CES DEVSECOPS MANUAL

AUTHOR(S)	:	Andrada Roman, John Janse, Sophie Bertrand, Ralf Thomas, Aljosja Molenaar, Parag Deshpande, Gabriel Munteanu
DOCUMENT NUMBER	:	MSD-U02-0027
VERSION	:	3.0
STATUS	:	Final
SOURCE	:	Atos
DOCUMENT DATE	:	16 November 2022
NUMBER OF PAGES	:	72
OWNER	:	Santi Ribas

Contents

1 Introduction 6

1.1 Scope 6
1.2 Target Audience 6
1.3 General Guidance 6

2 Organization and Setup of Service Delivery 7

2.1 Introduction to Agile and SAFe 7
2.1.1 What does Agile mean 7
2.1.2 Agile Frameworks 7
2.1.3 Minimal Viable Product 8
2.1.4 Scaled Agile Framework 8
2.2 Organization and roles 11
2.2.1 Organizational setup 11
2.2.2 SAFe Portfolio and Large Solution 12
2.2.3 Essential SAFe and DevSecOps 13
2.2.4 Other Roles 14
2.2.5 Roles RACI 16

3 Development processes in DevSecOps mode 17

3.1 Continuous Delivery Pipeline 17
3.1.1 Overview 17
3.1.2 DevSecOps processes and requirements 18
3.1.3 Prepare and plan (1) 18
3.1.4 Develop (2) 19
3.1.5 Build (3) 20
3.1.6 Test (4) 21
3.1.7 Deploy to Production (5) 22
3.1.8 Operate (6) 23
3.2 Quality dimensions in continual development 23
3.3 First time deployment for a customer Quality Assurance – Service activation 25
3.3.1 KPI's for DevSecOps 26
3.3.2 Customer Requested Requirements on existing services 26
3.3.3 Service Development and Implementation – Local Services 27
3.3.4 Service Development and Implementation – Exceptions 27
3.3.5 Brownfield Takeover 28

4 Service Delivery Processes 29

4.1 Support Groups and Categories 29
4.2 Event Management 29
4.2.1 Flow chart step descriptions 30
4.3 Incident Management 30
4.3.1 Flow chart step descriptions 31
31
4.4 Problem Management 32
4.4.1 Flow chart step descriptions 33
4.5 Production 34
4.5.1 Flow chart step descriptions 34
4.6 Request Fulfillment 35

4.7 Change Management 36
4.7.1 Standard Change Management 37
4.7.2 Flow chart step descriptions - Manual standard change 37
4.7.3 Non-Standard Change Management 38
4.7.4 Flow chart step descriptions 38
4.7.5 Urgent & Emergency Change 40
4.7.6 Change Advisory Board (CAB) structure 41
4.7.7 Continuous Integration and Continuous Deployment 42
4.8 Service Asset and Configuration Management 44
4.8.1 CMDB Update – Flow chart step descriptions 44
44
4.8.2 CMDB Verification – Flow chart step descriptions 44
4.9 Release Management and Service Life Cycle Management 45
4.9.1 Flow chart step descriptions 45
4.10 Technology Refresh and Obsolescence Management 46
4.10.1 Flow chart step descriptions 46
4.11 Service Level Management 47
4.11.1 Continual Service Improvement 48
4.11.2 Service and Business Review 48
4.12 Capacity management 48
4.12.1 Flow chart step descriptions 49
4.13 IT Service Continuity Management and Disaster Recovery 50
4.13.1 Define Service Continuity - Flow chart step descriptions 51
4.13.2 Test & Operate - Flow chart step descriptions 52

5 Quality, Security and Compliance 53

5.1 Information Security management 53
5.2 Patch management 53
5.2.1 Flow chart step descriptions 55
5.3 User Authorization Management 55
5.3.1 User authorization management – Flow chart step descriptions 57
5.3.2 User Authorization Review – Flow chart step descriptions 57
5.4 Technical Security Baseline 58
5.4.1 Flow chart step descriptions 58
5.5 Security Incident Management 59
5.6 Security Monitoring & Logging 60
5.6.1 Flow chart step descriptions 60
5.7 Antivirus Management 60
5.8 Security Certificate Management Process 61
5.8.1 Flow chart step descriptions 61
5.9 Encrypted Communication 62
5.10 Network Vulnerability Scans 62
5.11 Add devices to the Atos Service Network 63
5.12 Risk Management Process 63
5.12.1 Risk Acceptance Agreement for Customers 64
5.13 Software as a Service (SaaS) Management Process 64
5.13.1 Flow chart step descriptions 65

6 Monitoring – (Management) Controls 67

6.1 Controls (monitoring) 67
6.2 Document Control 68

6.3 Training, Qualification and Certification 70
6.4 Employee Screening 70
6.5 Quality Management and Audits 71
6.5.1 Atos Integrated Management System (AIMS) 71
6.5.2 ISO and Compliance Audits guided by the yearly global program 71
6.5.3 All other (Customer) Audits 71
6.5.4 Audit findings 72

List of changes

version	Date	Description	Author(s)
1.0	1st July 2021	Traditional Ops Manual was updated according to SAFe and DevSecOps. Chapter 2 and 3 were added in relation to DevSecOps process and Updated Organization Roles were updated All processes Service Delivery and Security Processes were adapted as per the new way of working	C. Geerts A. Roman J. Janse S. Bertrand M. Pierzchalska R. Thomas
1.01	15 October 2021	Updated ITCF controls	A. Roman
2.0	25 March 2022	CES Operations Manual 8.0 was incorporated in this version of the DevSecOps Manual Document Control Process updated Incident Management interaction with DevSecOps cycle update KPI's implemented for DevSecOps were added SaaS Management Process was added Naming convention for categories and support groups was updated Links update	A. Roman S. Bertrand J. Janse A. Molenaar P. Deshpande D. Skonieczna
3.0	16 Nov 2022	Added paragraph on Brownfield takeover (quality) Added paragraph on Continuous Integration and Continuous Delivery Added comments regarding use of personal data during testing. Added security incident triggering when user access is compromised.	J. Janse G. Munteanu A. Molenaar

1 Introduction

This document defines the common way of working in the CES organization. It is based on the following standards and with input from the following sources:

- **ASMM** (Atos Service Management Model) which is extended towards the operational use of the processes
- **ITCF** (Atos IT Control Framework version 12) A set of controls which is the basis for internal and external audits. All processes must be aligned with these process requirements and related evidence. Note: The ITCF 12 applicability matrix defines the applicable controls (select MS controls "ISAE and ITCF")
- **Atos Security Policy** which provide the framework for the security processes
- Using **ATF** Standards are mandatory for all Cloud Services.
- **COBIT 2019**
- **SAFe** (Scaled Agile Framework)
- **Norea DevOps study report**
- **ISACA controls** (Information Systems Audit and Control Association)

This DevSecOps Manual describes how IT Service management processes and product development must be applied.

1.1 Scope

This DevSecOps Manual is **mandatory** for all contracts and all DevSecOps teams within CES and (sub)-contracted organizations (in on-, off- and near-shore locations).

1.2 Target Audience

Group	Objective
Management and all Operational staff within CES	To use the daily execution of the DevSecOps processes in a common way-of-working and the tools to be used.
Contract -, Service Delivery –, Process-, Service-, Tower Service - and Line managers	To understand and use the standardized Cloud Services way of working for improved cooperation.

1.3 General Guidance

- All described workflows are mandatory unless otherwise described
- Wherever in this document the indicative pronoun "he" is used this will of course also apply to the female target group.

2 Organization and Setup of Service Delivery

2.1 Introduction to Agile and SAFe

2.1.1 What does Agile mean

Agile is a set of guiding values and principles created with the purpose to help IT Companies to be more customer-centric and adaptive through a better communication and collaboration internally and externally. It moves the focus on delivering working software and responding to change in a flexible, efficient and effective way.

The Agile principles are the following:

- Highest priority is to satisfy the customer through early and continuous delivery of valuable software
- Welcome changing requirements, even late in development
- Deliver working software frequently
- Business people and developers must work together daily
- Build projects around motivated individuals
- The most effective and efficient method of communication is face 2 face
- Working software is the primary measure of progress
- Agile processes promote sustainable development.
- Continuous attention to technical excellence and good design enhances agility
- Simplicity – the art of maximizing the amount of work not done – is essential
- The best architectures, requirements and designs emerge from self-organizing teams
- At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly

2.1.2 Agile Frameworks

The Agile principles and values are brought to life through related frameworks and methods:

- Scrum is a simple framework providing a small set of rules for effective team collaboration on complex projects
- Kanban board makes work visible, limits work in progress (WIP) and measures velocity (quantity of work done in an iteration).
- ITIL/ITSM defines the processes and best practices that underpin Agile SM and promotes an integrated process approach around a service lifecycle
- Lean thinking is to create more value for customers with fewer resources and less waste
- DevOps is a cultural and professional movement that stresses communication, collaboration and integration between software developers and IT Operations professionals
- Continuous Integration is a software development practice where members of a team code separately but integrate their work at least daily. The integration goes through an automated build and test to detect errors and defects
- Continuous Delivery is a software practice where the software is always in a releasable state. Continuous delivery means that you could release when needed (not continuously deploying)

- Continuous Deployment is a software practice that focusses on executing the deployment automatically after every change.

- Scaled Agile Framework (SAFe) is a scaling framework that implements existing agile frameworks as Scrum, Lean, Kanban and business agility at an enterprise level built on three pillars: Team, Program, Portfolio.

2.1.3 Minimal Viable Product

A Minimum Viable Product (MVP) is a product which contains the features required to enable the service described in the L4D, with an aim to receiving customer feedback as quickly and 'safely' as possible, such that investment in development activity has maximum impact. The MVP can be deployed AND operated by DevSecOps team in a manner which securely meets the defined SLAs and security compliancy requirements, whilst enabling both the necessary billing and usage reporting on all new features. Additional functionality, based upon feedback from customers, will be added via an Agile development process. For that reason, the quality of the developed MVP is checked by means of the regular quality gates in continual development (see 3.2).

Minimum Viable Product (MVP) is the most pared down version of a product (or process) that can still be released, and it has following main characteristics:

- It has enough value that people are willing to use it or buy it initially
- It has enough security implemented to offer a safe environment for customer data
- It demonstrates enough future benefit to retain early adopters
- It provides a feedback loop to guide future development

2.1.4 Scaled Agile Framework

Scaled Agile Framework (SAFe) is based on four core values alignment, transparency, built-in quality and program execution which are reflected in the implementation of the framework at all levels. The objective of SAFe is to create VALUE at the best quality by respecting the people and culture, having the right flow and optimizing sustainable value delivery, providing time and space for innovation and also taking in consideration relentless improvement.

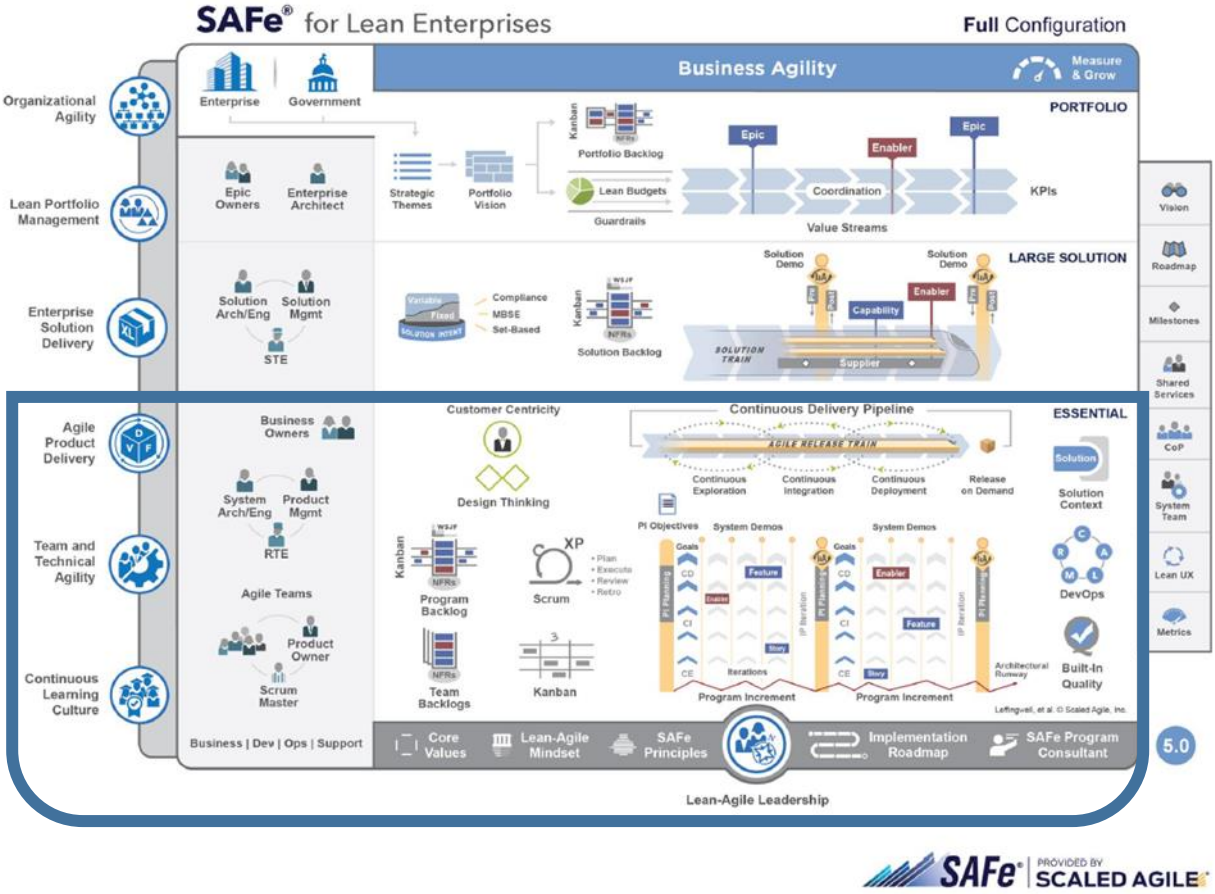
The scalability of SAFE is covering three areas. The configurations covered by this framework are the following:

- **Portfolio Configuration** provides portfolio strategy and investment funding, Agile Portfolio operations and Lean governance. The Portfolio Backlog is defined under this configuration. Portfolio configuration includes also the Essential SAFe.

- **Large Solution Configuration** describes additional roles, practices, and guidance to build and evolve large and complex solutions. The Solution Backlog is defined under this configuration.
  Large Solution configuration includes also the Essential SAFe.

- **Essential Configuration** is the most basic configuration of the framework and it provides the minimal elements necessary to be successful with SAFe. The Program Backlog, Team Backlog are defined and implemented under this configuration.

The Essential Configuration is reflecting the HOW from a product development and delivery point of view. By HOW we mean applying customer centricity with design thinking when building and delivering the product, also being aligned to the Vision and Solution objectives.



Note: This Operations manual focusses mainly on the Essential SAFe configuration.

The Agile Product Delivery when implementing SAFe is done through the following artifacts:

The Portfolio Backlog is the highest level backlog in SAFe. It provides a holding area for upcoming business and enabler **Epics** intended to create and evolve a comprehensive set of Solutions.

The Program and Solution backlogs are the repositories for all upcoming work that affects the solution. The Backlogs are a short term holding area for features and capabilities that have been approved for implementation.

Solution Backlog is the holding area for upcoming **Capabilities and Enablers**, each of which can span multiple Agile Release Trains and is intended to advance the Solution and build its architectural runway.

Program Backlog is the holding area for upcoming **Features** which are intended to adress user needs and deliver business benefits for a single Agile Release Train.

The Team Backlog contains user and enabler **stories** that originate from the Program Backlog. It may include other work items as well, representing all the team needs to do to advance their portion of the system.

Epics	An Epic is a container for a significant Solution development initiative that captures the more substantial investments that occur within a portfolio. Due to their considerable scope and impact, epics require the definition of a Minimum Viable Product (MVP) and approval by Lean Portfolio Management (LPM) before implementation.
Capabilities and Enablers	A Capability is a higher-level solution behavior that typically spans multiple ARTs. Capabilities are sized and split into multiple features to facilitate their implementation in a single PI. An Enabler supports the activities needed to extend the Architectural Runway to provide future business functionality. These include exploration, architecture, infrastructure, and compliance. Enablers are captured in the various backlogs and occur throughout the Framework.
Nonfunctional Requirements	Nonfunctional Requirements (NFRs) define system attributes such as security, reliability, performance, maintainability, scalanility, and usability. They serve as contraints or restrictions on the design of the system across the different backlogs.
Features	Feature is a service that fulfills a stakeholder need. Each feature includes a benefit hypothesis and acceptance criteria, and is sized or split as necessary to be delivered by a single Agile Release Train (ART) in a Program Increment (PI).
Stories	Stories are short descriptions of a small piece of desired functionality, written in the user's language. Agile Teams implement small, vertical slices of system functionality and are sized so they can be completed in a single Iteration.

