SCM (Service Continuity Management)

Service Continuity Plan Training
Cloud Infrastructure Services (CIS3/CISnext)

Oktober 2022

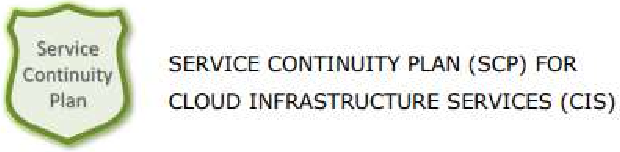
Trusted partner for your **Digital Journey**

Atos

Training objectives

Service Continuity Plan

- ▶ Understand the goal of the Atos Service Continuity Plan (SCP)
- ▶ Awareness of the SCP related documents
- ▶ Using the SCP documents as a reference during a disaster or disruption
- ▶ What to do when a disaster or disruption has occurred:
  - – Immediate actions
  - – Disaster management
  - – Recovery procedures
  - – Prevention
- ▶ The SCP document: “SCM: Service Continuity Plan”
    - describes the above-mentioned subjects.



SERVICE CONTINUITY PLAN (SCP) FOR
CLOUD INFRASTRUCTURE SERVICES (CIS)

1 SCP Introduction

Introduction

Service Continuity Plan

- The Service Continuity Plan (SCP) for service CIS was developed in Atos service line "Managed Services" (MS) in accordance with the valid process for IT Service Continuity Management (ITSCM). The framework for the development of the SCP is given by the Atos MS Business Continuity Management Policy (MSM-BCM-0110) and the approved Business Continuity Management program for Global Cloud Services.

- The SCP is a single module (a single service specific continuity plan) beside other modules in the IT Service Continuity Plan (ITSCP) which is again part of the overall Business Continuity Plan (BCP) for Atos.

- The nature of the SCP is to describe all actions to be performed. If other areas are affected (e.g. physical damage in a production center) other continuity plans might be invoked as well.

- The SCP is created based on the outcome of a BIA (Business Impact Analysis) and Risk Assessment.

Introduction
Service Continuity Plan definitions

- Disaster
  - A Disaster is a sudden unplanned event that causes great damage or serious loss to an organization. It results in an organization failing to provide critical business functions for some predetermined minimum period of time.

- Disaster Recovery
  - Disaster Recovery or DR is the ability of an organization to provide critical Information Technology (IT) and telecommunications capabilities and services, after it is disrupted by an incident, emergency or disaster. DR recovers the disrupted IT and telecommunications capabilities to ensure Critical Business Functions can continue within a minimum period of time, pre-determined by the organization, to planned levels of operations.

