ICT and Business Continuity Management Interconnect Bridge Framework

ISG-RF011, Ver. 1.1

Table of Contents

1 INTRODUCTION

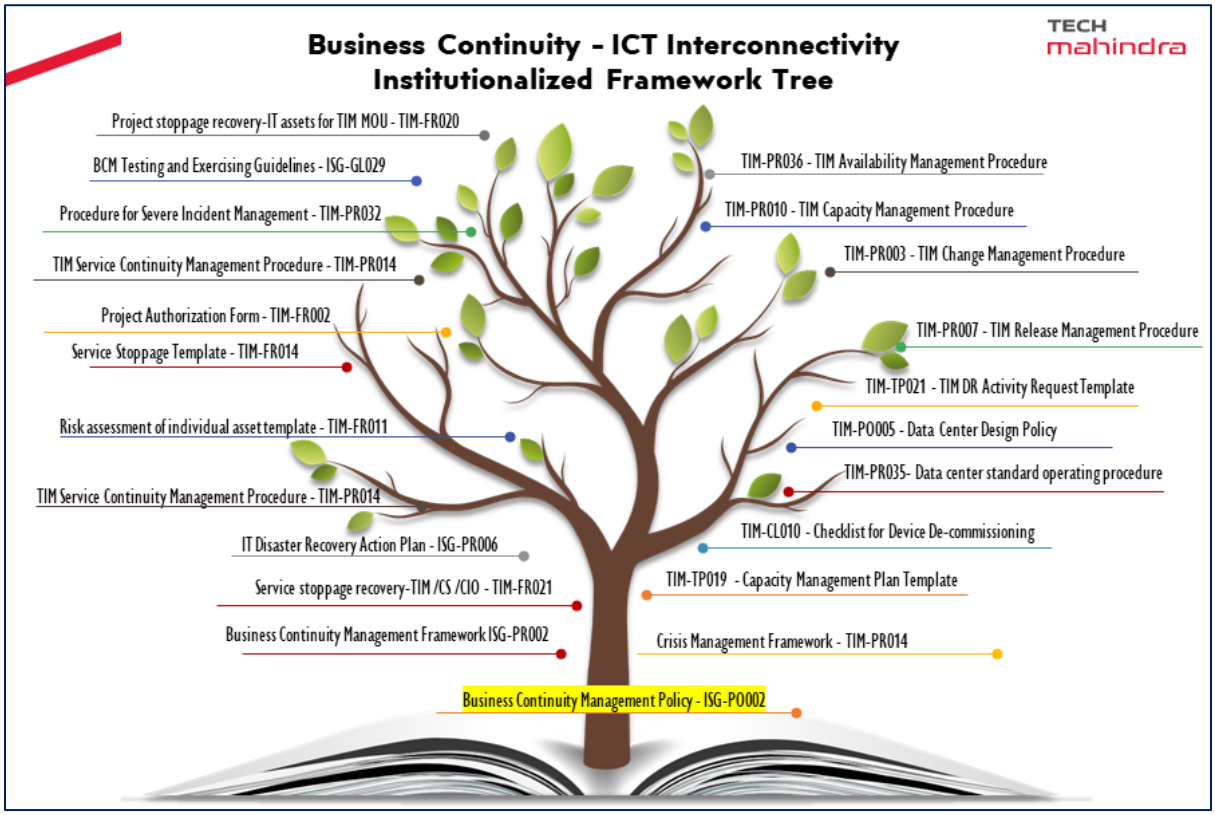
The ICT Business Continuity Interconnect Bridge Framework provides the essential linkages across the Business continuity policy, framework, response plans. This framework connects the required documentation across the organization to meet requirements ISO/2022 associated with ICT readiness for business continuity.

2 SCOPE

The scope of this interconnect bridge framework is to consolidate the interfaces which enable the ICT and business continuity program knit together to meet operational resilience and continuity. The below section provides the linkages to establish the inter-connectivity of the frameworks.

3 BRIDGE AND INTER-CONNECTIVITY

The extract of the standard and guidelines is embedded below to provide the inter-connectivity schema at the corporate global level. A Pictorial representation below provides a quick glance.



The interconnect tree above provides a glance of processes which include policies, frameworks, procedures, guidelines and templates integrated to form the institutionalized management systems for business continuity and ICT/DR across the organization.