Agile Release Train (ART) align Agile teams working simultaneously to a shared business and technology mission and along with other stakeholders, incrementally develops, delivers and where applicable operates, one or more solutions in a value stream.

Program Increment Objectives are a summary of the business and technical goals that an Agile team or train intends to achieve in the upcoming Program Increment (PI). The PI objectives are created by the teams during the PI Planning.

Program Increment (PI) is a timeboxed planning interval during which an Agile Release Train plans and delivers incremental value in the form of working, tested software and systems. SAFe divides the development timeline into a series of **iterations**, concluding with one Innovation and Planning (IP) Iteration. PI are typically 8-12 weeks long.

The Iterations are the basic building block of Agile development. Each Iteration is a standard, fixed length timebox, where Agile teams deliver incremental value in the form of working, tested software and system. Depending on the business context the length of the iteration may vary between 1-4 weeks.

When it comes Program Increment (PI) execution for a single Agile Release Train (ART), a sequence of events are taking place:

Program Events:

- Program Increment (PI) Planning
- System Demo

- Prepare for PI Planning
- Inspect & Adapt

Team Events:

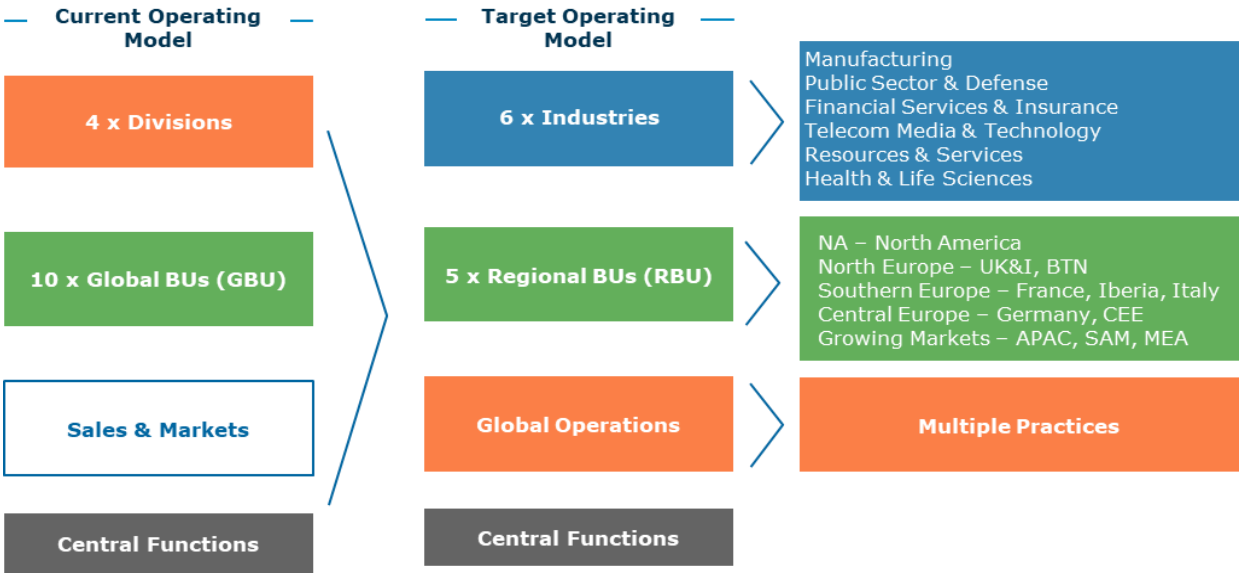
- Iteration Planning
- Daily Stand-up
- Iteration Review
- Backlog Refinement
- Iteration Retrospective

Each event is described in detail on this Link.

2.2 Organization and roles

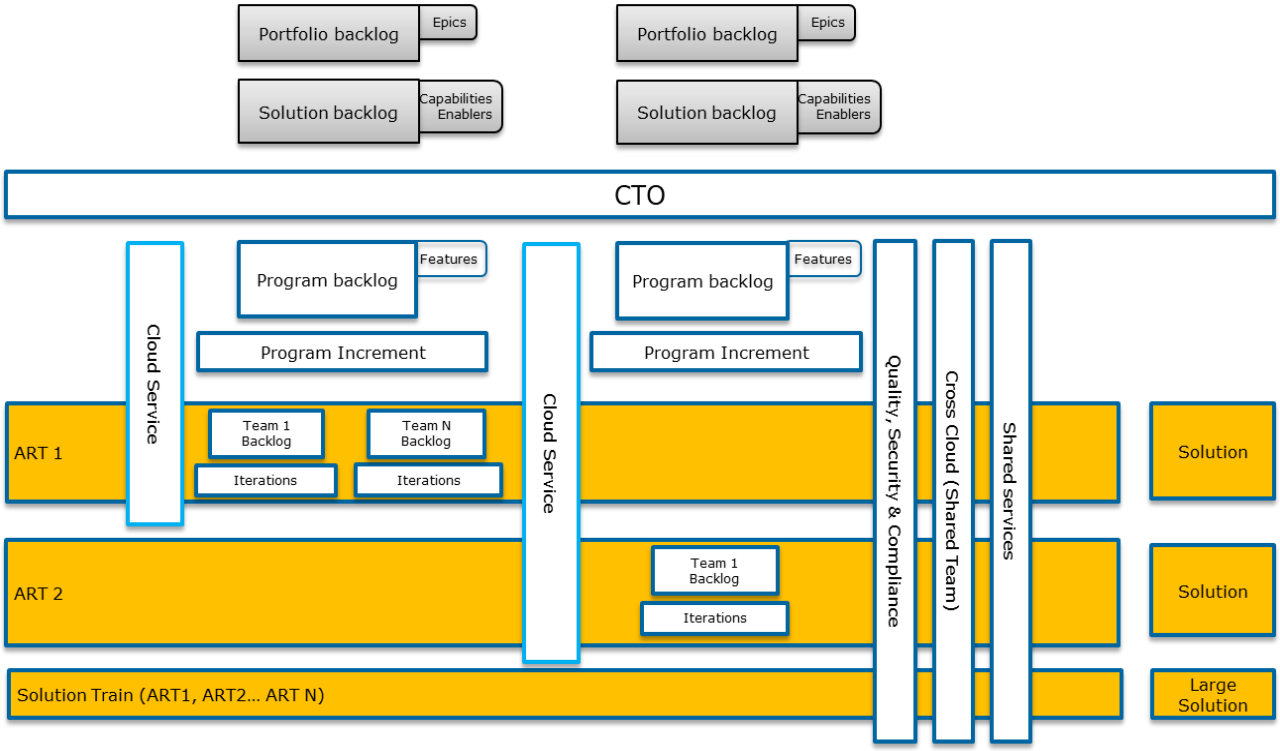
2.2.1 Organizational setup

Starting with 2020 Atos has started a program of reorganizing named SPRING. The scope of the program is to move from the current operating model where we have 4 Divisions, 10 GBU's, Sales and Markets and Central functions into a Target Operating Model designed to offer end-to-end value to the client, built around 6 Industries, 5 Regional Business Units (RBUs), Global Operations and Central Functions as it follows:



Two of the Practices in Global Operations focusing on Cloud Services are Cloud Enterprise Solutions (CES) and Data Centers and Hosting (DCH). The team in CES is delivering services across the full cloud lifecycle focusing on Public and Private Cloud and the team in DCH is delivering Storage and Backup solutions with wider scope towards Applications and OS Management.

The CES Practice will adopt SAFe for product development and the organization is reflected in the below diagram.



2.2.2 SAFe Portfolio and Large Solution

Portfolio Management Level

Portfolio Management is ensuring that the solutions designed meet customer demand and business needs. The organization strategy and investment funding are aligned to those objectives. The description of the solutions is done through an L4D. Before the solution starts to be developed the Business Case and Ready to sell milestone must be agreed by the stakeholders.

The roles defined by SAFe are mentioned below, but the implementation of the roles and the job title might differ based on business requirements:

Roles: Epic Owner, Enterprise Architect

Solution Management Level

Solution Management is responsible for defining and supporting the building of desirable, feasible, viable and sustainable large scale business solutions that meet customer needs over time. Responsibilities include working with portfolio stakeholders, customers, ART's and Solution Trains to understand the needs, build and prioritize the solution backlog.

The roles defined by SAFe are mentioned below, but the implementation of the roles and the job title might differ based on business requirements:

Roles: Solution Manager, Solution Architect/Engineer, Solution Train Engineer

2.2.3 Essential SAFe and DevSecOps

Program/Product Management Level

Program/Product Management is responsible for defining and supporting the building of desirable, feasible, viable, and sustainable products that meet customer needs over the product-market lifecycle.

Business Owner
Key stakeholders who are ultimately responsible for the business outcome. They have the primary business and technical responsibility for governance, compliance, and return on investment (ROI) for a Solution developed. They must actively participate in certain ART events and evaluate fitness for use. P&L responsibilities for the service.

Product Manager
Responsible for prioritizing features and ensuring they are well described and understood. Product Managers are responsible for managing changes to the product vision or roadmap based on the portfolio strategy and vision. Product Managers collaborate with a large set of business stakeholders in order for the products to be deployed to internal customers and also delivered to the market.

System (Technical) Architect
Responsible for defining and communicating a shared technical and architectural vision for an Agile Release Train (ART) to help ensure the system or Solution under development is fit for its intended purpose.

Release Train Engineer
Responsible for ensuring the agile release train (the team of agile teams) work well together and follow the processes.

DevSecOps Team

Product Owner
The Product Owner is responsible for defining user stories and prioritizing the team backlog. He / She is actively participating in the preparation of the PI Planning and all the events of the DevSecOps Team. The PO works with the team to detail stories with acceptance criteria in the form of acceptance tests and validates that the stories meet the acceptance criteria.

Scrum Master
Scrum Masters are servant leaders and coaches for the DevSecOps team encouraging a self-managing team. They also remove impediments and foster an environment for high performing team dynamics, continuous flow and relentless improvement.

Service Responsible Manager
Accountable for day-to-day management of the service delivery and makes sure that subcontractors are getting involved when required in the service delivery.
The Service Responsible Manager is the main contact to the MIM team. When not possible the TSM takes over this responsibility, the SRM remaining the direct contact for management reporting.
The SRM is accountable for the execution of the Service Continuity plans including testing, for correct User Management, for continuous implementation of the Technical Security baselines and timely implementation of patches.

DevSecOps Engineer (with following flavors):
Dev Engineer

The **Dev**SecOps Engineer writes and verifies code, fixes bugs, executes patch management, maintains asset and configuration repository and functions.

Ops Engineer
The DevSec**Ops** Engineer executes day-to-day technology operations (functional maintenance), monitors technology operations, performs Incident, Problem Management, manages Change Management processes.

Test Engineer
The Test Engineer creates and executes test scripts, automates tests, supports usability testing & UAT, and manages test environments and test data.

Network Engineer
Responsible for designing, implementing, and managing network within the Cloud Products.

Patch Manager
Responsible for evaluation and advice of patches for the respective layers. The patch manager is informed of the actual implementation of patches and is consulted by Operations in case gaps are identified.

Security Engineer
The Security Engineer makes sure that the product developed has integrated the security requirements (by design) and is in contact during development with the Global Security and Compliance Officer. Accountable for meeting the security acceptance criteria (definition on done completeness).

DevSecOps Quality, Security and Compliance Officer
Responsible with the E2E implementation and maintenance of the built in quality and security processes (including quality gates in development, deployment and operations).

Deployment and Release Manager
Responsible for the deployment of new Customer business and new /changed Services including the transition and hand-over to production. Responsible for release upgrades and ensure correct execution of Continuous Delivery/Deployment.

Technical Service Manager (TSM)
Primary service contact between CDE/SDM and delivery organization. Provides technical leadership in the operational matrix across Practices. Drive daily operations and Service Level Management.

2.2.4 Other Roles

Cross functional and Global Roles

Global Capacity Manager
The Global Capacity Manager takes leadership in the Portfolio capacity management topics. He chairs the Global Capacity Board, takes care of global capacity reporting, and advises the CES Management team in capacity topics. He owns the global capacity management process and ensures the implementation for CES Services.

Global Process Implementation Architect
Responsible for the implementation of (technical) service management processes for all services.

Supplier Manager
Maintains the strategic and operational contacts towards external suppliers and manages the supplier services.

Global Security and Compliance Officer (GOSCO)
The GOSCO takes leadership of the DevSecOps Quality, Security and Compliance Officers. Is responsible for the Compliance Self Assessment and Service Reviews. Participates in the development quality gates for security and compliance aspects. Is the SPOC for RACG and Global Security.

Global Deployment, Release and Security Officer
Is responsible for the full Service Activation (TOP) process and security process implementation for customers. Maintains the security processes as executed during implementation.

Global Business Continuity Coordinator (RACG)
Responsible for the availability of CES Services Service Continuity Plans based in Impact Analyses and Risk Assessment, the half yearly SCM program. The BCC will also make sure that the defined test plans are executed. Participates in the quality gate in development of service Disaster Recovery and DR testing.

Global CES Process Owner
Responsible for defining processes based on Atos (ASMM) standards, organizational and functional processes and assessing whether processes are executed according definitions. Participates in the development quality gates for ITSM integration topics. Accountable for the DevSecOps Manual.

Win 2 Deliver Improver/Approver
Ensure the standard offerings/services of Cloud Services to customers are protected and any deviations agreed are formally signed. Is also involved (consulted) in customer implementations to make sure services are delivered according to standard design. This role part of Win 2 Deliver process.

Local Delivery Center Roles

The roles defined in this section are inherited from the last version of the Operations Manual. They are applied in practice based on the organizational setup and the needs of the teams.

Delivery Center Manager
The Delivery Center Manager is mainly accountable for regional financial structures and staffing per Delivery Center. Also, involved in setting service models and making sure services are handled the same way across global delivery centers (Romania, India, Poland) and local delivery (US, UK, Morocco).

Regional Business Owner
Business Ownership resides in the RBU where the (major part) of the revenue is registered and where the assets are owned. The Regional Business Owners are de-facto the heads of the RBUs. The Regional Business Owner is accountable for contracts and services regardless if these are delivered from the Global or Local Delivery Centers.

Team Leader
Is accountable and responsible for the Engineers and the Work planner. He is also accountable for the Quality of Service. The Team Leader is initiating and chairing the Daily Huddles.

Work Planner
Has daily control of all activities done by Engineers. A major responsibility of the work planner is to maintain the quality with which the requests are handled and make sure they are handled within SLA. The work planner receives and assigns new activities by means of ATF-requests. Also, takes control of process implementation (like ATF) in the service.

Pro-Active Problem Manager
Skilled technician which does pro-active incident trend checks on a day-2-day basis (triggered out of the production plan). As a result of the checks pro-active problems are created to fix root causes and/or adjust monitoring rules.

Patch Advisory Competence Center
The Patch Advisory Competence Center role is responsible for the advisory of patches (VmWare, Dell).

Service Management Center (CO&A 1)

Concentrates on the definition and execution of Service Management Processes, based on ASMM. SMC activities for Cloud Services are globalized in one team and are mainly managed out of SMC India.

Service Management Center - Process Manager
Operational responsible for all non-standard requests which are assigned to the SMC; Non-Standard changes, Priority 1 incidents, Major Incident Management, Problem Management and Configuration Management. Also, responsible for assessing whether processes are executed according definitions.
A SMC Center of Excellence (CoE) is settled in India to cover all SMC activities for Global Cloud Services. In the CES Internal Contact List you'll find which services are already covered by CoE.

Service Management Center – Major and Critical Incident Manager
Responsible for managing Major incident after incident has been promoted to Major Incident (MI).

For more information on the ASMM roles refer to ASMM Pages.

Industry Roles (AST)

(Global) Client Delivery Executive ((G)CDE)
Responsible for contract and project execution, in line with defined budged and planning, and coordination of all key stakeholders including Industry Operations team and Global Operations Practices.

Service Delivery Manager (SDM)
Drive end 2 end project execution by orchestrating delivery between Industry and Practice Operations teams, in line with Atos delivery standards, defined budged and planning.

Customer Landscape Owner (CLO)
End-2-end responsible for delivering Atos services to a contract on technical integration of multiple Atos services.

Client Security Manager
Every customer must have an assigned Client Security Manager in line with the Atos model, who is responsible for aligning the Cloud Services security standards with the customer, all security communication to the customer and customer specific security agreements. If no CSM is assigned the SDM takes that role. The primary contact for the CSM in CO is the TSM.

