be simple to follow and user friendly, while containing the minimum detail to support its operation.

However, there are many supporting details that may be needed during DR activities. Some elements of supporting information will be placed within the plans (for example, the key IT asset DR personnel), but often this information can be documented in appendices or in referenced documents.

While the exact amount and types of supporting information will vary between agencies, areas to consider including or linking to include:

- Key IT asset DR personnel
- A full outline of current IT infrastructure
- Staff contact lists (e.g. names, addresses)
- Emergency recordkeeping arrangements and minimum expectations
- Vendor agreements
- Current service provider contacts, and details of services and agreements/expectations regarding the service
- Testing and maintenance processes
- Checklists for ensuring processes meet objectives, all IT infrastructure elements are restored
- Pre-prepared communication messages such as media releases and emails
- Funding/sponsoring sources.

References

COBIT 5 framework – ISACA

NIST publications

ISO 22301 – Business Continuity Standard

BS 25999:2007 - Business Continuity Standard

ISO/IEC 27031- Information technology — Security techniques — Guidelines for Information technology readiness for business continuity

ISO/IEC 20000 - 6.3 Service continuity and availability management

ISO/IEC 27002:2011 - 14. Business Continuity Management

ITIL V3 2011 - Service Design, 4.6 IT Continuity Management

Related abbreviations

- ABC – Activity Based Costing
- ABM – Activity Based Management
- BCM – Business Continuity Management
- BEAST – Baseline, Estimation, Analysis, Simulation, Trends
- BIA – Business Impact Analysis
- CAB – Change Advisory Board
- CAB/EC – CAB Executive Committee
- CDB – Capacity Database
- CFA – Component Failure Analysis
- CFIA – Component Failure Impact Analysis
- CI – Configuration Item
- CMDB – Configuration Management Database
- CRAMM – CCTA Risk Analysis and Management Method
- CRM - Customer Relationship Management
- DR – Disaster recovery
- DSL – Definitive Software Library
- DHS – Definitive Hardware Store
- FTA – Fault Tree Analysis
- ITSCF – Information Technology Continuity Framework
- ITCM - Information Technology Continuity Management
- IPKEC – Incident, Problem, Known Error, Change
- IRS-I-OM – Initiation, Requirements and Strategy, Implementation, Operational Management
- ITIL – Information Technology Infrastructure Library
- ITCM – IT Continuity Management
- ITCP – IT Continuity Plan
- KPI – Key Performance Indicators
- KRA – Key Result Areas
- MARSS – Maintainability, Availability, Reliability, Serviceability, Security
- MTBF – Mean Time Between Failures

• MTTR – Mean Time To Repair
• OGC – Office of Government Commerce
• OLA – Operational Level Agreement
• PCWARD-NMP – Performance, Capacity Database, workload, application Sizing, resource, Demand, Network Management, Modeling
• RCAP – Resource Capacity Management Plan
• RFC – Request For Change
• SCAP – Service Capacity Management
• SEATOP – Software, Equipment, Accommodation, Transfer, Organization, Provider
• SIP – Service Improvement Plan
• SLA – Service Level Agreement
• SLO – Service Level Objectives
• SLM – Service Level Management
• SLR – Service Level Requirements
• SOA – Systems Outage Analysis
• SOB – Service Opportunity Board
• SPAM – Support, Performance, Availability, Money
• TLA – Three Letter Acronym
• UC – Underpinning Contract
• VBF – Vital Business Function