

IT SERVICE CONTINUITY MANAGEMENT

PURPOSE

To support the overall business continuity management (BCM) process by ensuring that, by managing the risks that could seriously affect IT services, the IT service provider can always provide minimum agreed business continuity-related service levels.

In support of and alignment with the BCM process, ITSCM uses formal risk assessment and management techniques to:

- (Prevention) Reduce risks to IT services to agreed acceptable levels
- (Recovery) Plan and prepare for the recovery of IT services.

TRIGGERS


- New or changed business needs, or new or changed services
- New or changed targets within agreements (SLRs, SLAs, OLAs, contracts..)
- The occurrence of a major incident that requires assessment for potential invocation of either business or IT continuity plans
- Periodic activities such as the BIA or risk assessment activities, maintenance of continuity plans or other reviewing, revising or reporting activities
- Assessment of changes and attendance at CAB meetings
- Review and revision of business and IT plans and strategies
- Review and revision of designs and strategies
- Recognition or notification of a change of risk or impact of a business process or VBF, an IT service or component
- Initiation of tests of continuity and recovery plans
- Lessons learned from previous continuity events

INPUTS

- Business information: Business strategy, plans and financial plans, and information on their current and future requirements,
- IT information: from the IT strategy and plans and current budgets,
- A Business Continuity Strategy and a set of Business Continuity Plans
- Service Information: SLAs and SLRs
- Financial information
- Change information
- CMS
- Testing schedule (BCM and Availability Management)
- Capacity management information identifying the resources required to run the critical services in the event of a continuity event
- IT service continuity plans and test reports from supplier and partners, where appropriate.

IT Service Continuity Management

- Initiation (policy, scope, project initiation)
- Requirements and strategy (BIA, risk assessment, continuity strategy)
- Implementation (planning, implementation, initial testing)
- Ongoing operation (education, awareness, training, change management)
- (Invocation)

- 
- Business impact analysis
 - Risk analysis
 - Risk reduction measures
 - Service continuity plans

OUTPUTS

- A revised ITSCM policy and strategy
- A set of ITSCM plans, including all crisis management plans, emergency response plans and disaster recovery plans, together with a set of supporting plans and contracts with recovery service providers
- BIA exercises and reports
- Risk assessment and management reviews and reports
- ITSCM testing schedule
- ITSCM test scenarios
- ITSCM test reports and reviews