2.2.5 Roles RACI

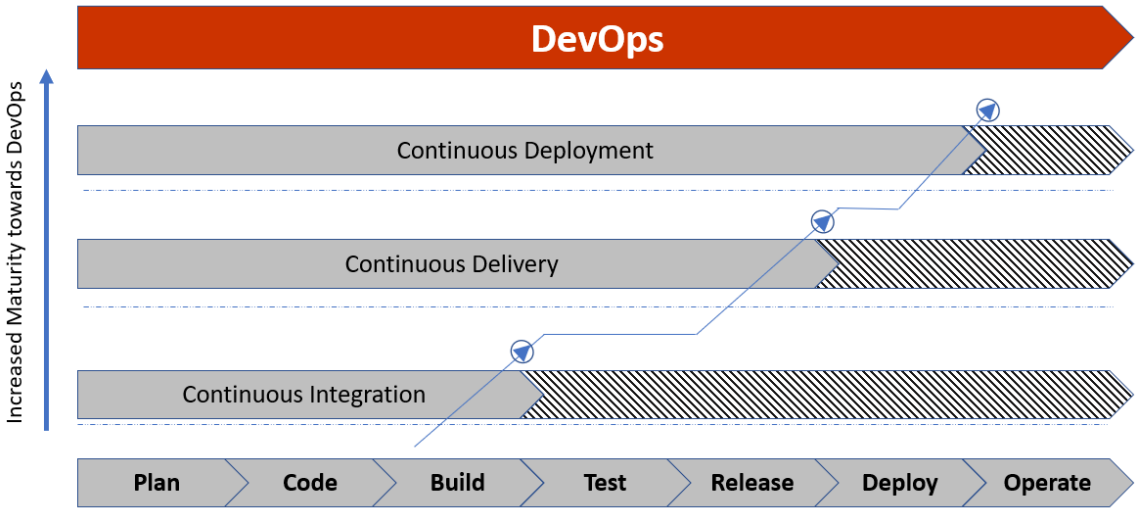
The DevSecOps roles and their responsibilities are described per process in this Cloud Operations Manual, but for more details refer to the Excel version here on SharePoint.

3 Development processes in DevSecOps mode

3.1 Continuous Delivery Pipeline

3.1.1 Overview

Continuous integration, delivery, and deployment, known collectively as CI/CD, is an integral part of a DevSecOps way of working intended to reduce errors during integration and deployment while increasing project velocity. CI/CD is a philosophy and set of practices augmented by robust tooling that emphasize automated testing at each stage of the software pipeline.



After the start of any DevSecOps setup the learning organization must pass a number of stages to become mature. Continuous deployment requires an immense mature way of working that must comply to a lot of organizational and process requirements explained in the next chapters. The three stages are:

- **Continuous Integration (CI)**: a development practice that requires developers to integrate code into a shared repository several times a day. Each check-in is then verified by an automated build, allowing teams to detect problems early. CI is an enhancement built upon the use of VCS.
- **Continuous Delivery (CD):** As an extension of CI and the next step in incremental software delivery, CD ensures that every version of the code in the CI repository that has been tested can be released at any moment. This is often referred to the concept of "maintaining code in a deployable state". It is achieved through a set of practices and methodologies designed to improve the process of software delivery and ensure reliable software releases. Leveraging automation, from CI builds, to (security) testing, to deployment, CD involves all dimensions of the development and operations organization. Ultimately, it enables the systematic, repeatable, and more frequent release of quality software to end customers.
- **Continuous Deployment:** As an extension to Continuous Delivery (CD), Continuous Deployment focusses on executing the deployment to production automatically after every change. It is the set of practices to enable frequently deploying small code changes to production by removing all manual steps in the Delivery pipeline. If a deployment causes a problem, it is quickly and reliably rolled back using an automated process. Through this robust automation, rollbacks are a reliable way to ensure stability for customers and at the same time are convenient for the developers because they can roll forward with a fix as soon as they have one.

3.1.2 DevSecOps processes and requirements

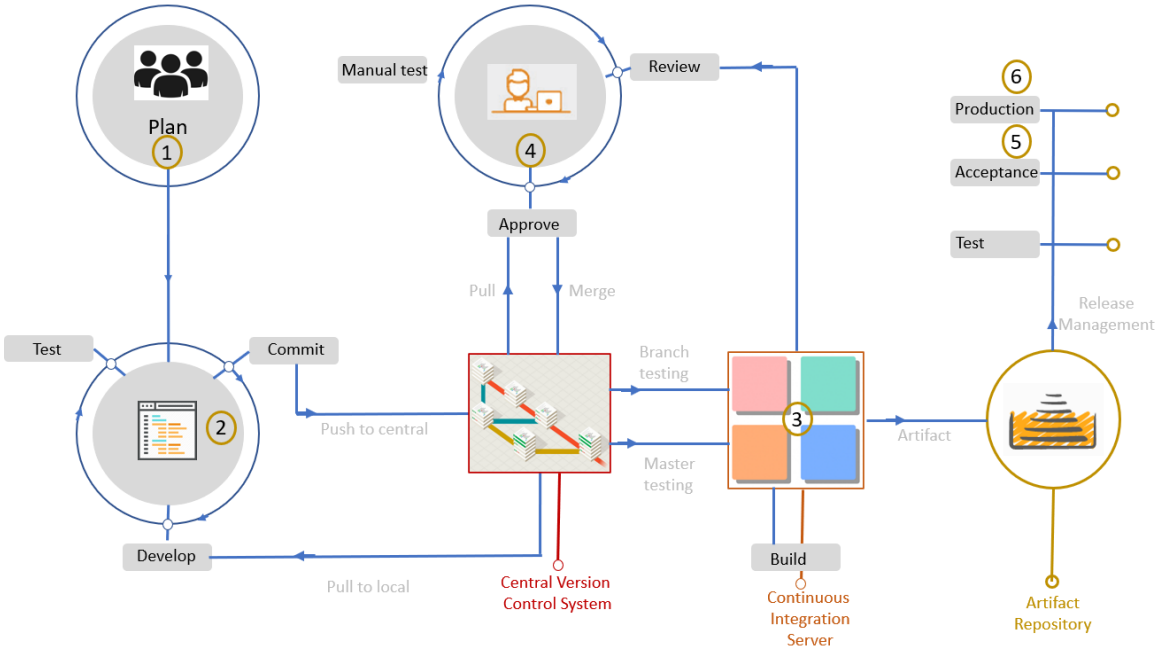
Customers will only accept and trust the highest DevSecOps maturity step of Continuous deployment if it can be evidenced that the processes are completely in control from all aspects: People, Tools and Organization.

Auditors are more likely to also audit the development process as well in order to be able to provide assurance statements to our customers that Atos remains in control end-to-end. The description below is therefore written with documentation from SAS (Statements on Auditing Standards), ISACA and Norea as major input and based on the newest COBIT 2019 release.

To manage DevSecOps in the various stages the requirements must be met to be in control and to drive the maturity of the DevSecOps organization and way of working. It is important to realize that the reason for doing it this way is not auditing but because of the products Quality, the products security, the DevSecOps efficiency and customer satisfaction.

Every stage of the Delivery Pipeline in the picture – from plan to production - is described to fulfill business and audit requirements. Please note that these are described at a high aggregation layer and that more detailed processes such as Iterations, PI planning must also comply.

These requirements are extracted from the COBIT controls for a DevSecOps way of working as extracted by Norea



3.1.3 Prepare and plan (1)

The implementation of prepare and plan fulfills the requirement that originate from the COBIT 2019 controls **BAI02.01 Define and Maintain functional and technical requirements, BAI03.09 Manage (changes to) Requirements, BAI02.12 Design Solutions based on defined development methodology, BAI03.01 Design High Level Solutions** and **BAI03.04 Procure solution components .**

Definitions & agreements

- In line with the company requirements and objectives, the development teams have selected and adopted a suitable development methodology which is properly documented.
- Based on the selected Agile method, product owners are assigned and responsible for selected business lines and/or products. Feature requests are initiated by business stakeholders (customers) and reviewed by the product owner.
- Ensure that all stakeholder requirements, including relevant acceptance criteria, are considered, captured, prioritized and recorded in a way that is understandable to all stakeholders.
- The product owner must review and adds "user stories" to the product backlog in line with the principles of the selected method. The backlog item is categorized, prioritized and Definition of Done is determined. The product owner continuously reviews prioritization of backlog items.
- Based on the service portfolio and the activities on which team members are working the high-level designs of the solutions in scope must be available. The level of detail maintained should be in line with the development method selected and appropriate for the solution.
- All relevant roles must provide input on the designs while ensuring proper stakeholders are involved.
- Supporting (IT) systems for the solution development should be properly documented (including the respective flow/interaction between the systems) throughout or after completion of the solution.
- Company procurement procedures including requirements (including security, privacy and compliance) must exist against which the candidate solutions are assessed.
- An overview must be available of all external tools/software used and matched with the acquisitions in an asset inventory.

3.1.4 Develop (2)

The implementation of develop fulfills the requirement that originate from the COBIT 2019 controls **BAI03.03 Develop solution components, BAI03.07 Prepare for Solution Testing, BAI07.04 Establish a test environment** and **BAI03.08 Execute Solution Testing**

Definitions & agreements

Maintain central control of software versions by using tools for enforcing automated version control on the code repository for Application, Infrastructure and Test code.

- A central Version Control System (VCS) must be in place and the team has enabled the proper configuration settings.
- All code changes must be logged (who, what, when) and the log data must be maintained for a sufficiently long period.
- Specific access rules must be defined for the solution in scope and must be properly implemented.
- A branch policy must be defined and followed (i.e., feature branches with review to enforce 4-eyes principle).
- Formal agreements must be made that passwords, access keys and other sensitive information is not put into the code (in unencrypted format); ideally periodic scans should be run to uncover sensitive information in the code.
- Ensure that the VCS tool is used as well for storing and maintaining the infrastructure code (unless not codified yet) as well as the test scripts.

Develop solution components progressively in a separate environment, in accordance with company standards.

- A coding standard must be available. The coding standard contains guidelines for the use of (a) programming language(s), programming style, practices and methods. The code should be automatically tested for adherence to the coding standard.
- Ensure the use of selected (secure) coding policies and enforcement of these policies by use of coding tools/frameworks integrated in the programming editor (e.g. eslint, pylint, pep8, etc.).
- Selection of external software components (including software libraries) is based on agreed upon guidelines to ensure compliance with security / maturity requirements.

Testing of the changes made should be part of the development process. The developer should produce automated test cases (e.g., Unit Tests or Component Tests) that prove the code works as intended. The automated test cases are included in the VCS together with the code, so that all future changes can be easily tested as well.

- A test approach is applicable requiring the execution of at least Unit Testing or Component Testing of the code changes made by the developer.
- The test approach must include requirements on test coverage, in order to be able to continually evaluate the test effectiveness based on a required level of minimal test coverage (e.g., 70%) per specific code module.
- The developer must update applicable automated acceptance tests when features are changed.

A peer review of the code is mandatory for the code changes based on code review guidelines.

- The team has documented their code review guidelines for performing the peer-review e.g. based on best practices such as Google Style Guide or, based on the application context, enriched with security checks from the OWASP Application Security Verification Standard (level 1 through 3).
- Once committed, the developer can push the local branch to the CVS. It must be ensured the developed code remains a branch in this stage, until further testing and merging/approval is completed.
- The VCS enforces a peer review of the code change by another developer of the team who can pull the new code change for review.

A qualified peer reviewer performs proper testing including documentation of findings and merging of code takes place only after successful testing. All actions performed are logged in the VCS.

- In case of findings, the peer reviewer provides comments to the original developer, who reviews and resolves these comments.
- The merge action is only performed after successfully passing the peer review. If the peer review fails, the merge request is declined, and the developer is responsible to fix the identified shortcomings.
- The peer reviewer checks automated builds and quality checks if included in the system (for example quality gates, unit test results, etc.) before completing the merge process .
- The VCS is configured to log all merges to master including pull requester, merger, date of merging, reference to backlog or change ticket number, code change documentation and optionally the merger's assessment comments.
- Peer reviews are performed by qualified developers that are knowledgeable with the existing code base.

3.1.5 Build (3)

The implementation of build fulfills the requirement that originate from the COBIT 2019 controls **BAI03.08 Execute solution testing, DSS05.02 Manage Network and Connectivity Security** and **DSS05.07 manage vulnerabilities and monitor the infrastructure for security-related events.**

Definitions & agreements

During the build process both the infrastructure and application code is (automatically) tested and analyzed thoroughly on for example security vulnerabilities, dependencies, third-party libraries.

- During the build process the following automated vulnerability scans should be performed (not all of it is common practice yet):
  - software vulnerability scanning;
  - third-party (open-source) component/library scanning for known vulnerabilities and licensing issues;
  - code dependency scanning for (weak) dependencies;
  - operating system baseline scanning;
  - static code analysis (conformance to defined rulesets and security testing).
- Validate the rules set by the team on failing the build (based on documented minimal requirements).

3.1.6 Test (4)

The implementation of test fulfills the requirement that originate from the COBIT 2019 controls **BAI03.07 Prepare for solution testing, BAI07.04 Establish a test environment** and **BAI03.08 Execute Solution testing.**

Definitions & agreements

After the successful build the (automated) delivery process is started by commencing a set of tests to be run on the whole code base on production-like environments. The executed (automated or manual) tests checks the module on a code level (e.g. unit tests), if the component integrates successfully with the dependent components (e.g. integration tests) and if major features of the product work as specified (e.g. acceptance tests).

- The team must create an integration test plan specifying which tests, test methods, test frequency and test tools to apply for the given change, including the resolution method to apply. Where applicable a generic test plan related to the complete solution may apply instead of a test plan per change.
- Create a test environment that is commensurate with the enterprise environment (i.e., production-like). However, to comply with privacy laws and regulations appropriate rules should be established for test data that comprises sensitive data, e.g. rules that specify for which types of personal data the test data sets should be anonymized (de-identified). Perform risk assessment, and get owner consent, if use of personal data cannot be avoided.
- Ensure the test plan, set-up of the test environment and the test results are validated with the business stakeholder (product owner).
- A register or log is maintained for test findings that need to be resolved. Tracking is performed in such a way that team members can easily follow the resolution of these findings to ensure safe delivery.

All testing scripts are developed and maintained in a version control system or versioned otherwise. This includes the test scripts for both the application code and the infrastructure.

- Ensure tests scripts are documented to ensure all team members can follow the test progress throughout the process.
- Document the minimum test coverage requirements per defined test and ensure that these are agreed upon with the product owner.
- Set up test coverage monitoring and, if currently below minimum requirement, ensure that test coverage goes up over time (in line with agreements made with the product owner).
- Where structural (testing) issues are present due to circumstances that cannot be remediated in the short term, these issues are properly documented including the cause, possible mitigation measures and suggestions for acceptance of the associated risk. These

issues are proposed towards the product owner for acceptance and proper tracking and management attention.

Tooling is used for performing integration testing on the created software builds, using predetermined test scenarios, to verify proper interoperation of (sub)systems.

- Ensure that the test approach and test plan include (automated) integration testing to be performed on all merged changes.
- Validate the integration test scripts for the inclusion of proper integration tests and use of proper tools for execution of the tests.
- Acceptance of test findings that need to be resolved is discussed within the team. When resolution is not possible in the short term, acceptance of the test finding and moving to production without resolution has to be done by the product owner, where needed in consultation with affected stakeholders.

Based on the identified test approach, proper security scans on the finished code (static code test) are performed in a timely manner (e.g. vulnerability scanning, code dependency, penetration testing). Exceptions are documented, prioritized and followed up.

- The defined test approach and test plan must include security testing and specifies the applicable testing frequency, which should be based on the context and risk profile of the solution.
- Team members who perform or review security testing must be properly qualified.
- Ensure proper registration and prioritization of the test findings. Test findings are appropriately and timely communicated to the product owner and affected or involved stakeholders.

(Automated) User Acceptance Testing (UAT) is performed on the created software build in a production like environment are performed, and noted exceptions are followed up. Business process owners and end users are involved in the UAT test.

- A test environment must be created that is commensurate with the enterprise environment (i.e., production-like). However, to comply with privacy laws and regulations appropriate rules should be established for test data that comprises sensitive data, e.g. rules that specify for which types of personal data the test data sets should be anonymized (de-identified).
- The test plan, set-up of the test environment and the test results must be validated with the business stakeholder (product owner).
- A register or log is maintained for test findings that need to be resolved. Tracking is performed in such a way that team members can easily follow the resolution of these findings to ensure safe delivery.

Note: In a CI/CD approach of a mature DevSecOps organization, where the automated tests in the Unit/Component Testing and Integration Testing phases cover all business rules, UAT tests are typically only needed to cover key usage scenarios.

3.1.7 Deploy to Production (5)

Approved and tested deliveries are (automatically) deployed to the production environment. Automatic and continuous deployment requires a mature DevSecOps organization having all previous steps in place. As long as the DevSecOps processes and organization are not mature enough Continuous Delivery instead of Continuous Deployment must be chosen.

- Perform deployment based on the change management procedure describing the CI/CD process. The procedure should also describe the different change categories: Standard, normal and emergency changes.
- Properly define the criteria for Standard changes (low-risk changes that are pre-approved e.g. infrastructure changes) and what the requirements for these changes are: e.g. do they need to be registered in the planning tool or is tracking in the VCS sufficient, what level of automated testing needs to be performed, is peer-approval required if sufficient automated testing is available etc.

