IT SERVICE CONTINUITY PROCESS

Version:

Owner:

Date:

DOCUMENT CHANGE HISTORY

Version	Date	Editor	Description of Change
0.1		Rhys Williams	Initial outline document

CONTRIBUTORS

Name	Role	Author / Review / Approve

TABLE OF CONTENTS

1 PROCESS OVERVIEW 4

1.1 Description 4
1.2 Objectives 4
1.3 Critical Success Factors 4

2 PROCESS FLOWCHART 5

3 PROCESS DESCRIPTION 7

4 ROLES AND RESPONSIBILITIES 17

5 SUPPORTING DOCUMENTS 20

6 GLOSSARY 21

1 PROCESS OVERVIEW

1.1 Description

IT Service Continuity Management (ITSCM) supports the overall Business Continuity Management process by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, technical support and service desk) can be resumed within required and agreed business timescales. A disaster may be as a result of an IT service being unavailable or may result from a business-impacting issue such as a building evacuation. In either scenario, ITSCM aims to support the business in maintaining its business processes / services while the underlying cause of the disaster is addressed.

ITSCM supports the Organisation's Business Continuity Management process and ensures that the recovery arrangements for designated services and components are aligned to identified and agreed business impacts, risks and needs.

ITSCM manages the risks that could seriously impact the performance and availability of IT services. Through testing, ITSCM ensures that the IT services can be resumed in accordance with the ITSC plan and relevant service levels.

The key stages in ITSCM are:

1. Requirements and Strategy
2. Implementation
3. On-going Operation
4. Invocation

1.2 Objectives

The key objectives of ITSCM are to:

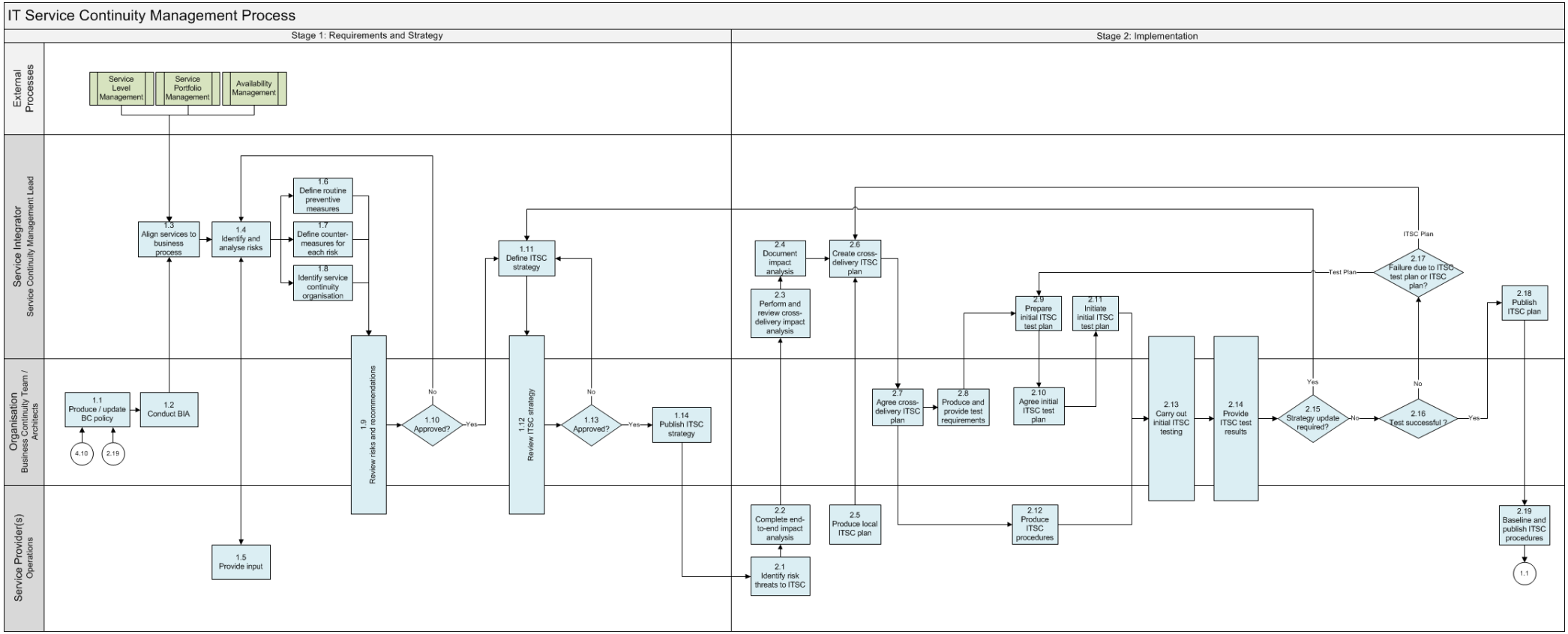
- Produce and maintain a set of IT Service Continuity (ITSC) plans that supports the overall business continuity plans of the Organisation.
- Ensure that all ITSC plans are maintained in-line with changing business impacts and requirements.
- Conduct regular risk assessments and management exercises to manage IT services within an agreed level of business risk.
- Provide advice and guidance to all other areas of the business and IT on all ITSCM-related issues.
- Ensure that appropriate continuity mechanisms are put in place to meet or exceed the agreed business continuity targets.
- Assess the impact of all changes on the IT service continuity plans and supporting methods and procedures.

