



1 MONTH TO COMPLETION

SCOPE – UNDERSTAND NEEDS AND ASSESSMENT PARAMETERS

Use of Existing Certification

Many organizations have some form of information security certification that addresses (but is not focused on) IT & Business Continuity.

Define Business Continuity Management System (BCMS) Scope

Logically define the scope of the BCMS to be consistent with initial objectives, efficiency, effectiveness and customer requirements. This approach optimizes likelihood of the plan's success (prevents "boil the ocean" exercises).



1-3 MONTHS TO COMPLETION

PRE-RECOVERY PLAN ANALYSIS (FOR EVERYTHING INCLUDED IN SCOPE)

Risk Assessment

Determine risk acceptance criteria	Identify criteria for performing risk assessments	Ensure repeatable, consistent, valid and comparable results	Identify risk owners
Assess potential consequences that would result if the identified risks were to materialize	Assess the likelihood of occurrence and determine risk levels	Determine the most effective, cost efficient and executable risk treatments	Prioritize the analyzed risks for treatment

Risk Treatment

Implement the risk treatment plan as determined through the risk assessment

Ensure retention of the risk treatment results

Business Impact Analysis

Assess the impacts over time of not performing services/providing products and assessing acceptable minimum operational levels

Setting prioritized timeframes for resuming activities at specified minimum acceptable levels, taking into consideration the time within which the impacts of not resuming them would become unacceptable

Identifying dependencies and supporting resources, including suppliers, outsource partners, single points of failure and other relevant interested parties

Recovery Strategies

Based on outputs from the Risk Assessment and the BIA

Strategies for the 5 possible impacts of any disaster

Ensure protection of prioritized activities and availability of essential resources, critical vendors and critical skill sets

Ensure stabilizing, continuing and resuming activities along with dependencies and supporting resources



Recovery Plan Development

Easy to execute procedures

Effective recovery organization

Ensure prioritized recovery

Implementing approved strategies that fulfill requirements from the BIA

Ensure client concerns are addressed

Consistency between team plans



1-12 MONTHS TO COMPLETION

INTEGRATION BRING PLAN INTO BUSINESS OPERATIONS

Exercise the BCMS

Develop and conduct exercises of the BCMS:

Table top

Fail over / Parallel processing

Disaster Simulation

Monitor the Environment

Tune the BCMS to facilitate monitoring. (The ongoing monitoring of the BCMS is integral to ISO 22301.)

Develop Continuous Improvement Principles

ISO 22301 mandates continuous improvement plans be developed prior to certification



ONGOING

CERTIFICATION + TRAINING + MAINTENANCE - ENSURE THE PLAN CONTINUES TO WORK

Internal BCMS Audit (Pre-Certification)

"Friendly" pre-audit structured in accordance with certification audit. (Tabletop Review then Compliance Review)

Certification Audit 22301

Certification Audit conducted by Certification Body resulting in issuance of ISO 22301 Certificate. HOORAY!

Enact Continuous Improvement Principles

Based on monitoring and testing, evolve the BCMS in a demonstrable manner. (ISO 22301 mandates continuous improvement.)

Surveillance Audit (Year 2 & 3)

Mini-audit conducted by the Certification Body to validate BCMS effectiveness. (BCMS scope extension possible)

Triennial Audit (Year 3 & Every 3rd year)

Re-Certification Audit conducted by Certification Body.