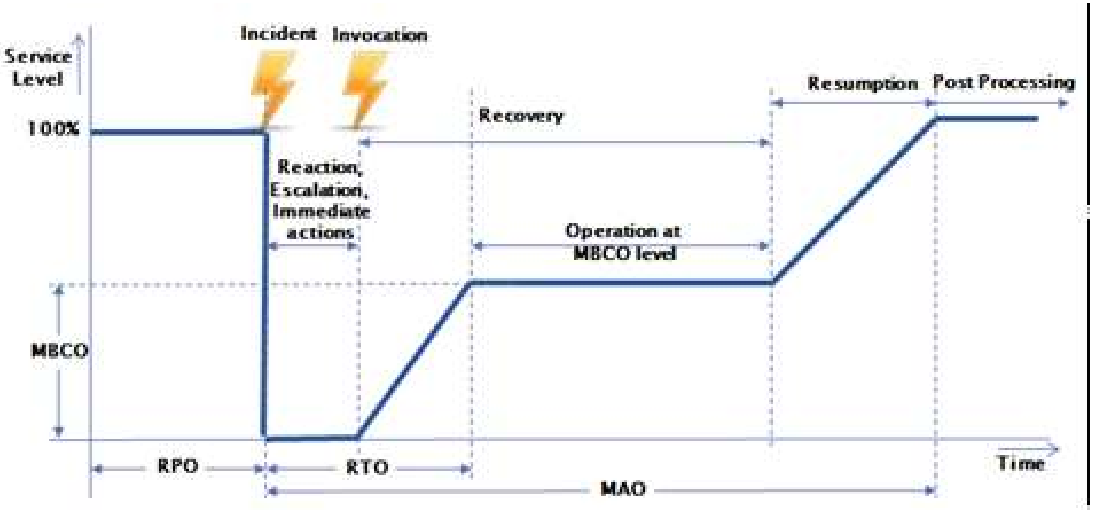
Introduction

SCM recovery requirements

- Key figures determine the requirements to be met during a disaster are listed below (*
  - Recovery Point Objective (RPO)
  - Recovery Time Objective (RTO)
  - Minimum Business Continuity Objective (MBCO)
  - Maximum Acceptable Outage (MAO)

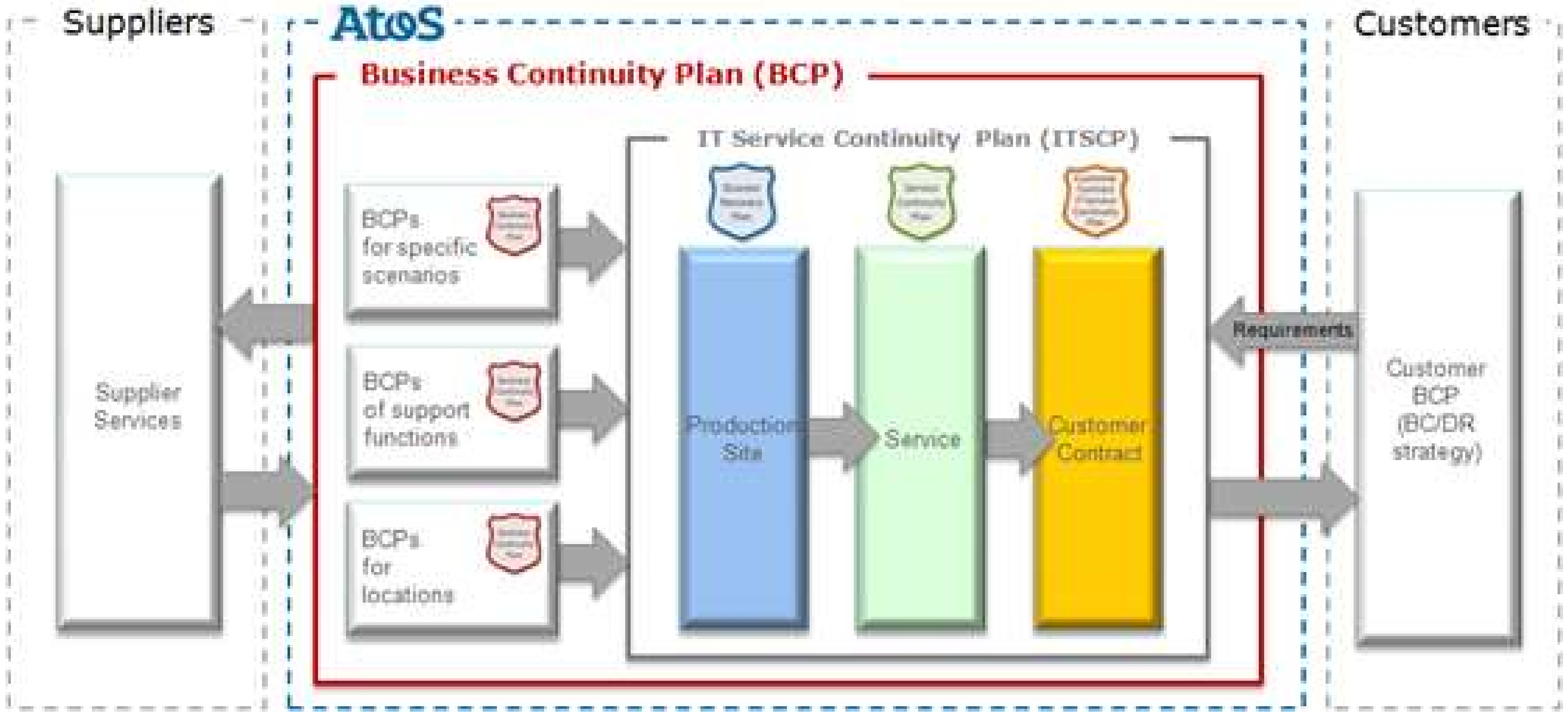
(The continuity plan is applied to customers who choose the DR option in the contract.*