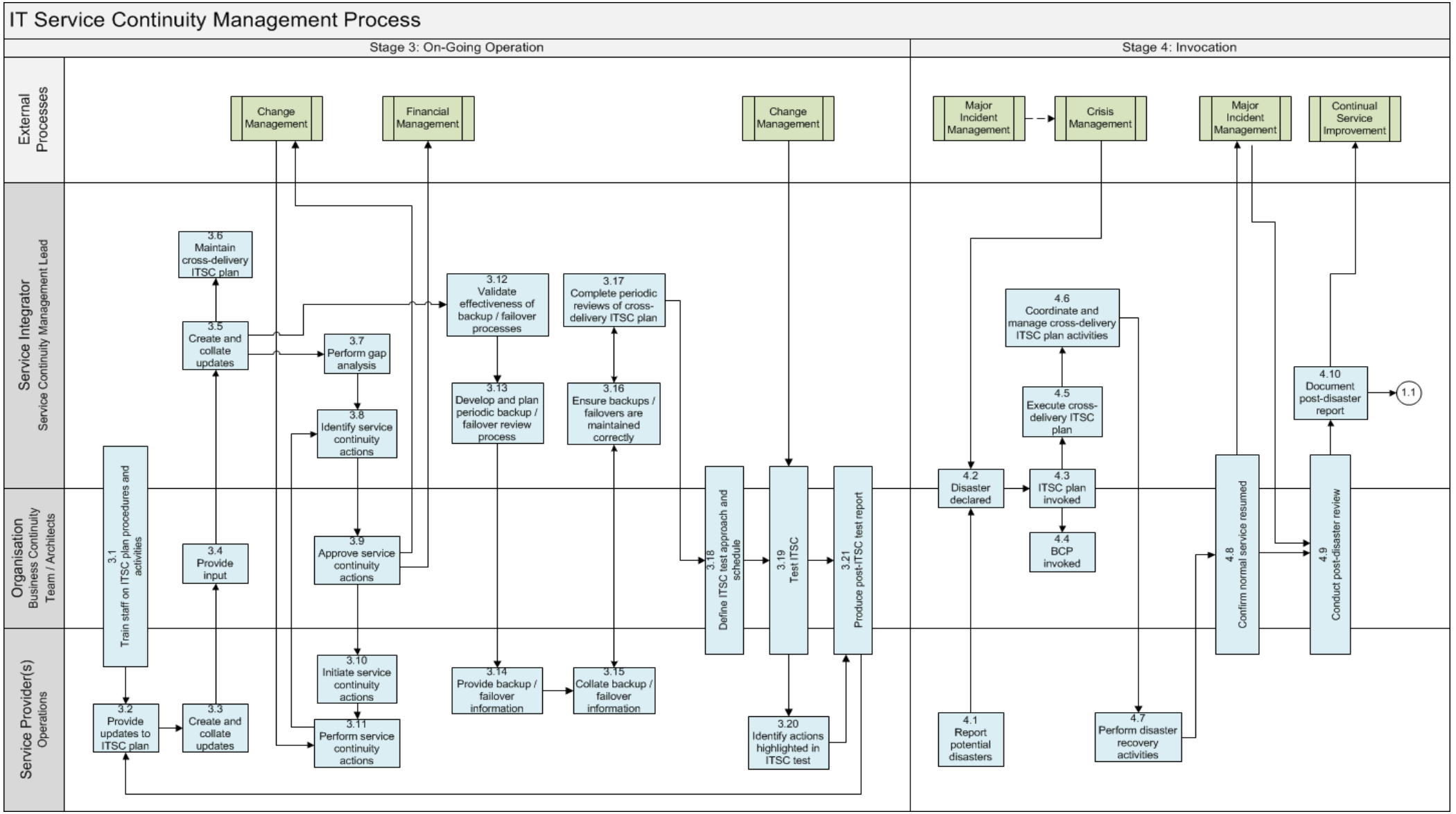
1.3 Critical Success Factors

The critical success factors for ITSCM are:

- ITSC plans are aligned to business continuity requirements.
- IT services can be recovered in-line with the ITSC plan(s).
- Involved parties are aware of their role in recovering services in the event of a disaster and understand how they will work with other parties to recover the services in a coordinated manner.

2 PROCESS FLOWCHART




IT Service Continuity Management Process
Stage 3: On-Going Operation
Stage 4: Invocation
External Processes
Service Integrator
Service Continuity Management Lead
Organisation
Business Continuity Team / Architects
Service Provider(s)
Operations
Change Management
Financial Management
Change Management
Major Incident Management
Crisis Management
Major Incident Management
Continual Service Improvement
3.6 Maintain cross-delivery ITSC plan
3.5 Create and collate updates
3.7 Perform gap analysis
3.8 Identify service continuity actions
3.12 Validate effectiveness of backup / failover processes
3.13 Develop and plan periodic backup / failover review process
3.17 Complete periodic reviews of cross-delivery ITSC plan
3.16 Ensure backups / failovers are maintained correctly
4.6 Coordinate and manage cross-delivery ITSC plan activities
4.5 Execute cross-delivery ITSC plan
4.10 Document post-disaster report
1.1
3.1 Train staff on ITSC plan procedures and activities
3.4 Provide input
3.9 Approve service continuity actions
3.18 Define ITSC test approach and schedule
3.19 Test ITSC
3.21 Produce post-ITSC test report
4.2 Disaster declared
4.3 ITSC plan invoked
4.4 BCP invoked
4.8 Confirm normal service resumed
4.9 Conduct post-disaster review
3.10 Initiate service continuity actions
3.11 Perform service continuity actions
3.14 Provide backup / failover information
3.15 Collate backup / failover information
3.2 Provide updates to ITSC plan
3.3 Create and collate updates
3.20 Identify actions highlighted in ITSC test
4.1 Report potential disasters
4.7 Perform disaster recovery activities