- If possible, link the deployed changes to the respective change request tickets in the work planning tools (e.g. JIRA) to allow more context for the executed changes such as linking them to feature defects, incidents or user stories. E.g. by including the ticket numbers from the planning tools in the comments associated with version control check-ins which are linked to the production deployments.
- Failed deliveries should have a clear fallback scenario (rollback / fix forward) and lead to a post-implementation review (PIR) to analyze the reason for failure and optimize the delivery pipeline if possible.

3.1.8 Operate (6)

Operational activities are performed in order to deliver the services to our customers at agreed costs and within contractual agreements. All operational processes are described in Chapter 4.

3.2 Quality dimensions in continual development

Quality dimensions are embedded in the E2E DevSecOps process. Stakeholders approval and peer review are included in the process and described below. Included in the Process are the defined Nonfunctional requirements and Service Requirements which are as important as the functional requirements (features and stories) and are included in the Team Backlog and also reflected in the management tool used by the DevSecOps Team (e.g. Jira).

In case of major release the Global Practice Process Owner and Global Security and Compliance Officer must be consulted.

Portfolio Deliverables

Portfolio deliverables are discussed and approved by the stakeholders prior to development. Stakeholders involved to approve and align with the deliverables are Product Manager, Business Owner, Product Owner, System (Technical) Architect, RTE/Scrum Master and Service Responsible Manager

Product Manager is accountable in delivering the documentation and engage the right stakeholders.

In scope:
Service Description (Epic)
Business Case Agreement
Ready to Sell
Service Termination Plan (if applicable)
Risk Register

Financials:
Maia Model
KPI’s for utilization
Template for FIT and/or CSI tool integration

Prepare and Plan (1)

In Prepare and Plan the Program Increment (PI) planning takes place and Definition of Done is defined and agreed by the Product Owner, DevSecOps Team and proper stakeholders.

Input: Service Description (Epic), Business Case Agreement, Ready to Sell milestone passed
Enabler: Selected development methodology, Organizational Setup including names and certifications required.
Output: Definition of Done, High-Level Design Technology (including supporting IT system), High Level Design Service (initiated), PI Planning output including feature and stories prioritization.

Develop (2)

In Develop step a peer review is mandatory and Definition of Done completion is confirmed by the Product Owner.

Input: Deliverables from Prepare and Plan (1)
Enablers:
Configure version control system (VCS)
Logged code changes
Defined branch policy
Defined coding standards
Defined test approach for unit and component testing
Code peer review guideline (findings, repair and merge conditions)
Event management rules and thresholds implemented
ITSM Integration (Event, Incident, Configuration, Change/SSR Management).
Output (results):
Code scanning results (detecting sensitive information and adherence to coding standards and policies)
Evidence that VCS contains the complete code including tests
Overview of selected external software components
Overview of automated test cases
Evidence that VCS enforces a peer review including successful tests
Low Level Design (depending on the complexity)
ITSM implementation (fully or partially)

Build (3)

In Build step a peer review is mandatory and Definition of Done completion is confirmed by the Product Owner.

Input: Deliverables from Develop (2)
Enablers:
Infrastructure and application testing
Security and Compliancy features integration
Output (results):
Vulnerability scan report
Technical Security Specification test report
Boarding new customer guide

Test (4)

In Test step a peer review is mandatory and Definition of Done completion is confirmed by the Product Owner.

Input: Deliverables from Build (3)
Enabler:
Define integration test plans (tests, methods, frequency, tools)
Setup the test environment (representing production) and perform unit, component and acceptance testing
Perform security scanning
Documented test scripts, minimum test coverage
Output (results):
Tests (unit, component and acceptance testing) are executed and log register created
Logged test findings
Long term remediation documented (including cause of issue, mitigation measures, accepted associated risks)

Stakeholders validation

Deploy to Production (5)

In step Deploy to Production Product Owner and Service Responsible Manager confirmation is required.

Input: Deliverables from Test (4)
Enabler:
Approved and tested deliveries
Change management process, CI/CD process defined for deployment (type of change, tool/VCS log, test)
Output (results):
Ticket registration related to the deployed changes
Fallback scenario for failed deliveries (PIR)

Non - functional Requirements

The completion of the Nonfunctional requirements must be confirmed by the Service Responsible Manager. The Non - functional requirements include also the Service Integration requirements (ITSM integration)

Requirements:
Metering for customer charging (FIT)
Reporting according to L4D (including WI)
Service Continuity Management Implementation
Capacity Management (means of metering and alerting)

Production Plan
OLA's & Third-Party Agreements
Customer Onboarding Runbook
Customer User Manual (e.g. portal, presentation)
Service Catalogue
Service RACI and contact sheet

The complete list of the Non – Functional Requirements can be found MSF-U02-0024 DevSecOps - Non Functional Requirements.

3.3 First time deployment for a customer Quality Assurance – Service activation

First time deployment, equal to Service Activation, validates the deployment of a service for a customer from project into operation for local and global services. Therefore, this is not an additional set of requirements but only validation whether the deployment complies with the design and can be operated and consumed by the customer.

In order to achieve this the deployment must be validated against:
- All operational and security controls which must be implemented and operated as designed where first operational reports are delivered as evidences.
- E2E testing and/or user acceptance testing but also as a performance test, which can only be done in production. This provides a critical sanity check that validates the behavior of the solution created by developers in an actual production environment.
- Non-functional requirements (NFRs) – system attributes such as security, reliability, maintainability and usability must also be tested before final acceptance.

Definitions & agreements

- Deployment Quality Assurance Process should be initiated at the early possible stage of deployment.
- It is a mandatory process for all CES Services and uses MSF-U02-0009 TOP Checklist which is also implemented in the Service Activation Tool. This template is to be used as a deployment quality assurance.
- For all exceptions during Service activation/ Deployment Quality Assurance risk assessment must be done. These exceptions must be documented with the risk assessment and accepted by Head of Operations.

Note: In a CI/CD approach of a mature DevSecOps organization, automation and tools will play a key role in this process. Till new tools are introduced every finalized CES Deployment Quality Assurance Checklist and must be stored on CES Services Quality Records for the related service.

Quality Records can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.

3.3.1 KPI's for DevSecOps

For program increments & sprints of CES services, below KPIs and dashboards have been introduced/rolled out :

- **Program Predictability (%)**

This KPI report gives feature wise business value planned & business value delivered or kept ready for release in a particular Program Increment. Completion of actual release of a service is different than the completion of program increment.
Based on the performance and trend of Program Predictability (i.e. Business value achieved in an Increment / Business Value Planned as per backlog at the beginning of an increment *100), the business and its stakeholders gets insight about effectiveness of planning & execution of program increments.

- **Sprint Velocity Variance % (Committed v/s completed)**

This report provides Team wise Sprint Velocity variance (%) between Committed vs. Completed velocity of an individual sprint.
Based on this KPI data and trend, the business and its stakeholders get insight about effectiveness of planning and execution of Sprints.

- **Average Spending Per Story Point**

This report provides Average Spending Per Story Point for individual CES services. This is computed quarterly.

For more details on above KPIs , please refer to the dashboard information page of PowerBi.

(Apart from above KPIs, certain SAFe metrics are being introduced/rolled as a part of SAFe adoption program of CES. For more details of those KPIs, please refer to the concerned dashboard information page.

3.3.2 Customer Requested Requirements on existing services

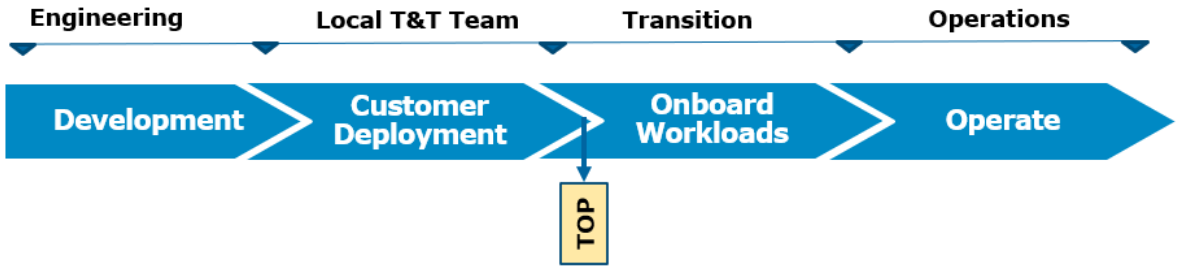
Definitions & agreements on Non-Standard Customer Requests on existing service

- A customer can request additions to its service which are not part of the standard delivery;

- If the basic service changes (release, functionality, costs etc.), DevSecOps quality gates must be passed. If the change fits within the scope of the standard service, regular change management is sufficient, and the change can be implemented by the DevSecOps team according to Change Management process;
- Portfolio Management determines whether the customer requested changes will become part of the standard service, or whether they will be treated as a customized request;
- Customized requests implementations might lead to development costs, additional investments and higher operational costs which must be aligned with the Industry (AST) and CES upfront;
- In case investments are required to adjust the service, the Business Owner and Product Manager will judge this in consultation with the related Epic Owners.
- The Product Manager decides what new features or updates are part of what release and what budget is agreed and available for the development of specific features. This is indeed also based on customer requests and input from the Product Owner and the DevSecOps team;The Product Owner determines when (in what Iteration/Sprint) the team works on what backlog story and so starts with the development of the new/updated feature;

3.3.3 Service Development and Implementation – Local Services

Specific customer requirements can lead to the development of local (GBU) Cloud services. After development and implementation, the GBU requires the service to be operated by a knowledgeable offshore support team. In this case the Cloud Services Global Delivery Centers – or when required a local cloud team – are by excellence qualified to accept the service into operation.



While such a developed service has often not followed the TOS checks and the implementation is already ongoing, a quality check (Service Activation) is required in order to ensure the service can be operated against contractual requirements.

This quality check consists of:
- A pre-agreed subset of the TOP checklist to be validated;
- A check against the requirements of the Cloud Services Security and Compliance Checklist. This check is based on Atos (security) policies and follows the rules from design principles for Cloud service designs;
- A check against the capability to fulfill the contractual requirements e.g. regulations (Hi-Trust, PCI-DSS, etc.) in designs and operations;
- A minimum set of agreed design documentation.

3.3.4 Service Development and Implementation – Exceptions

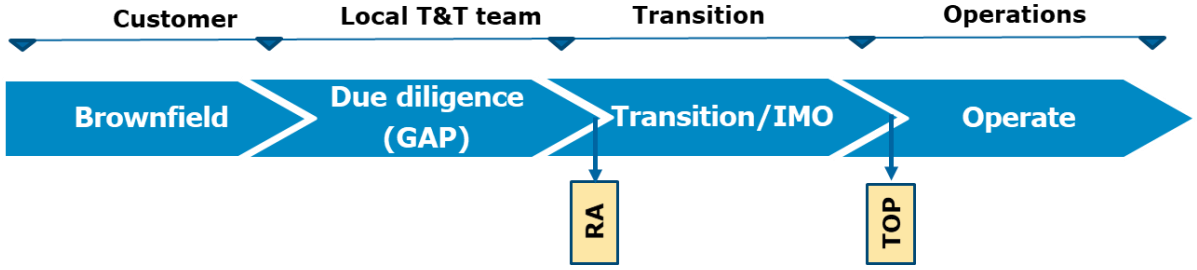
Exceptions occur only when there is a strong business justification to move a Cloud Service into operations while Service Acceptance has not passed. This is applicable for both Global Portfolio Services as well as Local Services. Note: These stages were named Early Life Support (incomplete

TOS) or Intermediate Mode of Operations (incomplete TOP). In such situations the following rules apply:

- When an SLA cannot or only partly be guaranteed. This must be documented and agreed with the Account Service Team;
- Risks from not meeting Security, Compliance or any other requirements must be documented, registered and formally accepted;
- The implementation team will not be discharged and remains responsible until acceptance to an agreed level. The involved costs are not part of operational services and are part of transition;
- The approval of taking a service into operations when Service Acceptance has not passed must be given by the Management Team;
- The **Operations Team is responsible for the full service** except for the documented and agreed exceptions. Be aware that this is not only on a best effort basis for availability. For instance, a process such as patching and user management must be executed.

3.3.5 Brownfield Takeover

A Brownfield takeover deployment requires to take over an existing infrastructure from a customer. TOP is not useable as this Brownfield will not be compliant to the ATOS during takeover. To take accountability for customer infrastructure a due diligence must be done and the GAP accepted by the customer for the period of transition. After the transition period a TOP can be done, and ATOS can take accountability for the infrastructure as described in the customer contract.



After signing the contract, a due diligence must be done on Quality, Security & Compliance on below points (based on applicability) based on reports:

1. (Security) monitoring
1. OS management
1. Patching
2. Hardening
3. Access management
4. Authorization Management
2. Problem and Incident Management
3. Change Management
4. E2E testing
5. Security testing

The GAP must be added into a Risk Acceptance form and accepted by the customer for the transition/IMO period. After the transition/IMO period ATOs can take full accountability for operations in TOP.

4 Service Delivery Processes

4.1 Support Groups and Categories

Definitions & agreements

- The rules mentioned here are applicable for the process to add/change/delete categories and support groups. E.g. not for adding an employee to a support group;
- The request for support group or category creation/deletion/modification must have the approval of the Service Responsible Manager and the Global Implementation Process Architect.
- The Global Standards for category creation can be found here.
- There are two options for category creation:
    - As **Uniformity**: to be used for Global Services with possibility of usage by multiple customers. In case of standard changes Global CES CAB and TOS approval are required for the related documentation (please see Change Management Process).
    - As **Non-Uniformity**: to be used for local services and customer specific need, in case Uniformity categories are not available. In case of standard changes Customer CAB approvals are required (please see Change Management Process).
    - Naming convention apply for all categories no matter if they are Uniformity or Non-Uniformity.

Naming convention

- Naming convention regarding the new support groups created is mandatory as follows:
    - Country.Cloud.Service-XXXX
    - *XXXX – only to be used by exception with proper justification

- In order to make sure we have accurate reporting and evidence for the CES Practice, please respect the following guidelines when creating the support group:
    - Practice = Cloud Enterprise Solution (CES)
    - Sub-Practice is one of the following – relevant for reporting:
        - "CTO-GDC" for services managed by India, Poland or Romania
        - "CTO-Private Cloud" for DHC services
        - "CTO-Public Cloud" for DCS services
        - "North America" for North American assignment groups
        - "Northern Europe" for assignment groups in the North European countries
        - "Southern Europe" for assignment groups in the South European countries
        - "Growing Market"
        - "ProcessMgmt"

- Naming convention regarding the new categories created in ATF 2 is mandatory as follows:
    - Incidents, Events and Problems: Cloud.<Platform>.<Service>
    - Changes: Cloud.<Platform>.<(Service-Number) Description>

* Numbering will be aligned with the Global Implementation Architect prior to the request for the category creation.

4.2 Event Management

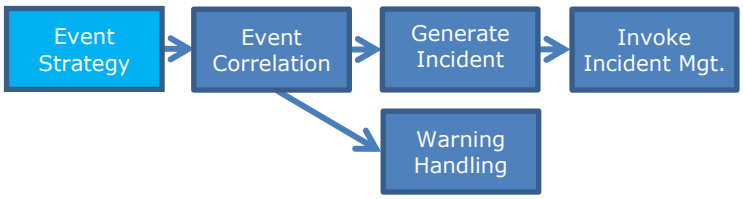
The goal of Event Management is to ensure proper handling of events generated by automated systems. Event handling can lead to a generated incident based on the event data.

The implementation fulfils the requirement that originate from the ITCF controls **EM-01 Event detection** and **EM-02 Event categorization and incident creation.**

Definitions & agreements

- Generation of event requests can be suppressed
  - to avoid having duplicated incidents based on different events e.g. multiple alerts on the same server within a short time period
  - to avoid having incidents where a warning is sufficient
- Event Strategy rules must be implemented by **Dev**SecOps Service Architect to settle the level of events (Informational, Warning or Exception)
- Events are in ITSM tool (e.g. ServiceNow) registered with a separate category next to the normal incident management categories.
- Component Capacity Management can be triggered out of an event.
- All detected events are split into categories (Informational, Warning or Exception). Incidents are created for events with specific category and are handled by the Incident Management process.
- An accurate CMDB setup is required for Event Management.

4.2.1 Flow chart step descriptions



Event Strategy *(System (Technical) Architect)*
Describe and implement event strategy in monitoring toolset.
Duplicate suppression is a part of the Event Strategy and must be reflected in the implementation.
Similar components must have a static and consistent approach for the event strategy.
(Governance over the strategies to manage event management will be defined)

Event Correlation *(Automated process implemented by **Dev**SecOps Engineer)*
Based on the correlation rules implemented the need of an incident creation will be defined.

Warning Handling *(DevSec**Ops** Engineer)*
Check generated events (activity triggered from Production Process) and act according to work instructions.

Generate Incident Request *(Automated process implemented by **Dev**SecOps Engineer)*
Tooling creates Incident Request in ITSM tool (e.g. ServiceNow).

Invoke Incident Management *(Various roles)*
Incident Request is issued in ITSM tool (e.g. ServiceNow). Normal Incident Management rules apply to handle this request.