Only for customers with DR option, Cloud Services can ensure the fulfillment of the contractual obligation concerning recovery of service within required RTO and RPO.



Introduction

Service Continuity Plan overview


Suppliers
Atos
Customers
Business Continuity Plan (BCP)
IT Service Continuity Plan (ITSCP)
BCPs for specific scenarios
BCPs of support functions
BCPs for locations
Supplier Services
Production Site
Service
Customer Contract
Requirements
Customer BCP (BC/DR strategy)

Introduction
Service Continuity Roles_1

- **Disaster Recovery Coordinator (DRC)**
  - A DRC is nominated as soon as the SCP has been invoked. He leads the Disaster Recovery Team (DRT) and coordinates all activities necessary to reduce the impact of the disaster and to meet specific recovery requirements such as RPO, RTO, MBCO and MAO. He is also responsible to report to the management and to involve and interact with crisis management if necessary. The DRC is the single point of contact to take first decisions and activities needed to reduce the impact of an incident

    For Cloud Services the role of DRC is the Service Responsible Manager (or the SRM’s backup).

- **Disaster Recovery Team (DRT)**
  - Consists of experts for each service involved in a disaster, executes the Service Continuity Plan and make sure that the recovery objectives are met. The team provides advice to the Disaster Recovery Coordinator in terms of selection of recovery options and priorities and sequence of work. Appendix C3 provides a list with experts from different practices in order to set-up a team quick, however, the DRC might change and expand the team as needed.
  - The Disaster Recovery Team is defined in the Major Incident Management system. The Major Incident Manager can add any employee required.

Introduction
Service Continuity Roles_2

- **Major Incident Manager (MIM)**
  - Any major business disruption is handled by the Major Incident Manager (MIM) as part of the Major Incident Management Process. The MIM will be responsible for contacting personnel as detailed in the COMET application. The MIM will be responsible for the first steps during a major business disruption or potential a potential major business disruption.
  - Depending on the complexity and the expected timeline for recovery actions, the MIM will also fulfill the role of the DRC until the DRC is appointed.
  - For Cloud Services the role of MIM is assigned from the pool of Major Incident Managers from the Service Management Center.

- **Account Service Team (AST)**
  - The AST maintains the primary relationship to the customer. In case of disaster, the AST supports the Disaster Recovery Coordinator in terms of providing customer communication. On the proactive part, the AST provides input such as customer requirements and impact to customer business and is therefore responsible to conduct customer-oriented BIAs on a regular basis. The AST also escalates risks where customer investment or acceptance is required. The AST is responsible for development, maintenance, testing and execution of customer specific continuity plans, if required by the customer.

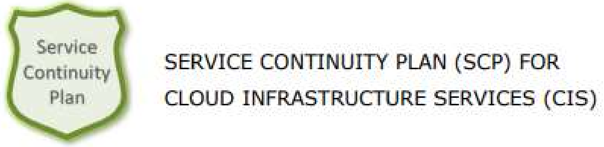
Introduction
Service Continuity Roles_3

- **Service Delivery Manager (SDM)**
  - The Service Delivery Manager (SDM) is as part of the recovery team responsible for escalating and informing the client of the current situation and keeping them informed of the progress of the recovery process.
  - The Service Delivery Manager uses the MIM as the single point of contact for the communication path during the recovery process.
  - Service Delivery Manager is currently part of AST team.