The subset of different categories of management systems and associated processes are listed in the sub sections below for a navigational understanding.

3.1 BUSINESS CONTINUITY MANAGEMENT SYSTEM

The business continuity management system is aligned to the ISO22301:2019 standard. This management system is a body of institutionalized processes governed across the organization.

These consist of the Business Continuity Policy, Framework, Testing Guidelines, Crisis Management Framework, Non-IT events disaster action plan and the IT Events Disaster action plan at the organization level. These are aligned to the requirements of the ISO22301:2019 standard.

Sr. No	Document ID	Document Name
1	ISG-PO002	Business Continuity Management Policy
2	ISG-PR002	Business Continuity Management Framework
3	ISG-PR006	IT Disaster Recovery Action Plan
4	ISG-PR07	Non-IT Disaster Recovery Action Plan
5	ISG-PR025	Tech Mahindra Crisis Management Framework
6	ISG-GL029	BCM Testing and Exercising Guidelines

Ownership of Documents	ISG- Business Continuity Management Unit
Hosted on	Business Management System

3.2 CIO - TECHNICAL INFRASTRUCTURE MANAGEMENT – SERVICE CONTINUITY

The Technical Infrastructure Management service continuity procedures and associated templates enable the ICT/DR activities to be integrated. Business Continuity Plan owners who have direct or indirect dependencies on ICT/DR support services integrate their respective ICT/Systems recovery requirements and assessments through these forms and set procedures.

Sr. No	Document ID	Document Name
1	TIM-PR014	IT Service Continuity Management Procedure
2	TIM-PR032	Procedure for Severe Incident Management
3	TIM-FR002	Project Authorization Form
4	TIM-FR011	Risk assessment of individual asset template
5	TIM-FR014	Service Stoppage Template
6	TIM-FR020	Project stoppage recovery-IT assets for TIM MOU
7	TIM-FR021	Service stoppage recovery-TIM /CS /CIO
8	TIM-TP021	TIM DR Activity Request Template

Ownership of Documents	CIO - Technical Infrastructure Management Group
Hosted on	Business Management System

3.3 BACKUP MANAGEMENT SYSTEM

The data backup and restoration management system is governed by the documentation stated below. Requirements of data backup and restoration management are provided by users. It is the responsibility of the respective data owner to engage with the Technical Infrastructure management team for backup schedules, backup failure and corrections, backup / restoration testing. The capability to test data recovery and ability to meet the recovery time objective and recovery point objective is the responsibility of the application owner, system owner and/or the respective accountable individual in the delivery, support, services groups as per internal organizational hierarchy.

Sr. No	Document ID	Document Name
1	TIM-PR004	Backup and Restore Procedure
2	TIM-FR002	Project Authorization Form
3	TIM-FR007	Backup Schedule
4	TIM-FR008	Backup Status Chart
5	TIM-FR009	Tape movement register
6	TIM-W009	Work instructions for Backup Tape movement
7	TIM-W007	Work instructions for Data Management on File Servers
8	TIM-TP001	TIM Data Declaration Template

Ownership of Documents	CIO - Technical Infrastructure Management Group
Hosted on	Business Management System

3.4 CHANGE MANAGEMENT & RELEASE MANAGEMENT

The change management and release management for IT infrastructure includes the processes for change management, checklists for device de-commissioning and release management procedures.

Sr. No	Document ID	Document Name
1	TIM-PR003	TIM Change Management Procedure,
2	TIM-CL010	Checklist for Device De-commissioning
3	TIM-PR007	TIM Release Management Procedure,

Ownership of Documents	CIO - Technical Infrastructure Management Group
Hosted on	Business Management System

3.5 DATA CENTER DESIGN, CAPACITY & AVAILABILITY MANAGEMENT

The data center design, capacity management and availability management procedures to create, monitor and maintain as well as ensure availability of ICT/systems various policies, procedures and templates enable this process.