Mandatory evidence for Event Management

- Documented Event Strategy
- Documented implemented solution in source code

4.3 Incident Management

The goal of (Major) Incident Management is to restore normal service operation (SLA) as quickly as possible and minimize the adverse impact on business operations. Failure of a configuration item that has not yet impacted service is also an Incident.

The implementation fulfils the requirement that originate from the ITCF controls **IM-01, IM-02 Incident Management** and **PM-02 Problem Management – Major Incidents**.

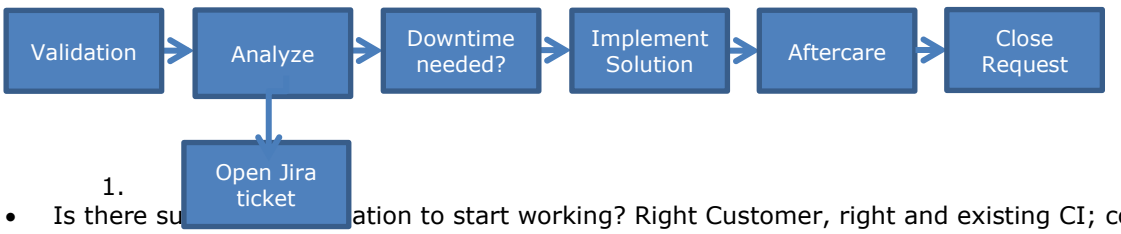
Definitions & agreements

- **Dev**SecOps team must be involved in Incident Management Process in order to achieve process improvement and be able to:
  - Plan responses to potential incidents upfront by identifying weaknesses in the system
  - Develop automated priority selection
  - Develop automated resolution
- Priority of an incident request indicates the Atos internal priority in the resolution of the incident. For details see Global Incident Management Process;
- Incidents must be integrated in an ITSM tool (e.g. ServiceNow). All required attributes must be filled out for the ticket to be properly worked on. For incidents generated by monitoring the required attributes must be filled out automatically (CI is mandatory field and must exist in the CMDB).
- Automated incident reporting must be available and trigger pro-active Problem Management process when required.
- At all times the request must contain the most actual status by means of adding regular log comments:
  - manually by the DevSecOps Engineer
  - from the automated solution implemented by the DevSecOps Engineer

Major Incident Management is an additional layer on top of Incident Management to provide a controlled and predictable framework for managing Major Incidents to reduce the recovery times of Critical Services. It covers primarily Major Incident, Major Incident Risk and additionally Priority 1 Incidents (wherever agreed with the customer, Account, or Atos Management).

- A Major Incident is any incident which requires Atos Executive Management awareness due to the likelihood of a client escalation because of the impact or risk to the client's critical business operations. Major Incident can be:
  - MI Risk: does not have a critical impact yet but needs to be resolved swiftly in order to prevent a Major Incident.
  - MI Confirmed: the risk has materialized into a real Major Incident.
- All Major Incidents and P1 Incidents (wherever agreed with the customer, account or Atos Management) are logged and regular status updates are sent via the Major Incident tool called "Comet". This is a self-subscribe service to receive notifications.
- The Lead TSM will take the role of Technical Escalation Lead during Critical Incidents.
- For every Priority 1 or Major Incident the **Dev**SecOps team must be engaged.

4.3.1 Flow chart step descriptions



1.

- Is there su ation to start working? Right Customer, right and existing CI; correct support group; enough information supplied?
- If additional information from the Requester is needed, the DevSec**Ops** Engineer contacts the Requester. DevSec**Ops** Engineer will keep the request on his own support group and fills the callback date where required
- If due to any circumstances the requester cannot be contacted involve TSM or SDM before closing the ticket or for additional clarifications.
- Wrongly assigned requests may be re-assigned, but only after mutual agreement (which must be logged into the request). The action to reassign the request must be done within short notice from request arrival. The fact that SLA resolve times have (almost) passed is no reason

not to accept a reassigned incident request. If the correct support group is unknown, then escalate to TSM or SDM.
- If all above is ok, the Incident request is assigned to a DevSec**Ops** Engineer to be worked upon.
- In case of a Priority 1 or Major Incident always inform the Service Responsible Manager and the Service Delivery Manager acting for the affected customer and activate Major Incident Management process by involving the MIM team.
- For other priorities, the contract level agreements are properly reflected in the ITSM tool (e.g. ServiceNow) and automated notifications must be sent when they are in danger to be breached.

Analyze *(DevSec**Ops** Engineer)*
- Start analyzing the reported disruption to ensure the incident is resolved ASAP.
- Escalate to Service Responsible Manager when resolution needs additional resources or disruption cannot or might not be resolved within SLA-target.

Open Jira ticket *(DevSec**Ops** Engineer and Product Owner)*
- If the conclusion of the analysis results in identifying a possible recurrent situation and it needs further development, open a Jira ticket and assign it to the Product Owner.
- The Product Owner will decide if the Incident resolution will be translated into a feature/story/bug in the next iteration and included in the DevSecOps workflow.

Implement solution *(DevSec**Ops** Engineer)*
- In case downtime of the service is needed, get approval from SRM, TSM and the customer's SDM. In case no downtime can be agreed, escalate towards SDM.

Aftercare *(DevSec**Ops** Engineer or in case of P1 Process Manager)*
- Create problem request when applicable (always in case of priority 1 or when a work-around was in scope which needs to be fixed).
- Update Root Cause and Log solution.

Close Request *(DevSec**Ops** Engineer or in case of P1 Process Manager)*
- The basic principle is to close a request immediately after solving it. In case of customer contracts where the auto-closure mechanism is available, set the request to resolved only.

Mandatory evidence for Incident Management
- Provide an overview of all closed Major Incidents for the service (per month)
- Provide an overview of all closed P1 requests for the service (per month)
- The documented Critical and Major Incident information in Comet, including the case history, which must be provided on request from the tool.
- Provide a report showing all closed Incidents for review purpose and to determine required development improvements which must be included in PI Planning
- Documented automated implemented solution in source code

4.4 Problem Management

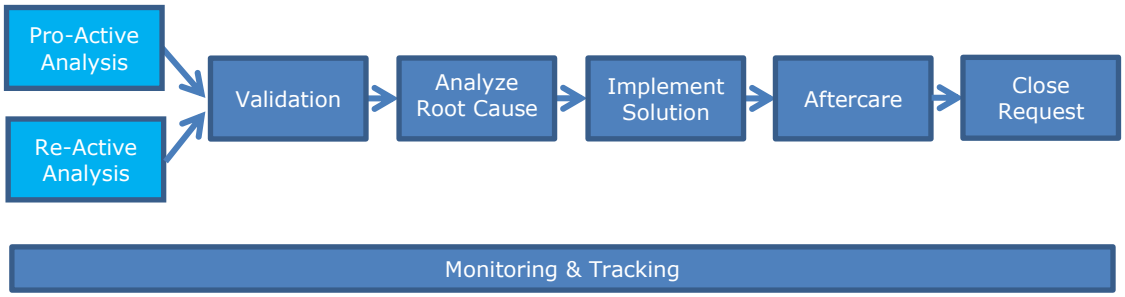
The goal of Problem Management is to prevent (re)-occurrence of incidents by eliminating their root cause.

The implementation fulfils the requirement that originate from the ITCF controls **PM-01 Problem Management** and **PM-02 Problem Management – Major Incidents**

Definitions & agreements
- Mandatory Problem Management process triggers:
  - A valid P1 incident or Major incident.

  - The mandatory periodic incident analyses by a DevSecOps engineer leads to improvement areas to be resolved via problem management. The analyses focus is on limiting repetitive incidents.
  - A Post Implementation Review (PIR) identified a structural problem which need to be resolved to prevent a future failed change.
  - An issue is identified during availability, capacity & performance analysis, IT Asset & CI verification that require initiation of the Problem Management process.
- Technical ownership resides with the applicable Cloud Services DevSecOps team and process ownership resides with the applicable Problem Manager.
- External customers cannot raise Problem requests unless contracted otherwise.
- Decide if the problem is a Single Customer or Multi Customer problem. If it is a Single-Customer problem, then Industry (AST) problem manager is acting Problem Manager. If it is a Multi Customer problem, then the CES Problem Manager is the owning Problem Manager.
- All Problems lead to a resolution: either to a structural resolution where the root cause is removed or a Known error with a workaround defined.
- A Root Cause Analysis (RCA) including root cause, action taken, action assignee and action due date must be defined based on one of the three RCA templates.
  - Major RCA template (MI confirmed usage)
  - RCA template (for usage in other reactive RCA's)
  - Pro-Active (for usage in pro-active problem management)
- The RCA can be used or a Customer Information Report (CIR). The CIR is an Industry responsibility, is not part of the problem management process and does not replace an RCA.

4.4.1 Flow chart step descriptions



Pro-Active Analysis *(DevSec**Ops** Engineer)*
- This step must be a mandatory action in the Production Plan.
- Review incident trends and reasoning reports and identify potential problems.

Re-Active Analysis *(Problem Manager/DevSec**Ops** Engineer)*
- This applies after a P1/Critical Incident or MI has been resolved.

Validation *(Problem Manager)*
- Is there sufficient information to start working? Otherwise go back to initiator of the problem to add required information to the description of the problem.
- When the problem is a Known Error close the request with connecting to the known error.
- In case problem already exists check if update is needed.

Analyze Root Cause *(**Dev**SecOps Engineer & Problem Manager for getting approvals)*
- Start analyzing, find the root-cause and define the solution for the reported problem. Engineer will start writing the RCA according global template, provided by the Problem Manager. Process Manager will coordinate request and quality.
- Define actions (defined in the solution) as WFT within the problem request.

- If the solution needs to be developed open a Jira ticket and assign it to the Product Owner.

Implement solution *(**Dev**SecOps Engineer)*
- Follow the applicable process to implement the build solution (Change Management / Continuous Delivery / Continuous Deployment).
- In case downtime is needed get approval for this from own management and Industry of customer via normal procedures.

Aftercare *(Problem Manager)*
- Check if problem has been solved: Are incidents related to this problem not occurring any more under the same circumstances as described in the problem.
- Set request to status Resolved and get approval from SRM to close the problem based on above evidence.
- Upload the final RCA document on SP and provide the URL into the problem ticket.

Close *(Problem Manager)*
- Check RCA lifecycle status.
- Set request to status Closed.

Monitoring & Tracking *(Problem Manager)*
- Perform Regular problem and action monitoring, tracing and tracking.
- Perform Escalation if required.

Mandatory evidence for Problem Management
- RCA initiated for all P1/Critical Incidents and Major Incidents
- RCA document when applicable to be stored on Quality Records Environment (add link to this document in the ATF request).
- Service Responsible Manager approval of RCA to be stored on Quality Records Environment.
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.

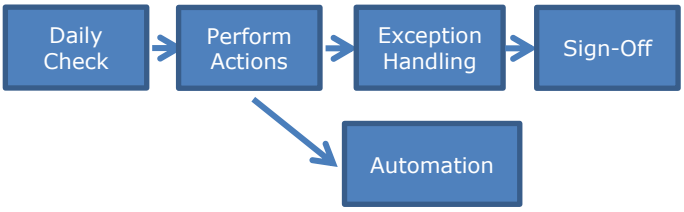
4.5 Production

The goal of (IT) Production is making and keeping the ongoing Services available, reliable and consistent.

The implementation fulfils the requirement that originate from the ITCF controls **LS-13 Antivirus / Malware, IM-02 SLA threshold monitoring, LS-15 Cryptographic Key Management, DB-02 Backup Monitoring** and **OP-02 Operations Monitoring**

Definitions & Agreements
A production plan contains recurring activities required to maintain a stable operational environment. The activities support other processes as:
  - Antivirus tooling
  - Security Certificates expiration
  - Backup Schedule
  - Obsolete components and technology refresh
  - Configuration management accuracy
  - Proactive problem management
  - Service Continuity Plan(s)
- Template to be found here;
- Besides these activities the production plan needs to be completed with service specific activities.
- DevSecOps has in important role in the automation of the operational activities.

4.5.1 Flow chart step descriptions



Daily Check *(DevSec**Ops** Engineer)*
- Check every morning at start of working day, the service production plan.
- Check which actions need to be done for that day (can be e.g. daily, weekly, monthly actions)

Perform Actions *(DevSec**Ops** Engineer)*
- Perform actions according plan and according associated work-instructions

Automation *(**Dev**SecOps Engineer)*
- Define automation actions to improve the execution of the activities
- Propose the actions to the Product Owner in order for them to be included in the Team Backlog

Exception Handling *(DevSec**Ops** Engineer)*
- In case issue/exception encountered during production check actions, issue incident request(s) and handle according regular incident management process.

Sign-Off *(DevSec**Ops** Engineer)*
- Provide mandatory evidence.

Mandatory evidence for Production Management
- Finalized and approved Production Plan
- Sign-Off your checking activities by means of registering this in a production plan log which is stored on Quality Records Environment. In case incidents are raised because of your check, name incident request numbers in the log-file.
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.
- Show that production-plan is quarterly checked on its content
- Configured backups including retention information (screenshot backup tool)
- Overview of pre-defined backup schedules and retention period
- Monthly trend check on backup failures including resulting actions
- Be prepared to provide change request sample in which backup schedule change is shown

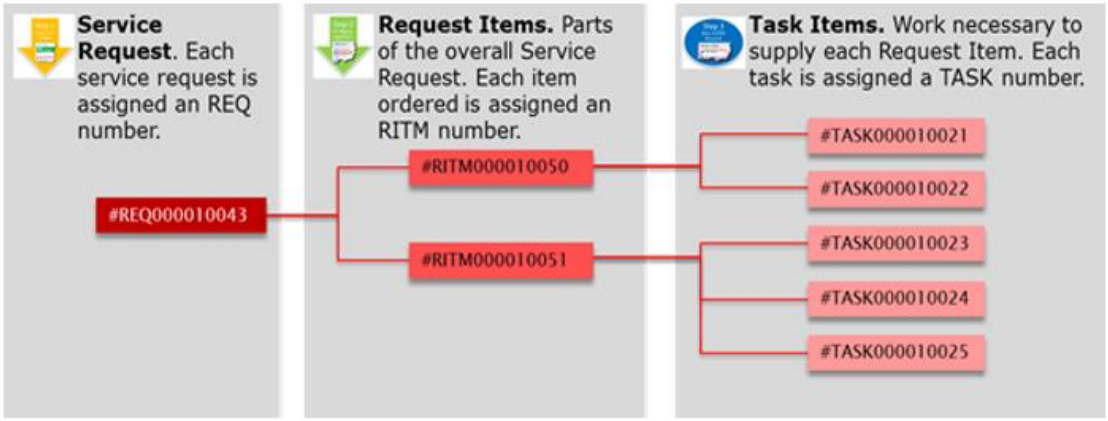
4.6 Request Fulfillment

The Request Fulfillment process was added in version 6 of the Operations Manual. It is a new process implemented and enabled by ServiceNow.

Catalogues in ServiceNow

Two different catalogue types are used to support the customer when issuing requests.
- The **Service Catalogue** contains the predefined **Standard Service Requests** which are part of Request Fulfillment;
- The **Change Catalogue** contains the predefined **Standard Changes** which are part of change management.

A **Standard Service Request** will result in one or more **pre-defined Request Items** and each Request Item in one or more **pre-defined Task Items**. It is important to note these are pre-defined and documented.



Definitions & agreements

- A standard service request (SSR) can be of one of the following types:
  - A Standard Service Request which is fully automated. All task items will be executed automatically, no manual work required or allowed;
  - A Semi-Automated Standard Service Request which contains one or more Task Item which have to be executed manually;
  - A fully Manual Standard Service Request, also called Order to Ticket (O2T), contains Task Items which are all manual.
- An SSR is to be repeatable with high success ratio;
- An SSR is designed and approved by Portfolio and respective service architects;
- An SSR is targeted for multiple customers;
- An SSR has a standardized workflow;
- A CSR (Customer Service Request) follows the same rules, however these are dedicated to one single customer and not available for other customer;
- CSR's are not recommended, instead the use of service defined SSR's must be considered;
- Both SSR and CSR are fully documented;
- SSR's can only be added to the Service Catalogue of the ServiceNow production system when the mandatory elements such as documentation and testing are checked and approved during the quality gates of a product development;
- All SSR's are integrated in the ITSM tool (e.g. ServiceNow) generating a record for audit and reporting purposes (including automated SSR's).
- An Incident request must automatically be created when an automated SSR fails. The SSR must be kept remaining open until the incident is resolved.

Note: Queries and Information Requests are not part of request fulfillment.

Mandatory evidence for Request Fulfillment - Generic

- Overview of all executed SSR's per type during a period
- Test result of the SSR's during product development
- Documentation of the design of the SSR (E.g. Work instruction, CIP or BIG stored on Global Cloud Service Library for every SSR)

4.7 Change Management

The goal of Change Management is to manage changes with minimum disruptions, risk and complexity while maintaining agreed Service levels

The implementation fulfils the requirement that originate from the ITCF control **CM-01 Change Management Process, CM-02 Change ticketing system, CM-03 Testing Execution, CM-04 User Acceptance and Promotion to production, CM-06 Handling of emergency changes** and **CM-07 monitoring of change management controls**

A change can be one of the following types:

- Standard Change
- Non-Standard Change
- Urgent and Emergency Change

Each change type will be described in the following sections.