- **Tower Service Manager (TSM)**
  - The Tower Service Manager (TSM) is kept informed about the disaster and is the primary contact from the service towards the Service Delivery Manager.

Introduction

- SCP is applied uniformly to all Cloud services.
  - SCP is relevant for CIS3, CISnext, Azure and AWS. (AWS and Azure are not relevant for CIS3 team)
  - Leads to standardized terminology.
  - SCP describes all actions to be performed in case of a disaster
    - Global Cloud Services Homepage, SCM – CIS



Service
Continuity
Plan

SERVICE CONTINUITY PLAN (SCP) FOR
CLOUD INFRASTRUCTURE SERVICES (CIS)

  - MIM will initiate a Disaster Recovery process
    - MIM is in the lead during a disaster recovery process
      - MIM website
      - MIM will invoke responsible teams to participate solving the problem.
  - DRC is assigned and coordinated the DRT
    - DRT expert team solving the problem.

2 Risk reducing measures

Risk reducing measures Generic

- 7 days 24 hours support and security - grants access for technicians (incident based only)
- Monitoring on system error states.
- Analysis of received capacity threshold alerts, monitor capacity trending metrics of different components
- A comprehensive backup and recovery scheme
- Redundant management environment with recovery capabilities for critical components
- Details about the implemented risk reducing measures are described in the Atos Cloud Service continuity plan.

Risk Reducing Measures CIS3

Based on best practices, results from regular risk assessments, lessons learned from real disasters and DR tests. Atos has implemented several measures in the design of a service setup.

These measures are either intended to avoid the occurrence of a disaster or at least reduce its impact.

- TWIN data center solution
- redundant Networks, Firewall, Network Connectivity, Cooling, Power supply's
- Cross datacenter Backup
- Per datacenter; protection against power outages with UPSs and energy generator(s).

- DR option via ASR

Risk Reducing Measures DHC/CISnext

Based on best practices, results from regular risk assessments, lessons learned from real disasters and DR tests. Atos has implemented several measures in the design of a service setup.

These measures are either intended to avoid the occurrence of a disaster or at least reduce its impact.

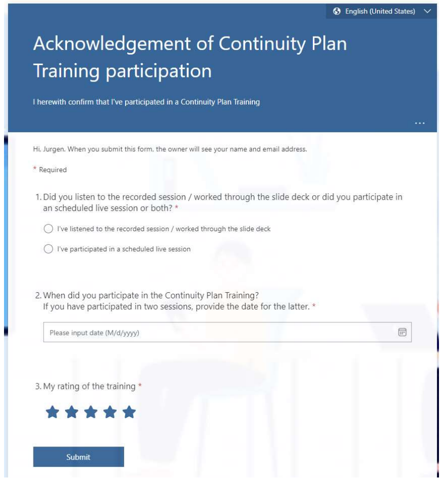
- TWIN data center solution
- redundant Networks, Firewall, Network Connectivity, Cooling, Power supply's
- Cross datacenter Backup
- Per datacenter; protection against power outages with UPSs and energy generator(s).

- DR option via Synchronous mirroring (Storage policy and affinity rules)

3 Questions

Don’t forget to fill in the attendance report

- ▶ It is mandatory to fill-in the SCM meeting attendance report.
- ▶ Please follow the attached link:
  - [Acknowledgement of Continuity Plan Training participation]()



Acknowledgement of Continuity Plan Training participation

I herewith confirm that I've participated in a Continuity Plan Training

Hi, Jurgen. When you submit this form, the owner will see your name and email address.

* Required

1. Did you listen to the recorded session / worked through the slide deck or did you participate in an scheduled live session or both? *

   ○ I've listened to the recorded session / worked through the slide deck

   ○ I've participated in a scheduled live session

2. When did you participate in the Continuity Plan Training?
   If you have participated in two sessions, provide the date for the latter. *

   Please input date (M/d/yyyy)

3. My rating of the training *

   ★★★★★