3 PROCESS DESCRIPTION

No.	Activity	Description	Inputs	Outputs	Responsible
Stage 1: Requirements and Strategy					
1.1	Produce / update BC policy	The Organisation's BC Manager is responsible for producing the BC Policy. Inputs will be taken from all areas of the Organisation and updates will be applied periodically to reflect changes in the Organisation structure and on an ad hoc basis, based on lessons learned from BC testing and any post-disaster reviews (see activity 4.9).	• Requirement to produce / update BC policy • Existing BC Policy (S1) • Post-Disaster Report (S29)	• BC Policy (S1)	• Organisation (BC Manager)
1.2	Conduct BIA	The Organisation conducts a Business Impact Analysis (BIA) to determine the impact to the business that the loss of service would have. The purpose of analysing business impact is to assess the risk by identifying: • Critical services • Potential damage or loss that may be caused to the organisation's brand as a result of a disruption to a service This analysis determines what recovery facilities should be provided and will ensure that service continuity management resources are allocated in the most appropriate way. Specifically, the business impact analysis identifies impacts resulting from an inability to use services. The impact analysis concentrates on scenarios where the impact on critical business processes is likely to be greatest. It will include: • 'Hard' impacts - failure to meet statutory reporting requirements, financial loss, breach of law, failure to achieve agreed service levels, increased costs of working • 'Soft' impacts - damage to reputation, political, corporate or personal embarrassment, loss of competitive advantage Consideration is also given to how the degree of damage or loss is likely to escalate after a service disruption. This enables identification of the minimum critical requirements for the continued operation of the service and the timescale within which such requirements should be provided. These requirements include: • Staffing, skills and services (including the applications and data recovery requirements) necessary to enable the service to continue operating at a minimum acceptable level • Time within which minimum levels of staffing and services should be recovered • Time within which the service should be fully recovered	• BC Policy (S1)	• Business Impact Assessment (S4)	• Organisation (BC Manager)

No.	Activity	Description	Inputs	Outputs	Responsible
		The business impact analysis should also consider any implications associated with loss of integrity of information and loss of data.			
1.3	Align services to business process	The business service priorities are determined by the SI Service Continuity Management Lead based on the findings of the BIA. This will identify the IT services that underpin the business service priority list.	• Business Impact Assessment (S4) • Service Portfolio Management Process (S2) • Service Level Management Process (S3) • Availability Management Process (S5)	• IT services aligned to business process	• SI Service Continuity Management Lead
1.4	Identify and analyse risks	The SI Service Continuity Management Lead conducts a risk assessment of the business services to identify the potential level of threat to the service and the extent to which it is vulnerable. These are key factors in determining service continuity management requirements. Activities covered by an assessment include: • Identification of risks • Appraisal of the failure of service providers or 3rd parties • Appraisal of the impact of single points of failure within the IT environment (e.g. unavailability of key staff). A risk assessment details threat and vulnerability levels where: • Threat is defined as "how likely is it that a business disruption will occur?" • Vulnerability is defined as "whether, and to what extent, the organisation will be affected if a threat materialises"	• Business Impact Assessment (S4) • IT services aligned to business process • Risk Register (S6)	• Risk Register (S6)	• SI Service Continuity Management Lead
1.5	Provide input	The Service Providers provide input and support to the SI Service Continuity Management Lead in the risk analysis and definition of any recommendations (which may include technical operating processes and support levels required) and disaster definition(s).	• Request for input	• Input	• Service Provider(s)
1.6	Define routine preventive measures	For each risk defined in activity 1.4, the SI Service Continuity Management Lead defines an action (or list of actions) that must be performed routinely to prevent or reduce the risk, or to allow recovery if it happens. These are known as routine preventive measures. The preventive measures need to be integrated with routine operational processes and procedures and are normally documented as specific risk preventive procedures and policies.	• Risk Register (S6)	• Risk Preventive Procedures and Policies (S7) • Routine Preventive Measures (S8)	• SI Service Continuity Management Lead

No.	Activity	Description	Inputs	Outputs	Responsible
1.7	Define counter-measures for each risk	As a result of the risk assessment, the SI Service Continuity Management Lead defines counter-measures that must be put in place for each individual risk. The counter-measures are a list of one or more actions which have to be carried out to recover from the risk if it occurs.	• Risk Register (S6)	• Counter-Measures (S9)	• SI Service Continuity Management Lead
1.8	Identify service continuity organisation	The SI Service Continuity Management Lead draws up a list of all personnel who have key roles within service continuity (i.e. who will be required to assist in the event of a service failure) or who need to be kept informed. These are recorded in an organisation chart in the service continuity organisation document, which forms part of the recovery plans and procedures. The SI Service Continuity Management Lead also establishes and keeps up-to-date contact details for all relevant personnel. These are recorded in the contact details section of the service continuity organisation document.	• Risk Register (S6)	• Service Continuity Organisation Document (S10)	• SI Service Continuity Management Lead
1.9	Review Risks and Recommendations	All parties involved in this process review the risks and recommendations produced in activities 1.6 to 1.8.	• Risk Register (S6) • Risk Preventive Procedures and Policies (S7) • Routine Preventive Measures (S8) • Counter-Measures (S9) • SC Organisation Document (S10)	• Risks and Recommendations (S31) - approved / rejected	• All
1.10	Approved?	If the risks and recommendations are approved, go to activity 1.11. If not, go back to activity 1.4	n/a	n/a	n/a
1.11	Define service continuity strategy	The service continuity strategy is developed by the SI Service Continuity Management Lead using information collated from the business impact analysis and the risk assessment. The strategy is presented as a series of options for the owners of the services to consider. These options should reflect a balance between risk reduction and recovery. The strategy should reflect the service continuity actions required for the 'as-is' service but should also take into consideration any known future changes / improvements ('to-be' service). Defining the options within the strategy is the most important stage of the process. If the requirements gathering is flawed the strategy will be flawed and will not fully support service recovery. Options may range from a low-cost strategy (such as do nothing if the impacts are minimal or if the service owner is prepared to accept	• Business Impact Assessment (S4) • Risk Register (S6) • Risks and Recommendations (S31) - approved	• IT Service Continuity Strategy (S11) - draft	• SI Service Continuity Management Lead