4.7.1 Standard Change Management

Definitions & Agreements

- For Cloud Services a standard change can be:
  - Manual Standard Change
  - Automated Standard Change if it's fully automated. No manual intervention is allowed.
- Standard changes must be pre-defined, implemented and frequently used.
- ITSM tool (e.g. ServiceNow) integration with required information is mandatory (workflow tasks and the correct group & service type assignment);
- Manual standard changes are verified and approved once by Global Cloud Services Change Advisory Board and Service Responsible Manager via quality gates during development and E2E testing. Standard Changes are not subject to CAB approval when called in operation.
- Are defined in the Global Cloud Services Standard Change and Catalog with required documentation (WI, CIP (manual standard changes), BIG or Blueprint design (automated standard changes))
- CI filled in every change request is mandatory. Use generic CIs in case of new CI creation and/or in case of multiple CIs involved.
- Customer organizations visibility is required in the ITSM tool.

4.7.2 Flow chart step descriptions - Manual standard change

Validate Change *(DevSec**Ops** Engineer)*

- Is it in the scope of the team(right support group)?
- Is ATF Organization correctly chosen?
- Is the category chosen valid for the change requested? (if applicable)
- Is CI field filled?

If one or more of the above checks are not fulfilled, request customer to adjust request and set request to status 'On Hold – Clock Stopped' and hold reason 'Waiting for Requester Input'. Add log comment.
Daily check on updates on request, if no update send reminder. If required update is not done within 3 working days, close request with

- Close Reason 'Invalid'
- Completion State 'Rejected'
- Fill reason for rejection in the field 'Solution Description'

In case the change is a non-standard or it is not for your service, transfer the request to the AST Change Management Group. Set the request status to 'Work in Progress' when request is accepted.

Implement Change *(DevSec**Ops** Engineer)*
Follow work instruction(s) which are described in Standard CIP and/or Change Catalog. Update CMDB when applicable (In Case of Automated Standard Changes the CMDB must be updated automatically)

Inform Customer *(DevSec**Ops** Engineer)*
Inform customer on completion by means of adding a log solution on what you did and set request to status completed. In case no aftercare is required, set the request to status 'Closed' in this stage.
(CES assumes manual notifications are set on ATF contract level where required by the customer)

Aftercare *(DevSec**Ops** Engineer)*
Make sure aftercare activities are done as described in the work instructions and/or workflow tasks. Also, store change evidence where applicable.

Close request *(DevSec**Ops** Engineer)*
Set request status to 'Closed'.

Mandatory evidence for Change Management – Standard Change

- Work instruction, CIP and BIG or Blueprint Design stored on a known location agreed with Document Control for every standard change
- Categories described in the Change Catalog are implemented in ITSM Tool (if applicable, but tooling constraints must be discussed prior with the Cloud Global Process Owner)
- CAB approval for all manual Standard Changes
- Documented standard changes in the Global Cloud Services Change and SSR Catalog with all required elements.

4.7.3 Non-Standard Change Management

Definitions & Agreements

- ALL changes which do not comply to standard change management requirements need to be handled as non-standard changes.
- Non-Standard change can be either a customer or a cloud service non-standard change. Based on the rule who is initiating the change is the owner of the change and managing the change.
- Define if it's a Single Customer or Multi Customer non-standard change:
  - If it is a Single Customer change then AST change manager is acting change manager and gathers approval in the AST CAB.
  - If it is a Single Customer change with potential impact over multiple customers, the multi customers change process is followed.
  - If it is a Multi Customer change then SMC change manager for CES is the owning change manager and requests approval internally in CES and applicable AST CABs. (request is assigned to acting change manager)
- For Shared Cloud Services (like CCIP, TAI2, CIS3, CIS4, etc) all non-standard changes to be handled by Global Cloud Change Manager and grant Global CES CAB approval.
- Be aware that for specific services a Disaster Recovery solution is part of the service. Make sure that you take this DR solution into account during the definition of a change. See 4.13 for more information about DR
- As part of a non-standard change there can be one or more standard changes. (described in workflow when to be issued and attached to non-standard change request as child request)

4.7.4 Flow chart step descriptions

Intake Meeting *(Change Manager)*
Organize intake meeting to discuss the non-standard change
Attendees;
Technical Service Architect, Service Responsible Manager, Product Owner, Requester (e.g. CLO), SMC Change Manager.
Topics to decide on;

- Is change allowed, feasible and how to cover costs (arrange WBS);
- Classification (Use classification matrix in CIP template);
- Required skills available;
- Required implementation date.

Approval *(Change Manager)*
Gather approval from Service Responsible Manager. Store email approval on Quality Records Environment.

Startup meeting *(Change Manager)*
Organize Startup meeting with Technical Service Architect, TSM, Product Owner, AST-Customer Landscape Owner and Change Manager. Depending on the change more roles might be involved. Discuss the plan, planning and required resources. Inquire all CIP required input in this meeting.

Planning and approval *(Change Manager)*

- Make sure the CIP is filled by the DevSecOps team(template) and an ATF request is issued with pre-defined Non-Standard workflow available for all customer contracts:
  - ServiceNow: Cloud.<Platform>.GenericWorkflowNonStandardChange.

  Include all GBUs and ASTs which are involved in this change and describe the impact per GBU and AST.
- Address request and CIP to Global CES Change Advisory Board with the request to discuss and approve in case of a multi customer change. In case of a single customer change, handover the change to the customer's change manager.
  Required CES CAB attendees are: Change Manager, Service Responsible Manager, Product Owner and Requester. For Medium (Significant) and Large (Major) changes, AST approval is mandatory.
- In case of a non-standard change type 'Large (Major)', also address the change to the Atos Global Delivery CAB. Send CIP and request information to the Global Process Owner for Change Management (mailbox) and request for approval
- Store all approvals including CES CAB (and if applicable global delivery CAB) approval meeting minutes on the Quality Records Environment.
- After approval has been granted, agree on implementation date (store implementation date in ITSM tool request) and inform AST Change Manager of the final implementation date.

Typically following lead-times (including approval process) need to be taken into account;

- Small change; 2 weeks (customer/AST approval not mandatory)
- Medium (Significant) change; 4 weeks (customer/AST approval mandatory)
- Large (Major) change; 6 weeks (customer/AST approval mandatory)

If a change is approved by Global Cloud CAB, there is a defined timeframe left for the customer to submit their eventual objections or concerns regarding change implementation. This can happen after the change is being communicated to the SDM or / and customer. For significant & major changes this minimum timeframe is 5 and 7 business days respectively.

Store the final version of the CIP on Quality Records Environment.

Implement and Test *(**Dev**SecOps Engineer)*

- Implement and test the change as described in approved CIP. Store test evidence on

Quality Records Environment. (Change must be tested before the production implementation on the mandatory Test Environment which should be available per service).
- Inform customer/requester on completion by means of adding a log comment on what you did and set request to status Completed.
  (CES assumes manual notifications are set on ATF contract level where required by the customer)
- To comply with privacy laws and regulations appropriate rules should be established for test data that comprises sensitive data, e.g. rules that specify for which types of personal data the test data sets should be anonymized (de-identified). Perform risk assessment, and get owner consent, if use of personal data cannot be avoided.

Aftercare *(Change Manager)*
- Make sure aftercare activities are performed as described in the CIP.
  For instance;
  - Update CMDB and set ATF CMDB Update task to status completed when update has been done.
- Send acknowledgement via email to all involved parties on the result of the change.

Close request *(Change Manager)*
Set request status to 'Closed' and fill required fields according final result of the change. This status can either be Successful or Failed. In case it failed, a Post Implementation Review (PIR) must be created.

Create PIR *(Change Manager)*
Create PIR (template is embedded in the Global CIP template) if implementation was not done according planning and/or design.
Store final PIR in Quality Records Environment.

Mandatory evidence for Change Management – Non-Standard Change
- Store email approval CAB, AST, CC and/or SRM on Quality Records Environment. (including CAB meeting minutes)
- Store the final version of the CIP on Quality Records Environment.
- Store test evidence on Quality Records Environment.
- Store final PIR in Quality Records Environment.
- Update CMDB if applicable.
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.
-

4.7.5 Urgent & Emergency Change

Urgent Change
An urgent change is a change where the Change implementation needs to be accelerated due to business reasons. Every urgent change must have justification for urgency documented within CIP before activity is submitted to Change Management Team.
In case a change request needs a shorter implementation time than formerly agreed, first try to make an arrangement with the DevSecOps Engineer. If not possible, escalate to the Service Responsible Manager and request assistance implementing your request quickly. Urgent flag must be set in ATF for this change (after approval from Service Responsible Manager).

Mandatory evidence for Change Management – Urgent Change
- Store Service Responsible Manager approval on Quality Records Environment.
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.

Emergency Change

An emergency change can only be applied when immediate action is necessary to resolve or prevent a Priority "1 or 2" incident. In this case ATF Change type must be set to 'Emergency Change'.

Emergency change preparation recognizes the same procedural steps as a non-standard change. However Senior Management (CES and AST) and Emergency-CAB approval is required, mandatory documentation may be written afterwards.

Emergency CAB is applicable in case of prevention of a priority 1 or 2. In case of resolving a priority 1 or 2, no CAB required.

Store all evidence as described in the Non-Standard change procedure including the senior management approvals.

Mandatory evidence for Change Management – Emergency Change

- Store CES and AST Senior Management approval on Quality Records Environment
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.
- All other Non-Standard change evidence (see 4.7.3)

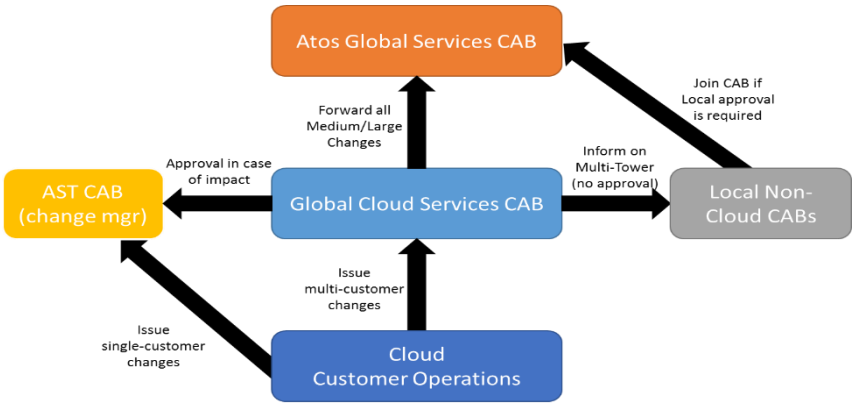
4.7.6 Change Advisory Board (CAB) structure

The Cloud Services CAB is mandatory **for every service**. This CAB has the accountability and responsibility to review and approve all Cloud Services standard changes (only once during development) and every multi-customer non-standard change. It is not allowed to implement a change without CAB approval.

In cases where a non-standard change affects multiple services, the CES Global CAB need to approve this change. These non-standard changes are always handled in ATF requesting systems.

The SMC Change Manager for Cloud Services is the chairman of the Cloud Services CAB. Service Architects are participants to the meeting. The respective TSM's are required as participants when a downtime is needed for a change. For urgent and emergency changes the approval of the Service Responsible Manager is required.

This schematic overview shows the relations between several CABs:



Global Cloud Services CAB

- Approves all new Standard Changes once, and Multi-Customer non-standard changes.

- Forward all Medium (Significant) and Large (Major) changes to Atos Global Services CAB.
- Ask for customer approval in case of service impact at the AST CABs.

AST CAB

- Handles and Approves all Single Customer Cloud non-standard changes.

Atos Global Services CAB

- Approves selected Medium (Significant) and Large (Major) changes to be decided by the Global Services CAB.

Other Non-Cloud CABs

- Will be informed by Global Services CAB on Multi-Tower Medium (Significant) and Large (Major) changes which have service impact on one or more towers.
- This is an informational message only. No approval request.

If applicable/required, the non-Cloud CAB is allowed to request for an approval.

4.7.7 Continuous Integration and Continuous Deployment

Scope

Continuous Integration and Continuous Deployment (referred from hereafter as CI/CD) is configured to build and release the changes done by a developer automatically or manually. The scope of CI/CD is to improve THE collaboration between Development and Operations by offering a more swift and reliable deployment from source code to implementation. Its target is to reduce the software development Lifecyle and provides a continuous delivery and higher software quality

Definition of CI/CD Changes

Any change requests done by a developer in Source Code Management will be automatically identified by CI/CD process and it executes the following stages: Check Out, Build, Code Quality Test and Deploy.
The code that will be executed can have two forms:
Imperative - Focuses on HOW to implement the code – how the code is written and what it contains
Declarative – Focuses on WHAT is implemented rather than what is written as code the main target is the outcome result rather than how to write the needed code to achieve the result; all Terraform code is Declarative code.

CI/CD Pipeline

CI/CD pipeline is a DevOps delivery process model for CI/CD changes. As a best practice CI/CD uses branching, version control and software configuration management (More details regarding the branching development model can be found in section 3.1.3 of the current DevSecOps manual).

The minimal steps for a CI/CD pipeline should be as follows:

- *Check Out* - A developer creates a change request (also referred to as a pull request). The implemented code must pass the application code check. Evidence must be present in selected tool that syntax and code has been checked and can be audited at any given time. The tool must have a section where the code pass is explicitly written and a report of all the changes can be generated with this information. Peer review is performed, and evidence is updated in the agreed ticketing system. Evidence must be present in selected tool with name of the reviewer, the code that has been checked, if the code has been altered a highlight of the syntax that has been checked and edited in both fixed and original form. As a good practice also a reason can be added as a comment but is not mandatory. A change record must be created in the agreed tool between Atos and the supported customer.
- *Code Quality Check* - Code quality is tested. At this phase only the syntax, empty lines or any other quality checks on the codes are being performed, as described in section 3.1.4 of the current DevSecOps manual. The functionality or outcome of the code are not tested. If the code passes the quality check and is approved by reviewer or reviewers will automatically trigger the Build and Code Functionality Test phases.
- *Build* - The actual code is being built and released to Code Function Test Phase.
- *Code Function Test* - Code is moved to pre-production (also referred to as CAT or Acceptance Environment) branch and is tested for the desired functionality. At this phase, code can be presented in the pre-production environment to the customer.
- *Customer Advisory Board Clearance* - – In order for the code to be sent for a new release and production environment to be updated, the change request must be approved by all Change Advisory Board (known from hereafter as CAB) members. Required CAB attendees are: Change Manager , Service Responsible Manager, Service Delivery Manager (or Account Lead). In CAB the deployment strategy must also be agreed and based on the deployment strategy the roll-back plan is also defined.
- *Deploy* -A new code version is released and deployed in the production environment
- *Maintenance* - After the new release has been deployed the code is being monitored for desired outcome or any possible incidents that may occur after the release.

Quality Control

To ensure service quality, the CI/CD changes must pass minimum quality standards:

- The implemented code must pass the application code check.
- Evidence must be present in selected tool that syntax and code has been checked and can be audited at any given time.
- The ticketing tool used and agreed with the customer must have a section where the code pass is explicitly written and a report of all the changes can be generated with this information.
- Peer review is passed, and evidence is updated in the ticketing system
- Evidence must be present in selected tool with name of the reviewer, the code that has been checked, if the code has been altered a highlight of the syntax that has been checked and edited in both fixed and original form

Minimal ticketing tool requirements

To ensure a good workflow, traceability and adherence to security and compliance regulation, the ticketing tool used must meet minimal criteria such as:

- Ticket number that can be traced and read by any approved party.
- Specific and separate fields for description, acceptance criteria, assignee group/member and approvers
- Date and time of creation plus audit log (type, modified, updated by, etc.)
- Once closed tickets must be still reachable for audit purpose , time of retain will be set by contract depending on the customer branch but with minimal retain period of 1 year

4.8 Service Asset and Configuration Management

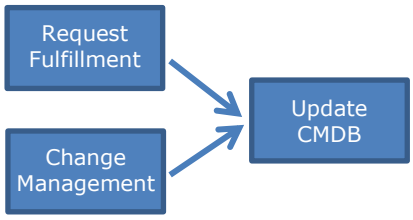
The goal of Service Asset and Configuration Management Process is to support the Atos business by providing an accurate automated representation of the managed IT services and IT infrastructure.

The implementation fulfils the requirement that originate from the ITCF controls **CF-01 Configuration Repository**, **CF-03 Configuration Data Audit & Verification, CF-02 Changes to the CMDB** and **CF-04 Configuration Data Accuracy**

Definitions & Agreements

- DevSecOps configuration management must span across development, deployment and operations
- A Configuration Item (CI) is the hardware, software, application or service object which is reflected in the CMDB data model.
- The level of detail should be based on the default out of the box data model.
- The data model can be expanded, or attributes can be added if there is a validated business requirement.
- CI update, creation and deletion into CMDB must be fully automated.
- In ServiceNow the automated CMDB updates are tasks of the RITM generated by the SSR.

