CERN IT Business Continuity Policy

This document covers the overall approach to Business Continuity in the IT department. It is complemented by the IT Business Continuity Plan and IT Disaster Recovery Procedures which provide the details of how to prepare, respond and recover. The policy focuses on what should be done compared to the plans documents which relate to how to execute.

Changes to this document are summarized in the following table in reverse chronological order (the latest version first).

Version	Date	Created by	Short Description of Changes
1.0	12th October 2023	Tim Bell	Approved by the IT department head office
0.2	30th August 2023	Tim Bell	Comments incorporated. Circulated to IT GLs and DROIT
0.1	5th July 2023	Tim Bell	Draft with comments from SL, WS and GM

Table of Contents

Introduction

CERN requires that business continuity plans be created such that operations can continue (potentially at a reduced capacity) and quickly recover following a loss of service or resources due to a major interruption. Our users, employees, contractors and other stakeholders depend on the IT department (http://cern.ch/it) to provide computing services as promised. This policy defines who is responsible for protecting the organisation's assets by planning for a disaster and what needs to be done to ensure that CERN can continue operations during and after a major outage.

In the IT department strategy 2022-2025 (https://cds.cern.ch/record/2799153/files/CERN%20IT%20department%20strategy%202022-2025.pdf), the lack of business continuity and disaster recovery (BC/DR) procedures was identified as a significant operational risk. The strategy goal to enable BC/DR for the department's services was agreed to "Enable teams to apply business continuity and disaster recovery policies through dedicated resources, training and senior buy-in to mitigate risks"

This policy is maintained by the Department Business Continuity Coordinator (DBCC) and will be reviewed annually. Significant changes will be submitted to the IT department head office for review and endorsement. The latest version is available at https://disaster-recovery.web.cern.ch/documents/cern-it-business-continuity-policy.

This policy was approved by IT management in October 2023. The IT department Business Continuity Plan (BCP) includes the roadmaps for implementation.

Definitions

The full glossary for BC/DR is at https://disaster-recovery.web.cern.ch/documents/cern-it-bcdr-glossary. Each term used in this document will be written in full the first time it is used with its acronym in brackets afterwards. The acronym is generally used thereafter. The list of terms is included in "Appendix #1: Definitions" for completeness.