No.	Activity	Description	Inputs	Outputs	Responsible
		the risk) to full continuity provision, with obvious cost implications. The latter may be justifiable if impact is high and/or risks are great. It may be necessary to consider different options for short-term and long-term recovery and all costs and benefits of each option need to be understood before a decision is made. Typically, a strategy will fall somewhere between the two and will be a balance of risk reduction and recovery.			
1.12	Review ITSC strategy	All parties involved in this process review the ITSC strategy, ensuring that it meets business requirements. If services are provided by a number of service providers, each of these will be contacted by the SI Service Continuity Management Lead and will be expected to agree with our service continuity strategy. This may result in the need to update the service providers' SLAs. The service providers are also expected to provide proof that they have implemented and tested their own business continuity processes.	• IT Service Continuity Strategy (S11) - draft	• IT Service Continuity Strategy (S11) - approved / rejected	• All
1.13	Approved?	If the ITSC strategy is approved, go to activity 1.14. If not, go back to activity 1.11	n/a	n/a	n/a
1.14	Publish ITSC strategy	The SI Service Continuity Management Lead publishes the ITSC strategy and identified internal and external people are informed about: • Their role and responsibility in the service continuity process • People to contact in the event of a major incident and how to contact them • The service continuity strategy • Implemented risk reduction measures	• IT Service Continuity Strategy (S11) - approved • Service Continuity Organisation Document (S10) • Risk reduction measures	• IT Service Continuity Strategy (S11) - published	• SI Service Continuity Management Lead
Stage 2: Implementation					
2.1	Identify risk threats to IT service continuity	The Service Provider(s) should identify and highlight risk threats to ITSC.	• IT Service Continuity Strategy (S11) - published	• Risk Threats identified	• Service Provider(s) - Operations
2.2	Complete end-to-end impact analysis	Threats identified by the Service Provider(s) are collated, reviewed and the end-to-end impact analysis is performed.	• Risk Threats identified	• Impact analysis of threats	• Service Provider(s) - Operations
2.3	Perform and review cross-delivery impact analysis	Threats identified by the Service Provider are collated, reviewed and the cross-delivery impact analysis is performed by the SI Service Continuity Management Lead to garner a view of all risks to service continuity.	• Impact analysis of threats	• Cross-Delivery Impact Analysis (S12) - draft	• SI Service Continuity Management Lead

No.	Activity	Description	Inputs	Outputs	Responsible
2.4	Document impact analysis	The full impact assessment is documented and distributed to all relevant parties by the SI Service Continuity Management Lead.	• Cross-Delivery Impact Analysis (S12) - draft	• Cross-Delivery Impact Analysis (S12) - completed	• SI Service Continuity Management Lead
2.5	Produce local ITSC plan	The Service Provider(s) produce local ITSC plans. The scope will be defined by the services that are under management by the operations.	n/a	• Local ITSC Plans (S13)	• Service Provider(s) - Operations
2.6	Create cross-delivery ITSC plan	Using the documented impact analysis and the agreed ITSC strategy and local ITSC plans, a cross-delivery ITSC plan is created by the SI Service Continuity Management Lead and sent to the Organisation representatives to approve. Once approved by the Organisation representatives, the cross-delivery ITSC plan can be tested (where possible and appropriate).	• IT Service Continuity Strategy (S11) - published • Cross-Delivery Impact Analysis (S12) - completed • Local ITSC Plans (S13) OR • Testing unsuccessful due to failure in Cross-Delivery ITSC Plan (S14)	• Cross-Delivery ITSC Plan (S14) - draft	• SI Service Continuity Management Lead
2.7	Agree cross-delivery ITSC plan	The Organisation agrees the cross-delivery ITSC plan. Note: Some re-work may be required before agreement is reached.	• Cross-Delivery ITSC Plan (S14) - draft	• Cross-Delivery ITSC Plan (S14) - approved	• Organisation (BC Manager)
2.8	Produce and provide test requirements	The Organisation's BC Manager produces a list of test requirements, taking input from the relevant test resources and Enterprise Architects. The test requirements are provided to the SI Service Continuity Management Lead.	• Cross-Delivery ITSC Plan (S14) - approved	• Test Requirements (S15)	• Organisation (BC Manager)
2.9	Prepare initial ITSC test plan	The SI Service Continuity Management Lead prepares an initial ITSC test plan to test the cross-delivery ITSC plan in full - or the various component ITSC plans, including success criteria.	• Cross-Delivery ITSC Plan (S14) - approved • Test Requirements (S15) OR • Testing unsuccessful due to failure in ITSC Test Plan (S16)	• ITSC Test Plan (S16) - draft	• SI Service Continuity Management Lead
2.10	Agree initial ITSC test plan	The Organisation agrees the initial ITSC test plan. Note: Some re-work may be required before agreement is reached.	• ITSC Test Plan (S16) - draft	• ITSC Test Plan (S16) - approved	• Organisation (BC Manager)
2.11	Initiate initial ITSC test plan	The SI Service Continuity Management Lead initiates the testing of the ITSC plan(s).	• ITSC Test Plan (S16) - approved	• ITSC Test Plan (S16) - initiated	• SI Service Continuity Management Lead
2.12	Produce ITSC procedures	Based on the published ITSC plan, the Service Provider(s) produces the various ITSC procedures.	• Cross-Delivery ITSC Plan (S14) - approved	• ITSC Procedures (S17)	• Service Provider(s) - Operations