4.8.1 CMDB Update – Flow chart step descriptions



Update CMDB *(Automated process or Configuration Analyst/DevSec**Ops** Engineer)*

- Every CMDB update generated by an SSR is a fully automated process. Automated updates must guarantee a consistent CMDB without any manual work.
  - By exception, for example in case of a new customer implementation, manual updates are allowed.
- For the manual CMDB update Change Management process applies, and a standard CIP is required.
- In case of manual SSR's, the CMDB update is included in the workflow and is part of the ticket generated by the SSR (TASK).

4.8.2 CMDB Verification – Flow chart step descriptions

Production Activity *(**Dev**SecOps Engineer)*

Schedule at least an automated monthly action to verify the CMDB versus the actual installed base. Must be part of the production plan.

- Automated process to check the content of the CMDB with the real live environment resulting in a correction. Automated correction reporting is preferred.

Perform Verification *(Automated process or Configuration Analyst)*

Perform verifications;

- Verification Inventory = automated comparison between CMDB and Inventory output.

- Verification Defects = check content of CMDB based on agreed data rules & relations (Data Model).

Store Evidence *(Configuration Analyst/DevSec**Ops** Engineer)*
Store mandatory evidence

Mandatory evidence for Configuration Management

- Evidence that verification run was scheduled and the generated results (sample of actual versus registered CMDB)
- Result of the deviation correction: updated report or evidence for successful scripts implementation
- The results of the verifications should be archived on the Quality Records Environment
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.

4.9 Release Management and Service Life Cycle Management

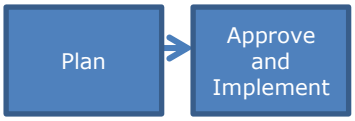
The goal of Release Management and Service Life Cycle is to group and manage individual changes into logical and recognizable modules (releases) that can be planned, developed, tested and implemented in a coherent way.

The implementation fulfils the requirement that originate from the ITCF control **AS-03 Software Version Management**.

Definitions & Agreements

- Release Management and Service Life Cycle is part of the service's technical roadmap and releases are planned accordingly;
- Each Service has a release plan which is actively maintained;
- New requirements are collected by the Product Manager and Product Owner and included in the Product Backlog;
- During the PI Planning prioritization of the Team Backlog for the following iterations is done and approved by the Product Owner;
- A release for a service consists of one (or more consecutive) iterations;
- Releases are planned with clear version control via the Version Control System (VCS);
- Regular system software, firmware and middleware updates must be part of the releases in order to contain security patches and to maintain support from the supplier;
- DevSecOps team is responsible for development of the service releases;
- When the quality gates are successfully passed the service release including firmware, middleware and RCM upgrades are made available into the repository; They can be deployed to the customer either by controlled changes or by the continuous deployment process;
- The implementation of the Service Releases and RCM upgrades is executed by the DevSecOps team.
- In principle a customer cannot decline a Life Cycle Management update. In exceptional cases a decline is allowed only when a Risk Acceptance Agreement is agreed with and signed by the customer. Skipping a release in the life cycle leads to higher costs for a next deployment and must be agreed at the time of the decline as well.
- ITSM Tool (e.g. ServiceNow) integration - attribute for service version used by the customer, including automated update after customer upgrade.

4.9.1 Flow chart step descriptions



Plan *(Deployment and Release Manager)*
Define release Forward Schedule and content with Product Owner, Service Responsible Manager and Technical Service Architect. This plan is integrated in the development cadence according to SAFe, maintained by the DevSecOps team and communicated to customers in line with the above principles.

Approve and Implement *(Release Management Board)*
Release Management Board is consisting of: Product Owner, System (Technical) Architect, Service Responsible Manager and RTE / Scrum Master.

- Each available release is reviewed and approved by the Release Management Board based on the repository.
- An available release must have passed the development Quality Gates;
- The deployment to the various customers of the versions are planned by the Release Management Board.

Once the release is approved, deploy to production process will be followed according to plan and Change Management procedure or the Continuous Deployment Process (when possible).

Emergency releases follow the Emergency Change procedure.

Mandatory evidence for Release Management

- Roadmap per service
- Release/PI planning outcome per service
- Release approval and passed quality gates documented
- All other Non-Standard change related mandatory evidence

4.10 Technology Refresh and Obsolescence Management

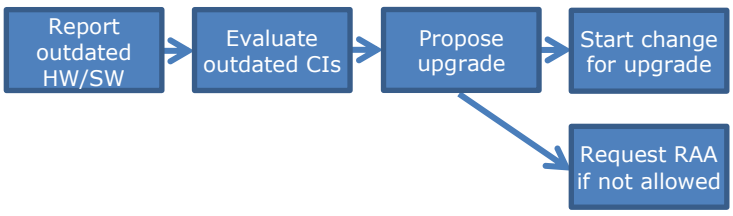
The goal of Technology Refresh and Obsolescence Management is to ensure that systems (hardware) remain supported and do not cause security or availability risks.

The implementation fulfils the requirement that originate from the ITCF control **AM-01 Hardware and Software Refresh.** It is aligned with the global process MSP-AMT-0001 Asset & Liability Management obsolescence process.

Definitions & Agreements

- End of life dates must be registered for all hardware components. Preferably this functionality should be available in the ITSM tool CMDB (e.g. ServiceNow), but when not possible, alternative solutions are accepted.
- Software components are part of DevSecOps process. Latest versions should be continuously upgraded for releases, therefore no separate registration would be required.
- Automated notification on component expiration must be generated.
- Automated reporting on customer components must be available.

4.10.1 Flow chart step descriptions



Report Outdated HW *(Deployment and Release Manager/Automated process)*
Generate report based on checks as described in the Production Plan.

Evaluate Outdated CIs *(Deployment and Release Manager)*
Evaluate the monthly report of obsolete CI's.

Propose Upgrade *(Deployment and Release Manager)*
Prepare an upgrade proposal for obsolete components. Present it to (account) management for approval. Ensure that the version repository contains the version which are tested with the latest HW versions.

Start change for upgrade *(Deployment and Release Manager)*
If the plan is accepted store the approval as evidence and hand over to the DevSec**Ops** team as regular Non-Standard change.

Request RAA if not allowed *(Deployment and Release Manager)*
If the plan is not accepted by a customer and the infrastructure cannot be upgraded create a Risk Acceptance Agreement (see 5.12.1) and present it to the AST.

Mandatory evidence for Technology Refresh and Obsolescence Management (*store on* Quality Records Environment)

- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.
- Monthly report of obsolete components (End-Of-Life (EOL) reports)
- Proposed upgrade plan for obsolete components (if any)
- Approval of the upgrade plan
- RAA's in case a customer does not approve the upgrade
- Provide evidence which shows that End-Of-Life dates are properly filled

4.11 Service Level Management

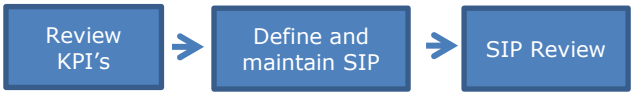
The goal of Service Level Management is to ensure that the delivery of a Service is at least in line with the agreement made with the Customer.

The implementation fulfils the requirement that originate from the ITCF control **SL-01 SLA Reporting**.

Definitions & agreements

- All services delivered to Customers/Industries, are delivered according to service design (L4D) service levels.
- If the contractual agreed SLA's are different that the SLA's defined in the L4D, an upfront agreement is required.
- Monthly automated reporting and reviewing of delivered agreed service levels (KPI's) is mandatory;
- The Service Delivery Manager is accountable for the continuous monitoring of the agreed Service levels (KPI's) with the customer;
- The Technical Service Manager (TSM) is accountable for the continuous monitoring of the agreed Service levels (KPI's) for his/her Practice;
- A periodic Internal Service Review is executed for all accounts;
- A Service Improvement Plan (SIP) is mandatory for every structural breach in agreed Service Levels (KPI's), and is i.e. based on the Service Review reporting;
- SIP's are tracked to completion according agreed plan and timelines;

4.11.1 Continual Service Improvement



Review KPI's *(Technical Service Manager (TSM))*
- Reviewing the services delivered by CES Practice, Continual Service Improvement is executed on a daily, weekly and monthly basis.
- Automated reporting must be available for the review of the KPI's
- SLA KPI's and internal KPI's must be held to agreed boundaries.

Define Service Improvement Plan (SIP) *(Service Responsible Manager)*
- If the KPI's are breached a Service Improvement Plan including the actions to be executed has to be defined and maintained.
- The results of the defined actions are included into Service Review Documentation by its action owners.

SIP Review *(Service Responsible Manager)*
- SIP reviews are done on a regular basis by at least the Service Responsible Managers and CES Management.
- The status of the SIP is presented in the Service Reviews.

4.11.2 Service and Business Review

- Service Reviews and Business Reviews are initiated by CES Management and can take place in the same time.
- In the Service Review are discussed multiple aspects of the service, like KPI's for Customer Satisfaction, Service Operation, Service Change and Service Assurance (based on CSA tooling).
- In the Business Review are discussed business updates, financial performance, KPI's and Budget planning.
- On Global Level an SLA Fulfillment Review is held. Top-x customer's performance is reviewed.

Mandatory evidence for Service Level Management
- Service review PowerPoint presentation document available on the Quality Records Environment.
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.
- Improvement plans from the Service Review must be registered in the Service Review documentation.
- Operational Level Agreements settled with internal sub-contractors if applicable.

4.12 Capacity management

The goal of Capacity Management is to ensure that the capacity of the IT services meets the business requirements in a cost effective, efficient, and timely manner.

There are no controls in the current ITCF for Capacity Management. The controls from the Compliance Self-Assessment are used.

Definitions & Agreements
- Capacity management for DevSecOps services must be executed on 2 levels:
  - Business Capacity Management – involves gathering of business requirements. Business volumes are mapped to service throughput and component utilization.

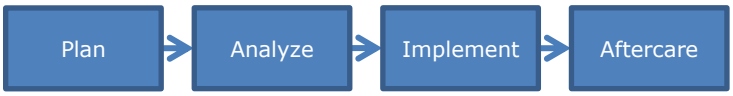
Business strategy, plans and forecast supplied by internal and external customers are used to predict future service capacity requirements.
Executed by the Industry and not the Practice.

  - Service Capacity Management: management of the capacity and performance of operational IT services covered by Service Description. It ensures the service performance and capacity is monitored and measured against service targets with appropriate thresholds.
  - Component Capacity Management: management of the capacity and performance of individual IT service components. It ensures the utilization of all components and measured with appropriate thresholds.
- Service Capacity Management requirements:
  - (Automated) Measurement of Capacity Management KPI's
  - Automated data and trend report
  - Automated forecast planning based on history trends to support timely extension of the infrastructure
- Component Capacity Management requirements:
  - Regular automated checks against defined thresholds resulting in notification;
  - Automated extension of the virtual capacity (e.g. adding LUN's, CPU's) within contractual limits

Global Capacity Board

- The capacity analysts of the services meet monthly in the Cloud Services Global Capacity Board, which is chaired by the Global Cloud Capacity Manager;
- The Global Capacity Board is tasked to:
  - Align demand and supply;
  - Analyze actual capacity versus (customer and trended) forecasted capacity;
  - Support of the approval of required investments;
  - Drive capacity short-term tunings.
- Global Capacity Management documentation can be found on the Global Cloud Services Library.
- Mandatory inputs for the Global Capacity Board:
  - New and existing customers' expansion (Rainbow);
  - Reports from the existing services and trends;
  - Input from transition projects.
- The following approach is applicable for:
  - Private and Public Cloud: capacity management is driven via the TSM towards the ASTs;
  - Shared Cloud: capacity management is driven by Cloud Services Management.

4.12.1 Flow chart step descriptions



Plan *(DevSec**Ops** Engineer)*
Check Capacity KPIs as described in the service's Production plan.
This is typically collected using automated monitoring systems.

Analyze *(DevSec**Ops** Engineer)*
Analyze KPI results. In case of thresholds exceeded, issue change request (standard or non-standard) to expand capacity. In case of high priority expansions classify the request as 'Emergency' change.
If escalation is needed, involve TSM in case of a Private Cloud solution and CES Management team in case of a Shared Cloud solution.

Implement *(Capacity Analyst)*
Guide and monitor the progress of the implementation of the capacity expansion.

Aftercare *(Capacity Analyst)*
Store mandatory evidence.

Mandatory evidence for Capacity Management

- Approved and published Capacity Management plan & procedure which includes the Capacity Management KPIs and Thresholds per KPI.
- Store analysis results (including exceptions) on Quality Records Environment.
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.
- Provide a Service Capacity Management trend report incl. actual advises and their follow-up.
- Provide Capacity Management reports as defined in the capacity management policy.
- Provide a sample of Capacity Incident reports.

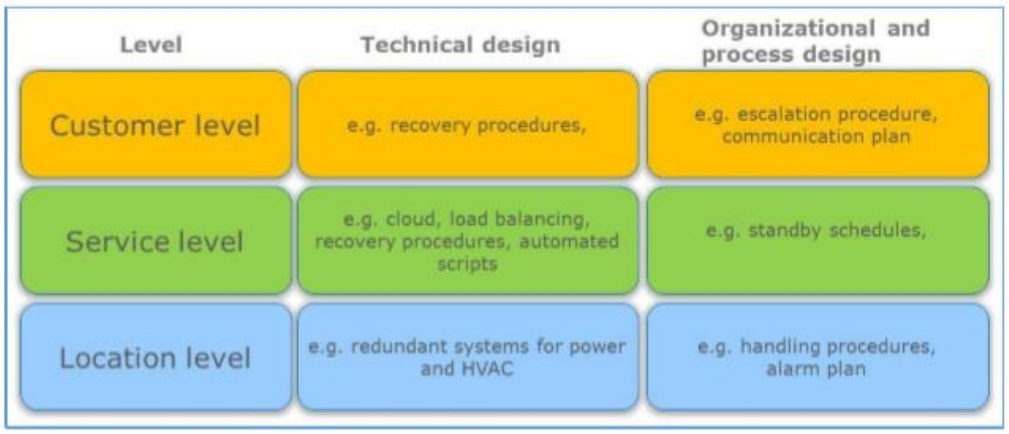
4.13 IT Service Continuity Management and Disaster Recovery

IT Service Continuity Management & Disaster Recovery (ITSCM & DR) aim to ensure that the cloud component of Atos's service offering to the client remains resilient and continues to operate effectively and efficiently in the event of a major operational disruption.

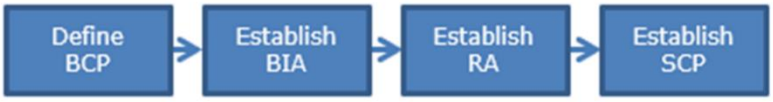
The implementation fulfils the requirement that originate from the ITCF controls **BC-01 Continuity Framework, BC-02 Continuity Program, BC-03 Continuity Plans, BC-04 Continuity testing and BC-05 Continuity Monitoring Control.**

Definitions & Agreements

- Continuity Plans are needed to fulfill requirements of ISO22301, ISO27001, ISAE3402
- CES Management has the role of Business Continuity Owner for CES Practice;
- The Global Business Continuity Coordinator, is responsible for defining CES Services Continuity processes based on Atos standards and assessing whether processes are executed according to definitions;
- Within ITSCM & DR, the Quality, Security and Compliance Officer takes responsibility for additional processes and the implementation of Business Continuity;
- The Quality, Security and Compliance Officer will engage with the Global Business Continuity Coordinator (BCC), when required, to ensure that processes are in line for all services delivered by CES;
- The Service Responsible Manager is responsible that Service Continuity for the Service is implemented, maintained, employees are trained and that tests are executed according to the agreed schedules;
- When Service Continuity Plan is invoked the SRM also takes the role of Disaster Recovery Coordinator;
- The Major Incident Manager is responsible for organizing and coordinating work during first phase after significant service disruption including contacting personnel according to alerting and escalation rules;
- It's vital to develop a failover mechanism to allow service to resume quickly, or even avoid service interruption. Disaster recovery must be planned, architected into the service, and practiced.
- All SCM documentation for CES is defined for the service level. Customer Level has to be settled by the AST, location level by the corresponding (internal) services. (See next picture)



4.13.1 Define Service Continuity - Flow chart step descriptions



Define SCP *(Global Business Continuity Coordinator)*
A Service Continuity Program defining the Service Continuity Management activities for CES, is reviewed every half year.

Establish Business Impact Analysis *(Quality, Security and Compliance Officer)*
Every newly developed service must have a design-in of a Service Continuity strategy, technology enablement and defined processes. These are used to support Service Continuity Management for the service during operations.