Sr. No	Document ID	Document Name
1	TIM-PO005	Data Center Design Policy
2	TIM-PR035	Data Center Standard Operating Procedure
3	TIM-PR010	TIM Capacity Management Procedure
4	TIM-TP019	Capacity Management Plan Template
5	TIM-PR036	TIM Availability Management Procedure

Ownership of Documents	CIO - Technical Infrastructure Management Group
Hosted on	Business Management System

3.6 FACILITIES, INFRASTRUCTURE & FIRE SAFETY

The safety and facilities management with respect to continuity of business and environmental safety (Climate Change environmental aspects with respect to Air Quality, HVAC including office space allocation and general facilities management) is supported by the Corporate Services across Tech Mahindra Locations. These services are provided by internal as well as service engagements through third party suppliers for service. These services follow standard operating procedures as

well as the supplier risk management framework across the organization Listed are important documents. Guidelines and templates references are available in the Business Management System (BMS) the repository of policy, guideline, procedure documentation across the organization.

Sr. No	Document ID	Document Name
1	CS-PR012	Contingency Plan
2	CS-PR016	Operations and maintenance of DG
3	CS-PR009	Air Conditioning Operations Procedure
4	CS-PR011	Breakdown Maintenance Procedure
5	CS-PR017	Operations of UPS
6	CS-PR015	Preventive Maintenance Procedure
7	CS-PO001	Pest Control Procedure
8	CS-PR018	Vendor Evaluation for AMC
9	CS-FM000	Corporate Services Function Manual
10	CS-PR064	Space Management Procedure
11	CS-PR028	Physical Security Procedure
12	CS-GL002	Fire Evacuation Guidelines
13	CS-PR040	Planning and Design Stage Procedure – Infrastructure
14	CS-PR042	Infrastructure Project Management Procedure
15	CS-PR068	Process for Development New Infrastructure
16	CS-PR004	Food & Beverage Operations Procedure

Ownership of Documents	Corporate Services
Hosted on	Business Management System

3.7 SUPPORTING GOVERNING REFERENCES

The associated documents which enable crisis management activities across locations to establish governance at locations for the organization are listed below as a reference.

Sr. No	Document ID	Document Name
1	MCOM-PR012	Crisis Management of MARCOM – Org Crisis communication strategy
2	ISG-PO004	Acceptable Usage Policy
3	ISG-PO003	Information Security Incident Management Policy

Ownership of Documents	Marketing, Global Corporate Communications, ISG
Hosted on	Business Management System

4 ENVIGIL

enVIGIL is a platform which hosts a spectrum of tools integrated through in-house developed interfaces. A brief of each Vigil component is provided below along with a pictorial representation. These Vigil suites of applications can be accessed from the ISG Website by users across the organization.

1. **ISG Base Data** – This is the base data amalgamated across organization systems for overall vigilance
2. **Continuity Vigil** – This is the organization Continuity planning, Testing and organization resilience portal
3. **Health Vigil** – The real time project security health vigilance is catered through this portal
4. **Incident Vigil** – This portal is the organization incident management portal

5. **Account Vigil** – MSA insights are available in this portal for management of security in contracts
6. **Audit Vigil** – Audit life cycle management across the organization is managed
7. **Insight Vigil** – Risk and Compliance analytics is provided across the organization
8. **Privacy Vigil** – Privacy information is managed in this portal
9. **Third-Party Vigil** – Third party & supplier risk management is accounted
10. **App Vigil** – Application security and availability vigilance is converged
11. **Subsidiary Vigil** – Security insights of our subsidiaries is visualized
12. **Risk Vigil** – Identification of security and privacy risks is managed
13. **DLP Vigil** – Information about the DLP control points is attained
14. **Cloud Vigil** – Cloud risks are managed through this interface
15. **Compliance Vigil** – This is the foundation vigil which provides the overall compliance performance.