No.	Activity	Description	Inputs	Outputs	Responsible
2.13	Carry out initial ITSC testing	All relevant parties involved in this process perform the initial testing according to the plan.	• ITSC Test Plan (S16) - initiated • ITSC Procedures (S17)	• Initial ITSC testing performed	• All
2.14	Provide ITSC test results	All relevant parties involved in this process provide the various ITSC test results.	• Initial ITSC testing performed	• ITSC Test Results (S18)	• All
2.15	Strategy update required?	The Organisation determines whether an update to the ITSC strategy is required as a consequence of the test results.	• ITSC Test Results (S18)	• IT Service Continuity Strategy (S11) - update required / not required	• Organisation (EAs)
2.16	Test successful?	All relevant parties involved in this process determine whether the tests were successful against the success criteria.	• Initial ITSC testing performed • ITSC Test Results (S18)	• Test successful / unsuccessful	• All
2.17	Failure due to ITSC test plan or ITSC plan?	If the testing was not successful, the SI Service Continuity Management Lead determines whether it was due to a failure in the ITSC plan, which defines the activities to be undertaken in the event of a disaster or the test plan, which defines the mechanisms that are used to test ITSC plan.	• Test unsuccessful	• Testing unsuccessful due to failure in Cross-Delivery ITSC Plan (S14) OR • Testing unsuccessful due to failure in ITSC Test Plan (S16)	• SI Service Continuity Management Lead
2.18	Publish ITSC plan	If the test was successful, the SI Service Continuity Management Lead issues the ITSC plan.	• Test successful • Cross-Delivery ITSC Plan (S14) - approved	• Cross-Delivery ITSC Plan (S14) - published	• SI Service Continuity Management Lead
2.19	Baseline and publish ITSC procedures	The Service Provider(s) performs any required updates to the ITSC procedures, baselines and publishes the procedures.	• Cross-Delivery ITSC Plan (S14) - published • ITSC Procedures (S17)	• ITSC Procedures (S17) - published	• Service Provider(s) - Operations
Stage 3: On-Going Operation					
3.1	Train staff on ITSC plan procedures and activities	All staff should be trained on the appropriate ITSC plan and their actions and responsibilities during a disaster. The ITSC plan should be held in several locations and formats to ensure it is available in all situations to all relevant parties.	• Local ITSC Plans (S13) • ITSC Procedures (S17)	• Staff trained	• All
3.2	Provide updates to ITSC plan	Following the ITSC plan tests, updates should be made by the Service Provider(s) to the local ITSC plans as to the actions completed and timelines of recovery to ensure accuracy.	• Local ITSC Plans (S13) • ITSC Procedures (S17) • Post-ITSC Test Report (S24)	• Local ITSC Plans (S13) - updated	• Service Provider(s) - Operations
3.3	Create and collate updates	The updates following the ITSC plan tests should be collated to provide updates to the ITSC plan held by the Service Provider, covering all services under their management.	• Local ITSC Plans (S13) - updated	• Local ITSC Plans (S13) - collated	• Service Provider(s) - Operations

No.	Activity	Description	Inputs	Outputs	Responsible
3.4	Provide input	The Organisation's BC manager will review the collated local ITSC plans and provide any relevant input to the SI Service Continuity Management Lead.	• Local ITSC Plans (S13) - collated	• Input provided to SI Service Continuity Management Lead	• Organisation (BC Manager)
3.5	Create and collate updates	Updates to the local ITSC plans are collated by the SI Service Continuity Management Lead and used to update the overarching cross-delivery ITSC plan.	• Local ITSC Plans (S13) - collated • Cross-Delivery ITSC Plan (S14)	• Cross-Delivery ITSC Plan (S14) - updated	• SI Service Continuity Management Lead
3.6	Maintain cross delivery ITSC plan	The cross-delivery ITSC plan should be updated regularly by the SI Service Continuity Management Lead; this will include updates from other service management processes and the results from the ITSC tests.	• Cross-Delivery ITSC Plan (S14) • ITSC Test Results (S18) • Relevant Service Management Processes	• Cross-Delivery ITSC Plan (S14) - maintained	• SI Service Continuity Management Lead
3.7	Perform gap analysis	The SI Service Continuity Management Lead performs a gap analysis, which identifies areas of weakness in Service Continuity between the delivered services and the continuity requirements.	• Cross-Delivery ITSC Plan (S14) • Delivered Services	• Gap Analysis Results (S19)	• SI Service Continuity Management Lead
3.8	Identify service continuity actions	Actions required to mitigate the weaknesses identified in the gap analysis are determined by the SI Service Continuity Management Lead.	• Gap Analysis Results (S19)	• Service Continuity Actions (S20) - identified	• SI Service Continuity Management Lead
3.9	Approve service continuity actions	The Organisation approves the actions required to mitigate the identified service continuity weaknesses. These actions will then need to be escalated to the Change Management and Financial Management processes as required.	• Service Continuity Actions (S20) - identified	• Service Continuity Actions (S20) - approved • Change Management Process (S21) • Financial Management Process (S22)	• Organisation (BC Manager)
3.10	Initiate service continuity actions	The actions approved by Change Management / Financial Management are passed to the relevant Service Provider(s) for allocation to the appropriate resource.	• Service Continuity Actions (S20) - approved	• Service Continuity Actions (S20) - initiated	• Service Provider(s) - Operations
3.11	Perform service continuity actions	The actions that have been assigned are completed by the Service Provider(s) as per the detailed instructions in the RFC.	• Service Continuity Actions (S20) - initiated • Change Management Process (S21)	• Service Continuity Actions (S20) - performed	• Service Provider(s) - Operations
3.12	Validate effectiveness of backup / failover processes	The effectiveness of the backup / failover processes is validated by the SI Service Continuity Management Lead to ensure backups / failovers are being completed and maintained in a suitable manner.	• Cross-Delivery ITSC Plan (S14) - updated	• Effectiveness of backup / failover processes validated	• SI Service Continuity Management Lead
3.13	Develop and plan periodic backup / failover review process	The backup / failover processes are reviewed and tested at regular intervals by the SI Service Continuity Management Lead. A plan should be devised that will ensure the backups / failovers are being maintained in the agreed way.	• Effectiveness of Backup / Failover Processes - validated	• Effectiveness of Backup / Failover Processes - reviewed	• SI Service Continuity Management Lead