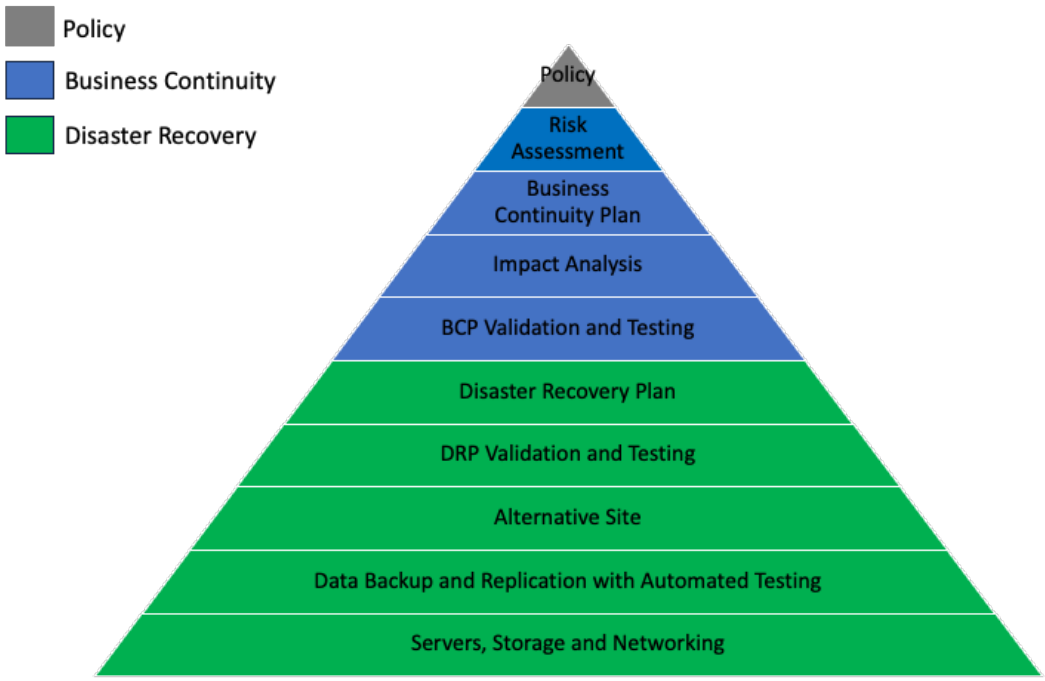
Scope

This policy encompasses all IT and business processes used in the day-to-day operation of the IT department, i.e. the role as a provider. Every employee of the department is responsible for understanding their activity in following this policy.

Throughout this document, IT services will be used to describe the processes and IT applications, frameworks and systems used to deliver them.

Policy

The IT department is required to create, maintain, and test a business continuity plan for services under their responsibility.



The following sections list the activities that must be performed.

Risk Assessment

The IT department will maintain an IT department risk register including details of the impact and likelihood of risks to IT services.

This risk register is maintained by the IT Department Risk Manager (DRM) following these guidelines and is updated annually. Following a review with the IT Department Head, the results are submitted to the CERN Enterprise Risk Management team.

Following the ERM process, the criteria for department risk registers is defined as the following sections.

Critical Resources and Key Processes Identification

A Business Impact Analysis (BIA) must be performed for each key process and system used in the department's areas of responsibility. Each critical system and source of data for these systems must be identified and the importance to the Organisation documented. The BIA and risk assessments must include:

a) An exhaustive list of all processes necessary for the department to function
b) Financial, scientific and reputation impact for the loss of an IT service
c) Regulatory or legal requirements impacted by the loss of an IT service
d) The Recovery Time Objective (RTO) for each IT service
e) The Recovery Point Objective (RPO) for data and applicable resources

The BIA will be reviewed annually with the business units via the IT engagement channel and with the IT Technical Delivery to confirm that the desired and tested recovery objectives are consistent.

Service Design

All IT services should consider recoverability as a central part of their design and implementation.

Each system should clearly identify the backup and recovery processes including frequency, retention, resilience, and verification. This information should be made easily accessible to users of the service as part of the service level description. Any significant change in the design should be reviewed by the IT Architecture Review Board (ARB) according to the Data Recoverability concepts and the ARB checklists. The IT Change and Release Management Board (CRMB) checklist should include the need to produce evidence of compliance according to the CIS Critical Security Controls - control 11.

Each IT service is responsible to ensure that the recovery objectives of any IT service it depends on is compatible with its service levels.

Business Continuity Plan

The IT Business Continuity Plan (BCP) covers how an incident would be handled. This is based on a "Prepare, Respond and Recover" approach.

The DBCC is responsible for validating that the BCP is kept up to date and is tested on a regular basis.

The IT Service Catalog as defined in Service Now will be used to structure the analysis and planning. Where this process suggests improvements to the catalog, these will be reviewed in conjunction with the IT Service Management team.

"Prepare" covers the steps prior to an incident such as

a) Defining responsibilities and roles
b) Ensuring availability of recovery sites and resources
c) Document steps to recover and testing details to demonstrate the correctness
d) Defining a framework to update plans as changes occur, and perform regular testing thereof

"Respond" must include the following:

a) An emergency notification plan for executive management and department heads
b) A communication plan for different parts of the user community
c) Mitigation plans to allow critical process to continue, potentially with reduced capacity, in the event of an outage. This should be reviewed regularly as defined in the BCP.