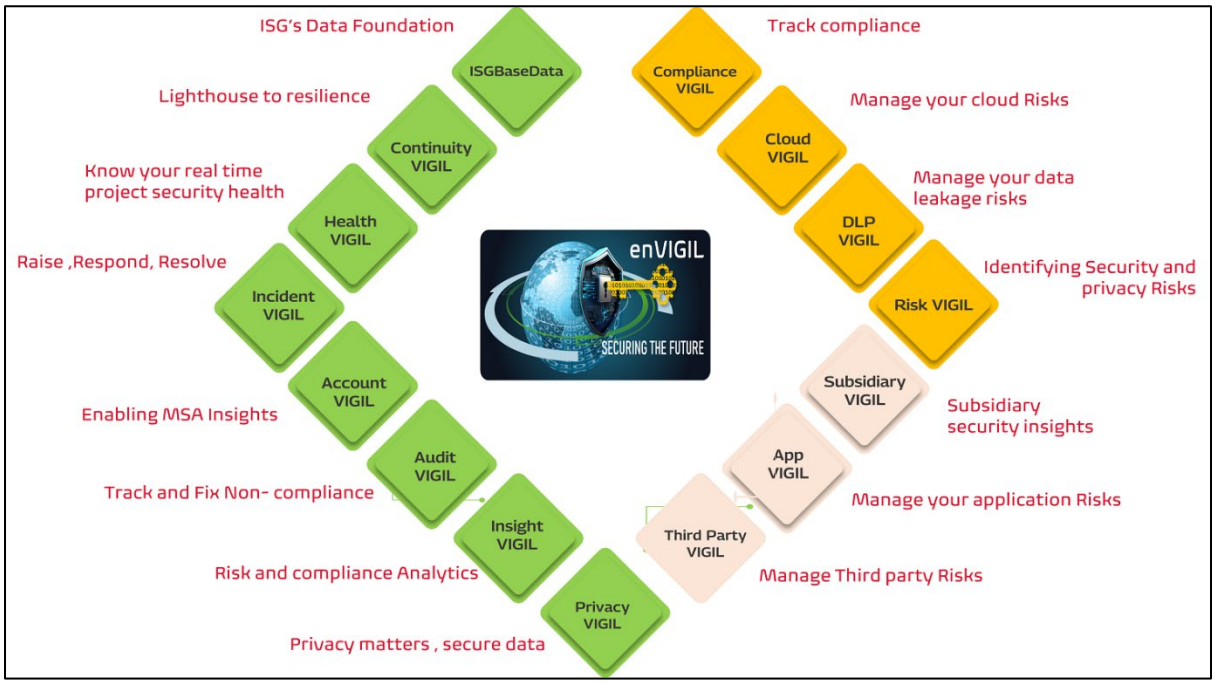
For the business continuity and ICT/DR and associated availability risk management the managers (Projects, Functions, Support team representatives, Location representatives) document their continuity plans in LIGHTHOUSE – Continuity Vigil.

The continuity plans are tested as per schedules and results are documented in Lighthouse – Continuity Vigil. Learning and risks are documented in respective risk treatment plans by the associated plan owners and tracked to closure.

Continuity Vigil – lighthouse to resilience provides an observatory of operational risks with respect to continuity plans, memorandum of understanding for dependent services documentation, testing insights to enable the plan owners take necessary action.

This enables the plan owner to ensure that the risk exposure is maintained at sustainable acceptable risk levels to ensure the recovery time objectives, and the minimum operating levels are met across People, Environments, ICT/DR requirements, Facilities support requirements and continuity of business integrated to asset protection and safety.

The risk management team provides analysis and documents the information security risk register highlights consolidating organization wide risks. The board is provided with highlights through periodic updates as a continuous practice of governance. The enVIGIL applications and analytical tools are the sources for data and analytical views.



5 ACCEPTABLE USAGE POLICY APPLICABILITY

The organization acceptable usage policy is applicable across potential disruptions which could result in ICT/DR procedure activation as well as a Business Continuity potential scenario or disruption where the ICT/DR procedures, plans are activated as well as partial or full business continuity plans are activated.

6 DOCUMENTATION REVIEW

This document is reviewed annually for changes. Intermediary reviews are executed on a case-to-case basis.

7 DOCUMENT HISTORY

Version	Date	Author (function)	Reviewed by	Approved by	Nature of changes
Issue 1.0	20 Aug 2024	Global Business Continuity	Harsha Sastry	Lucius Lobo	Integrated First issue for ISO27001:2022 as a Bridge Interconnect for ICT/DR & Business Continuity A.5.30
1.1	12th Dec 2024	Jayesh	Harsha Sastry	Lucius Lobo	Reviewed copy of the Apex Document for ICT/DR & BCM for ISO22301:2019 and ISO27K: - including of enVIGIL applications information, Corporate Services and References for People Safety, Environment Safety and Fire Evacuation practices

8 APPENDIX A: ANNUAL REVIEW HISTORY

Annual Review Conducted On	Version Reviewed	Is Change Required (Y/N)	Document Uploaded in BMS (Date)	Remarks