No.	Activity	Description	Inputs	Outputs	Responsible
3.14	Provide backup / failover information	A report of backups / failovers is created by the Service Provider(s) to provide evidence of the effectiveness of the backup / failover processes.	• Effectiveness of Backup / Failover Processes - reviewed	• Report of Backups / Failovers	• Service Provider(s) - Operations
3.15	Collate backup / failover information	The reports of backups / failovers are collated by the Service Provider(s) to confirm the end-to-end service backup / failover effectiveness.	• Report of Backups / Failovers	• Report of Backups / Failovers - collated	• Service Provider(s) - Operations
3.16	Ensure backups / failovers are maintained correctly	The SI Service Continuity Management Lead ensures that backups / failovers are maintained correctly and as agreed in the backup / failover processes.	• Report of Backups / Failovers - collated	• Backups / Failovers maintained correctly	• SI Service Continuity Management Lead
3.17	Complete periodic reviews of the cross-delivery ITSC plan	The cross-delivery ITSC plan(s) is reviewed at scheduled intervals by the SI Service Continuity Management Lead; this is to ensure that the data, contacts, processes, policies and actions still meet the requirements and any changes to the BCP.	• Cross-Delivery ITSC Plan (S14)	• Cross-Delivery ITSC Plan (S14) - periodically reviewed and updated	• SI Service Continuity Management Lead
3.18	Define ITSC test approach and schedule	All relevant parties are involved with the joint creation of test objectives, scenarios and data sets. A schedule to test the cross-delivery ITSC plan(s) should be designed and implemented. During testing of the ITSC plan(s), all services should remain in operation wherever possible. Where services are unavailable, downtime is agreed with the business via Change Management and appropriate communication / notification is sent to the users. These services should not be affected during critical time periods.	• Cross-Delivery ITSC Plan (S14) - periodically reviewed and updated	• ITSC Test Schedule (S23) • ITSC Test Plan (S16)	• All
3.19	Test ITSC	The ITSC plan is tested by all relevant parties as per the test schedule and as approved by Change Management. Prior to the initiation of the ITSC plan tests, all users should be informed and any possible impacts should be detailed.	• ITSC Test Schedule (S23) • ITSC Test Plan (S16) • Cross-Delivery ITSC Plan (S14) • Change Management Process (S21)	• Cross-Delivery ITSC Plan (S14) - tested • ITSC Test Results (S18)	• All
3.20	Identify actions highlighted in ITSC test	Following the ITSC test, the Service Provider(s) identifies any actions that need to be completed.	• Cross-Delivery ITSC Plan (S14) - tested • ITSC Test Results (S18)	• Actions to be completed	• Service Provider(s) - Operations
3.21	Produce post-ITSC test report	When the ITSC tests have been completed, a report is produced, by all relevant parties, that details the activities that where completed, any lessons learned and recommendations for improvement to the ITSC plan(s). This includes all working instructions and processes.	• Cross-Delivery ITSC Plan (S14) - tested • ITSC Test Results (S18) • Actions to be completed	• Post-ITSC Test Report (S24)	• All

No.	Activity	Description	Inputs	Outputs	Responsible
Stage 4: Invocation					
4.1	Report potential disasters	Any potential disaster situations should be reported at the earliest opportunity. This includes any situations that may result in a disaster being declared.	• Potential disaster situations	• Potential disaster situations reported	• Service Provider(s) - Operations
4.2	Disaster declared	Using the agreed and published disaster definition, included in the ITSC strategy, a disaster will be declared when a service impact, that reduces the level of operation below the required threshold, occurs. The declaration of a disaster is defined in the Crisis Management Process.	• Disaster occurs • Crisis Management Process (S25) • ITSC Strategy (S11)	• Disaster declared	• Organisation (BC Manager) • SI Service Continuity Management Lead
4.3	ITSC plan invoked	When a disaster is declared, the relevant parts of the ITSC plan will be invoked by the BC Manager and SI Service Continuity Management Lead.	• Disaster declared • Cross-Delivery ITSC Plan (S14)	• Cross-Delivery ITSC Plan (S14) - invoked	• Organisation (BC Manager) • SI Service Continuity Management Lead
4.4	BCP invoked	Dependent on the disaster that is declared, the BCP may also be invoked. The Organisation instigates the BCP as a separate activity from the invocation of the ITSC plan. In some cases, they may be instigated in isolation.	• Disaster declared • Business Continuity Plan (S26)	• Business Continuity Plan (S26) - invoked	• Organisation (BC Manager)
4.5	Execute cross-delivery ITSC plan	The actions detailed in the cross-delivery ITSC plan will be delegated to the appropriate Service Provider by the SI Service Continuity Management Lead, so they can coordinate with the relevant resources to restore the service in an efficient and controlled manner. The SI Service Continuity Management Lead will retain overall management responsibility.	• Disaster declared • Cross-Delivery ITSC Plan (S14)	• Cross-Delivery ITSC Plan (S14) - delegated to the appropriate Service Provider(s)	• SI Service Continuity Management Lead
4.6	Coordinate and manage cross-delivery ITSC plan activities	The SI Service Continuity Management Lead coordinates and manages the activities performed by the Service Provider during the disaster and receives regular progress updates.	• Cross-Delivery ITSC Plan (S14) - delegated to the appropriate Service Provider(s)	• Coordination and management of Cross-Delivery ITSC Plan activities	• SI Service Continuity Management Lead
4.7	Perform disaster recovery activities	The relevant Service Providers, and any necessary 3rd parties, will perform the disaster recovery activities as detailed in the cross-delivery ITSC plan.	• Cross-Delivery ITSC Plan (S14) - delegated to the appropriate Service Provider(s)	• Disaster recovery activities performed	• Service Provider(s) - Operations