"Recover" must include the following:

a) Information required to restore systems and processes identified in the BIA
b) Prioritisation of business function recovery after a disaster
c) Prioritisation of all critical technology components needed to recover services for other sectors
d) A Disaster Recovery Plan (DRP) for each IT service including the steps needed to restore access after a disaster (such as at an alternative site or infrastructure).
e) The DRP must be updated after a significant change of the IT service.
f) Document how the plan will meet the RTO and RPO for each IT service

Plan Maintenance and Testing

The following minimum requirements should be met:

a) The BCP should be reviewed regularly for new or changed risks and updated to reflect any organizational changes. Frequency to be defined in the BCP, but at least annually.
b) Each service should execute a test of its individual DRP regularly (such as to restore an environment and validate functionality) and recovery times from the disaster scenario logged. Frequency to be defined in the DRP, but at least annually. This is part of the standard responsibilities of all IT services.
c) Where there are differences between the desired recovery objectives from the business and the actual results from the testing, these should be addressed via new initiatives with the engagement channels or modification of the service levels if the risk of delayed recovery is accepted
d) The test of the IT BCP and the DRP for each IT service must be performed at least during every accelerator long shutdown to ensure compliance with RTO/RPO defined in the IT service level. An example scenario would be a disconnect test of one of the CERN data centres.
e) Any exemptions should be submitted including justification to the DBCC. If these are accepted, they will be documented in the corresponding plan documentation.

Training

The BCP for the IT department should define a training plan for those IT department members who may be involved in designing, testing and recovery of IT services.

Standards

There are a number of industry standards in this area such as ISO22301 (Business Continuity) and ISO 27001 (Disaster Recovery). While these can provide inspiration for some of the approaches, it is not proposed to become certified due to the significant effort to fully comply (even if not relevant to CERN IT service delivery) and handling divergence between industry and CERN governance.

For assessments, checklists such as **CIS Critical Security Controls** can be used to provide an industry framework.

Open Points

Any open issues with the BC/DR policy are tracked in https://its.cern.ch/jira/browse/BCDR-33.

Compliance

An as-is assessment on the status of the BCP will be performed by the DBCC annually with a report submitted to the IT Department Head Office (DHO).

Appendix #1: Definitions

Term	*Definitions*
Architecture Review Board (ARB)	The Architecture Review Board is the IT governance body that assesses project compliance with the standard IT technical architecture. In this capacity, the Architecture Review Board reviews how projects integrate with the services, standards and frameworks of the department, ensuring compatibility and cohesion across the environment.
Business Continuity Plan (BCP)	A Business Continuity Plan provides documented procedures to guide CERN IT to prepare, respond and recover to a pre-defined level of operation following disruption.
Business Impact Analysis (BIA)	Process of analysing CERN business processes and the CERN IT services and activities including the effect of a business disruption in the event of an outage.
Change and Release Management Board (CRMB)	The Change and Release Management Board assesses the suitability of significant service changes or project releases for production deployment. The CRMB is chaired by the Technical Delivery lead and meets monthly, aligned with the Demand Management Review and Architecture Review Board meetings. In exceptional cases board meetings may be organised on demand.
Departmental Business Continuity Coordinator (DBCC)	The department lead for business continuity, providing BC advice and guidance across the department, and ensuring that suitable BC arrangements are in place that are exercised and reviewed on a regular basis.
Department Business Continuity Program Sponsor (DBCPS)	An executive sponsor of Business Continuity who reviews and approves changes to the plans and signs off the annual test report.
Disaster Recovery Plan (DRP)	The description of how each IT service will recover from an incident along with how it would be tested.
Recovery Point Objective (RPO)	The loss of data in the event of an incident. This will depend on the backup frequency and recovery infrastructure. A daily backup would therefore have an RPO of 24 hours.
Recovery Time Objective (RTO)	The time taken to restore an application and its associated data in the event of an incident. This will depend on the recovery strategy such as active/active or cold and the scenario. The RTO can be specified as estimated (eRTO from architecture), actual (aRTO from testing) or desired (dRTO for business processes)

Service Component (SC)	As defined in Enterprise Architecture, the service components are part of a service element describing a unique part which has specific characteristics.
Service Element (SE)	The unit of IT service delivered as seen by the end users. This is based on ITIL standard and implemented in ServiceNow (SNOW)

Background Material

Description	Description
BC/DR concepts	Acronyms and overall approach to implement BC/DR in CERN IT
Data Recoverability Concepts and Strategy	How backup and restore should be implemented and validated in CERN IT