No.	Activity	Description	Inputs	Outputs	Responsible
4.8	Confirm normal service resumed	All parties involved in the execution of disaster recovery activities will confirm when services have resumed to normal / agreed operations. This will be managed through the Major Incident Management process.	• Disaster recovery activities performed	• Confirmation that normal service has been resumed • Major Incident Management Process (S27)	• All
4.9	Conduct post-disaster review	All involved and relevant parties will be required to attend a post-disaster review. This meeting will discuss the origin of the disaster, the activities completed to rectify the issues, lessons learned, remedial actions that are required to return to normal operation and the preventive measures that can be introduced. Input is received from Major Incident Management in the form of the incident report, which includes timelines, resources involved and actions taken.	• Confirmation that normal service has been resumed • Incident Report (S28) • Major Incident Management Process (S27)	• Post-Disaster Review conducted	• All
4.10	Document post-disaster report	The SI Service Continuity Management Lead produces the post-disaster review. This includes details of the timeline actions, activities completed and inputs from incident reports. Lessons learned and opportunities for improvement will be identified and fed into the CSI process. These could lead to changes to services, the ITSC strategy, ITSC plan, ITSC test plan or schedule.	• Post-Disaster Review conducted	• Post-Disaster Report (S29) • Continual Service Improvement Process (S30)	• SI Service Continuity Management Lead • Service Provider(s) - Operations

4 ROLES AND RESPONSIBILITIES

	Activity	**Service Integrator** Service Continuity Management Lead	**Organisation** BC Manager	**Organisation** Enterprise Architects	**Service Provider(s)** Operations
	Stage 1: Requirements and Strategy				
1.1	Produce / update BC policy	C / I	R / A	C / I	C / I
1.2	Conduct BIA	C	R / A	C	
1.3	Provide input	R / A	I		
1.4	Conduct risk assessment	C	R / A	C	
1.5	Issue business service priorities	I	R / A	I	I
1.6	Issue threat assessment	I	R / A	I	I
1.7	Align services to business process	R / A	I		C
1.8	Define business continuity requirements	I	R / A	C	I
1.9	Define disaster definition	C / I	R / A	C	I
1.10	Provide input	I	I		R / A
1.11	Define ITSC strategy	C	C	R / A	C
1.12	Agree ITSC strategy	C	C	R / A	C
1.13	Publish ITSC strategy	C	C	R / A	C
	Stage 2: Implementation				
2.1	Identify risk threats to IT service continuity	C / I	I		R / A
2.2	Complete end-to-end impact analysis	C / I	I		R / A
2.3	Perform and review cross-delivery impact analysis	R / A	I	I	I
2.4	Document impact analysis	R / A	I	I	I
2.5	Produce local ITSC plan	I	I		R / A
2.6	Create cross-delivery ITSC plan	R / A	I		I
2.7	Agree cross-delivery ITSC plan	I	R / A		
2.8	Produce and provide test requirements	I	R / A		I
2.9	Prepare initial ITSC test plan	R / A	I		I
2.10	Agree initial ITSC test plan	I	R / A		I

Activity		**Service Integrator** Service Continuity Management Lead	**Organisation** BC Manager	**Organisation** Enterprise Architects	**Service Provider(s)** Operations
2.11	Initiate initial ITSC test plan	R / A	I		I
2.12	Produce ITSC procedures	I	I		R / A
2.13	Carry out initial ITSC testing	R	R / A		R
2.14	Provide ITSC test results	R	R / A	I	R
2.15	Strategy update required?	C	C	R / A	C
2.16	Test successful?	R	R / A	I	R
2.17	Failure due to ITSC test plan or ITSC plan?	R / A	C		C
2.18	Publish ITSC plan	R / A			
2.19	Baseline and publish ITSC procedures	I	I	I	R / A
	Stage 3: On-Going Operation				
3.1	Train staff on ITSC plan procedures and activities	R	R / A		R
3.2	Provide updates to ITSC plan	I	I		R / A
3.3	Create and collate updates	I	I		R / A
3.4	Provide input	I	R / A		
3.5	Create and collate updates	R / A			
3.6	Maintain cross delivery ITSC plan	R / A	C		C
3.7	Perform gap analysis	R / A	I		C
3.8	Identify service continuity actions	R / A	I		C
3.9	Approve service continuity actions	I	R / A		I
3.10	Initiate service continuity actions	I			R / A
3.11	Perform service continuity actions	I			R / A
3.12	Validate effectiveness of backup / failover processes	R / A	C		C
3.13	Develop and plan periodic backup / failover review process	R / A	C		C
3.14	Provide backup / failover information	I	I		R / A
3.15	Collate backup / failover information	I	I		R / A
3.16	Ensure backups / failovers are maintained correctly	R / A	I		C

Activity		**Service Integrator** Service Continuity Management Lead	**Organisation** BC Manager	**Organisation** Enterprise Architects	**Service Provider(s)** Operations
3.17	Complete periodic reviews of the cross-delivery ITSC plan	R / A	C		C
3.18	Define ITSC test approach and schedule	R / A	R		R
3.19	Test ITSC	R / A	R		R
3.20	Identify actions highlighted in ITSC test	I	I		R / A
3.21	Produce post-ITSC test report	R / A	R	I	R
	Stage 4: Invocation				
4.1	Report potential disasters	I	I		R / A
4.2	Disaster declared	R	R / A	I	I
4.3	ITSC plan invoked	R / A	R		I
4.4	BCP invoked	I	R / A		I
4.5	Execute cross-delivery ITSC plan	R / A	I		I
4.6	Coordinate and manage cross-delivery ITSC plan activities	R / A	I		I
4.7	Perform disaster recovery activities	C / I	I		R / A
4.8	Confirm normal service resumed	R	R / A		R
4.9	Conduct post-disaster review	R	R / A	C	R
4.10	Document post-disaster report	R / A	I	I	I

Key to RACI Chart:

Responsible **(R)** : The person / group who has to perform the task
Accountable **(A)** : The person / group who is accountable for the deliverables of the task
Consulted **(C)** : Persons who must always be consulted before a decision / action is taken
Informed **(I)** : Persons who must always be informed after a decision / action is taken

5 SUPPORTING DOCUMENTS

No.	Document Name	Owner	Location
S1	BC Policy	Business Continuity Manager	Service Knowledge Management System
S2	Service Portfolio Management Process	SI Service Portfolio Management Lead	Service Knowledge Management System
S3	Service Level Management Process	SI Service Manager	Service Knowledge Management System
S4	Business Impact Assessment	Business Continuity Manager	Service Knowledge Management System
S5	Availability Management Process	SI Availability Management Lead	Service Knowledge Management System
S6	Risk Register	SI Service Continuity Management Lead	Service Knowledge Management System
S7	Risk Preventive Procedures and Policies	SI Service Continuity Management Lead	Service Knowledge Management System
S8	Routine Preventive Measures	SI Service Continuity Management Lead	Service Knowledge Management System
S9	Counter-Measures	SI Service Continuity Management Lead	Service Knowledge Management System
S10	SC Organisation Document	SI Service Continuity Management Lead	Service Knowledge Management System
S11	IT Service Continuity Strategy	SI Service Continuity Management Lead	Service Knowledge Management System
S12	Cross-Delivery Impact Analysis	SI Service Continuity Management Lead	Service Knowledge Management System
S13	Local ITSC Plans	SI Service Continuity Management Lead	Service Knowledge Management System
S14	Cross-Delivery ITSC Plan	SI Service Continuity Management Lead	Service Knowledge Management System
S15	Test Requirements	Business Continuity Manager	Service Knowledge Management System
S16	ITSC Test Plan	SI Service Continuity Management Lead	Service Knowledge Management System
S17	ITSC Procedures	SI Service Continuity Management Lead	Service Knowledge Management System
S18	ITSC Test Results	SI Service Continuity Management Lead	Service Knowledge Management System
S19	Gap Analysis Results	SI Service Continuity Management Lead	Service Knowledge Management System
S20	Service Continuity Actions	SI Service Continuity Management Lead	Service Knowledge Management System
S21	Change Management Process	SI Change Management Lead	Service Knowledge Management System
S22	Financial Management Process	SI Financial Management Lead	Service Knowledge Management System
S23	ITSC Test Schedule	SI Service Continuity Management Lead	Service Knowledge Management System
S24	Post-ITSC Test Report	SI Service Continuity Management Lead	Service Knowledge Management System
S25	Crisis Management Process	Crisis Manager	Service Knowledge Management System
S26	Business Continuity Plan	Business Continuity Manager	Service Knowledge Management System
S27	Major Incident Management Process	SI Major Incident Management Lead	Service Knowledge Management System
S28	Incident Report	SI Incident Management Lead	Service Management Tool
S29	Post-Disaster Report	Business Continuity Manager	Service Knowledge Management System
S30	Continual Service Improvement Process	SI Continual Service Improvement Lead	Service Knowledge Management System
S31	Risks and Recommendations	SI Continual Service Improvement Lead	Service Knowledge Management System

6 GLOSSARY

BC	Business Continuity
BCP	Business Continuity Plan
BIA	Business Impact Analysis
Business Continuity Management	"The business process responsible for managing risks that could seriously affect the business. Business continuity management safeguards the interests of key stakeholders, reputation, brand and value-creating activities. The process involves reducing risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur. Business continuity management sets the objectives, scope and requirements for IT service continuity management." (*ITIL definition*)
Business Continuity Plan	"A plan defining the steps required to restore business processes following a disruption. The plan also identifies the triggers for invocation, people to be involved, communications, etc. IT service continuity plans form a significant part of business continuity plans." (*ITIL definition*)
CSI	Continual Service Improvement
EA	Enterprise Architect
IT Service Continuity Management	"The process responsible for managing risks that could seriously affect IT services. IT service continuity management ensures that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services. IT service continuity management supports business continuity management." (*ITIL definition*)
IT Service Continuity Plan	"A plan defining the steps required to recover one or more IT services. The plan also identifies the triggers for invocation, people to be involved, communications, etc. The IT service continuity plan should be part of a business continuity plan." (*ITIL definition*)
ITIL	IT Infrastructure Library
ITSC	IT Service Continuity
ITSCM	IT Service Continuity Management
RFC	Request for Change
SC	Service Continuity
SI	Service Integrator
SLA	Service Level Agreement