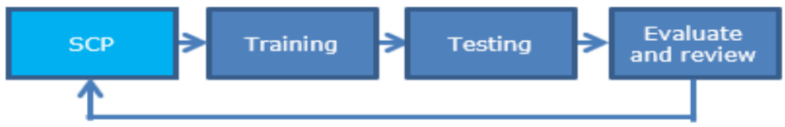
Business Impact Analyses (BIA): Conduct Business Impact Analysis (BIA) to identify the most critical service areas. Assess the impact over time of these areas, set Recovery Time Objective (RTO) and Recovery Point Objective (RPO) – when applicable. Based on result of BIA the organization will be able to focus on areas which are crucial for the service. BIA and RA need to be reviewed once a year.

Establish Risk Assessment *(Quality, Security and Compliance Officer)*
Risk Assessment (RA): Establish, Implement and maintain a formal documented RA process that systematically identifies, analyses, and evaluates the likelihood of the risk occurrence and the size of damage could create for the critical areas for the service. There are 3 possible result of RA:

- the list of existing risk mitigation actions in place,
- new mitigations actions to be done,
- risk is known and accepted by Management.

Establish Service Continuity Plan *(Quality, Security and Compliance Officer)*
Service Continuity Plan (SCP): Create the Service Continuity Plan for the service in line with the developed strategy and technology and including the output from the Risk Assessments. The format must be based on the Cloud Services global templates including the supporting appendices.

4.13.2 Test & Operate - Flow chart step descriptions



SCP Input *(Quality, Security and Compliance Officer)*
Use Service Continuity Plan as created in the definition phase.

Training *(Quality, Security and Compliance Officer)*
Conduct appropriate training to ensure all those involved are fully prepared to operate in a service continuity situation; acknowledge that employees will take on their responsibilities when the service continuity plan has to be used in case of disaster Perform a hands-on exercise in order to build confidence amongst all interested parties in the process.

Testing *(Quality, Security and Compliance Officer)*
Ensure all technical recovery procedures are periodically tested according to predefined test plans.

Evaluate and Review *(Quality, Security and Compliance Officer)*
Evaluate the test results and use for review and improvement of the SCP.

Mandatory evidence for IT Service Continuity & Disaster Recovery
- Filled Service Continuity Program template (One Global document)
- Business Impact Analysis
- Risk Assessment
- Service Continuity Plan
- Periodic testing Schedule
- Test Reports
- Training Evidence

Note: SCP Plans are a useful business continuity planning process outcome, in that they capture information that's hard to memorize and serves as guidance – on how to manage the response to a disruption. In new CI/CD approach of a mature DevSecOps organization, tools will play a key role in order to create fit for purpose documentation for SCP Process.

5 Quality, Security and Compliance

5.1 Information Security management

The goal of Information Security Management is to meet the external and internal security requirements in order to deliver secure services towards our customers.

Definitions & agreements

- The Product Owner is accountable for Compliance to ATOS policies and regulations and for Security in his DevSecOps team.
- The Product Owner is accountable for Security and Compliance awareness and mandatory trainings for a DevSecOps team.
- The security processes are mandatory for every Cloud Service and DevSecOps team;
- Information Security management is integral part of all ASMM, DevSecOps teams, security and production processes and is part of everyone's daily work;
- Atos is certified for ISO27001. External auditors perform regular surveillance audits; Audits on ISO27001 are guided via the GBU's;
- The Atos security policy is documented in ASM-SEC-0001 Atos Information Security Framework;
- For CES a Cloud Security Policy is documented in ASD-SEC-0019 Atos Cloud Security Policy;
- Atos employees have to attend the yearly Security Awareness Training. This is an on-line web based training which changes regularly and can be found on the Atos My Learning site.

5.2 Patch management

The goal of patch management is to maintain a secure computing environment continuously protected against known vulnerabilities.

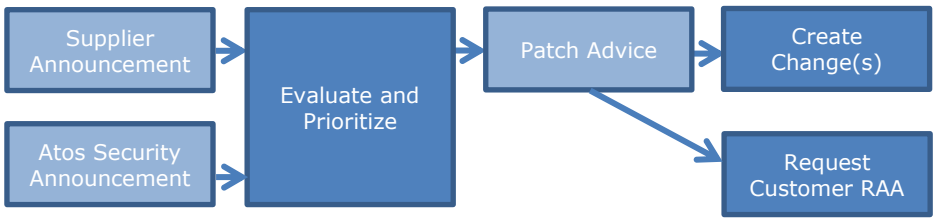
The implementation fulfils the requirement that originate from the ISO27001 standard and the ITCF control **PA-01 Patch Management (timing)** and **PA-02 Patch Deployment**.

Definitions & agreements

- Systems must be kept up-to-date with the latest security patches, as advised by the suppliers. See ASP-SEC-0014 the Atos global patch policy. (Atos Security Policy Library);
- Cloud Services often distinguish between the Cloud Management Stack and the Customer Environments, where the workloads (VM's) reside. The patch process can differ but must be compliant to the Atos global patch policy. Possible exceptions must be documented and approved.
- As a general rule the Cloud Management Stack must always be segregated from the Internet, Customer and Service Networks; To mitigate the risk;
- The Customer Environment OS patches must be implemented in line with the patch advisories;
- The Management Stack and tooling is handled different depending on the type:
    - Public Cloud Management Stack provided by a third party and patching must be in the contract with the public cloud provider.
    - The DevSecOps tools provided by a third party and patching must be in the contract with the (SaaS) provider.
    - Vblock or Vxrack is subject to the Release Certification Matrix to stay in support with vendor VCE; So, deployment of security patches must be agreed with the vendor. This is the responsibility for Patch Manager and vendor approval added to the advice.
    - Any other non-Vblock, non-VXrack and non-Public (in fact when regular systems are used) must be patched in line with the patch advisories for all of its components
- The Patch manager must maintain an overview of all applications and tools for the Cloud Service in order to track patches.
- The Patch Manager evaluate supplier information on patches and create patch advisories which are stored as evidence with the (DevSecOps) Service Documentation for that Service:

  - RCM Advisories (VCE)
  - VMware Advisories (based on VMWare competence center advisories).
  - EMC advisories
  - OS advisories (Windows and Linux) based on the GPP advisories
  - Other components such as proxy, midserver, middleware, steppingstone e.g. google, java
  - Image versions release notes
- Security patches must be deployed and agreed with the vendor for support. Patches in scope for RCM support are in three categories:
  - Patches are tested and supported by the vendor
  - Patches are supported by the vendor but not tested
  - Patches are not supported by the vendor
- Patches that are supported by the vendor must be tested or evaluated by DevSecOps and part of the Sprint (Iteration) Cycle;
  - For DPC version N or N-1 DevSecOps Team will test the patch and provide a work instruction for deploying the patches.
  - For previous DPC releases DevSecOps team will do a "paper exercise" whether the patch is applicable and compatible for the previous DPC release. And based on that study an advice will be provided to the Patch Manager for the previous DPC releases
- Patches that are not supported by the vendor will not be deployed and require a risk assessment and should be deployed risk based or accepted.
- Patching and testing of patches is part of the iteration (or Sprint) and added in the PI planning for that Iteration.
- Patches for all components must be provided as continuous delivery (automated) including:
  - Results of testing
  - Patch status for all components.
- The Product Owner is accountable for deploying patches in production per deployment/customer.
- If Cloud native images or AHS images are used (to replace patching) it should follow the same process including testing and status.
- Any Cloud (native) image must come with evidence for patching and hardening.
- The named Patch Manager manages a database of applicable patches.
- The named Patch Manager processes the patch advisories. The patch advice and the current patch status drive the Change management process and follow Change Management rules. Patches should therefore be implemented via Change requests;
- Patches must be approved and pushed to production per deployment/customer by the DevSecOps team.
- The DevSecOps team maintains overviews of implemented and recommended patches per Customer and Service under their responsibility;
- The DevSecOps team must also keep track of installed components and keep track of vulnerabilities/patches for these components;
- Maintenance windows must be either defined out of the standard shared service or are formally agreed with customer in case of dedicated service;
- The Product Owner is accountable for the timely implementation of the patches via the Change Management process;
- A Risk Acceptance Agreement must be issued when the Customer does not want to implement the advised patches. Not allowed in case of Atos owned shared CIs;
- The Service Delivery Manager is accountable to have the RAA (see 5.12.1) signed by the Customer;
- RACI on Patching is included in the overall RACI.

5.2.1 Flow chart step descriptions



Evaluate and Prioritize *(Patch Manager)*
Evaluate and prioritize the Supplier and Atos Security Announcements (input) as described in the Patch Policy and generate a Patch Advice (output).

Create a JIRA ticket and add to the backlog to test the patch and provide a work instruction or advice to deploy the patch.

The DevSecOps patch manager tracks the progress in a patch tracker. The tracker must contain:
- The patch advisories from vendors or ATOS patch advisories;
- Patch advisories with on the backlog for testing;
- Patches (changes) with on the backlog for deployment;

Create Change(s) *(Dev**Sec**Ops Engineer)*
Issue change(s) to implement patches as described in the Patch Advise.
When during patch implementation one or more patches fail, incident request should be created. This to ensure the missed patch will be installed in a later stage.

Request Customer RAA *(Service Delivery Manager)*
In case a customer wants to skip a patch cycle, Patch Manager issues a RAA request (see 5.12.1) towards the Product Owner. It's a Service Delivery Manager responsibility to get RAA approved and signed by Customer.

Mandatory evidence for Patch management
- Patch Advices must be available as evidence. Note: if a patch is not applicable this should also be reflected in the patch advice
- Change requests which are used to apply the advised patches must be available as evidence
- Risk Acceptance Agreements must be available when applicable
- Overviews of installed and non-installed patches must be available per service and per customer for Cloud Services managed environments (e.g. unmanaged systems)

5.3 User Authorization Management

The goal of User Authorization Management is to ensure the correct Atos user authorizations are issued and maintained.

The implementation fulfils the requirements that originate from the ISO27001 standard and the ITCF controls **LS-03 Administrator Account Authorization**, **LS-05 Authentication, LS-06 Account Removal,** and **LS-08 Administrator Account Periodic Access Review**

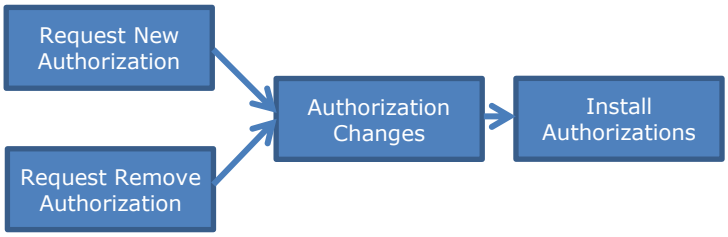
Structure and trend
The DevSecOps team builds the connection to ASN and the Global Identity and Authorization Management system will be implemented. For Cloud Services it means that the access via the ASN to the Cloud Management Environments will be controlled.

- Every Cloud Service and tool (SaaS) must have a Role Based Access Model based on least privilege.
- All access requests should be directed to the SAaCon ASN team.
- The role matrices must be verified and implemented
    - Requestors and approvers for authorizations of a service
    - The roles required for access must be defined for the services
    - The authorization matrix for the service must be correct
- The review of roles assigned to employees will be transferred to the global IAM system when applicable. Authorizations outside the Global IAM system must be in the authorization matrix for that Cloud Service and reviewed every quarter.
- Requesting and approving access will be transferred to the IAM system. Requesters and approvers will have direct access to maintain the authorizations online.

Definitions & agreements

- The Product Owner is accountable for correct User management;
- The process is mandatory for Atos employees and Employees working on behalf of Atos for customer services;
- The process is mandatory for all Cloud Service including (external) tools used. For instance SaaS tools used in DevSecOps.
- User management is based on the Logical Security Baseline MSM-GSS-0002; the naming-convention of Atos User ID's must be based on the DAS account;
- A user management procedure to be used; this can be a procedure aligned with local regulations.
- All access is granted according to the principle of least privilege, i.e. what is needed for the normal day-to-day functioning of a certain role or function;
- Extra (attention to) access controls are required for access to (personal) data, utility programs (capable of bypassing normal operations or security procedures), secret authentication information and log information.
- Only personal user ID's are allowed to be used and must be based on the DAS user account i.e. they may be prefixed or suffixed;
- All requests for access must be traceable. Change requests should be used showing the requested authorizations and approvals;
- All units have defined Approvers, who are responsible for the allocation of access and privileges for the Service(s) that that units provide;
- Each Service has defined the roles per Service and has assigned employees to role(s) in an authorization matrix
- Roles must be assigned to employees in line with the Role Based Design for the service and segregation of duties must be respected in the role assignment
- When an employee changes jobs, all access rights must be reviewed, and revoked where needed. This must be done when the employee moves to another department, but also when he or she moves to another job within the current department;
- When an employee leaves the employment of Atos, all access rights MUST be revoked within 5 business days;
- The MSF-U02-0002 Checklist for transfer or leave of employees must be used to register what actions have been taken when an employee leaves or changes jobs. This checklist is preferred unless a GBU specific checklist is required;
- The Practice delivering the service is responsible for timely initiation and execution of the user review;
- Access to a customer environment is only allowed via the Atos Service Network
- For specific customers, High Privilege customer controlled agents in Atos Cloud Environments are available. Details on how to handle are described in MSD-U02-0018.
- A security incident should be raised in case user access has been compromised.

5.3.1 User authorization management – Flow chart step descriptions



Request New or Remove Authorization *(Anybody)*
Issue a standard change request with the request for adding or removing authorization

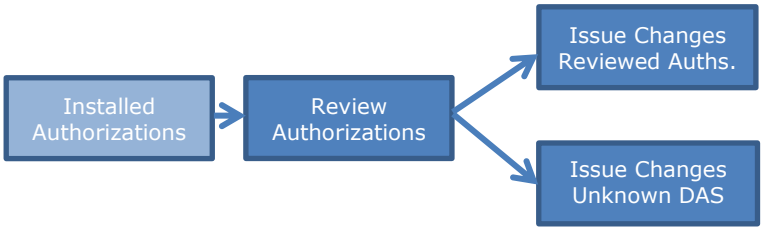
Authorization Changes *(Product owner/Service Responsible Manager)*
Authorize change by means of completing the mandatory WFT task in the change

Install Authorization *(DevSec**Ops** Engineer)*
Perform change according work instruction

Mandatory evidence for User Authorization Management

- Change requests for authorization changes must be readily available as evidence; approvals must be stored on Quality Records Environment.
- Updated authorization matrix.
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.

5.3.2 User Authorization Review – Flow chart step descriptions



Install Authorization *(DevSec**Ops** Engineer)*
The access rights of all employees must be **reviewed each quarter** against the installed authorizations and the overview of roles and assignment of employees. A report must be generated.

Review Authorizations *(Service Responsible Manager)*
Service Responsible Managers are asked to review the authorizations of employees reporting to them, participation in this review is mandatory.

Issue Changes from review *(DevSec**Ops** Engineer)*
Following the review, **Change requests** must be entered to remove revoked and unknown accounts for both known and unknown DAS users. All changes must be executed right after the review.

Mandatory evidence for User Authorization Management

- Overview of roles and the assignment of roles to employees (the authorization matrix)
- Evidence of the quarterly review of authorizations of all Atos employees by management;
- Evidence of the results of the review: changes for revokes

- Overview of employees that have left the organization (per period)
- Evidence of changes to revoke rights of the leaving employees
- Provide evidence of approval of the authorization matrix
- Provide an overview of authorization change requests for the service

5.4 Technical Security Baseline

The goal of the technical security baselines is to configure and maintain the security related parameters of every technology layer according to predefined settings in order to maintain a secure service.

The implementation fulfils the requirement that originate from the ISO27001 standard and the ITCF control **LS-01 Security Policy**, **LS-07 Account and Password Parameters** and **LS-20 Security Settings.**

Structure and trends

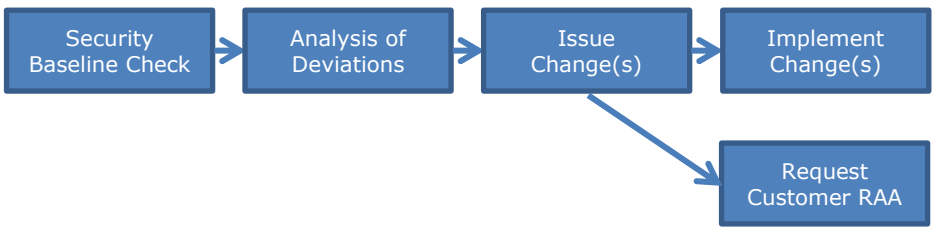
The definition of security settings is a major part of the security baselines. For many layers a description is available called Technical Security Specifications (TSS).

If no baseline is defined for Cloud Services, the Atos TSS must be used.

Definitions & agreements

- Every Cloud technology layer (virtualization, OS, network, SaaS…) must have a defined baseline or TSS which is selected or defined during the service design by the. The baselines are maintained by DevSecOps via release management of the service part of an iteration;
- A Technical security baseline contains generally accepted best practices related to the security of a given managed platform. It also describes how the Atos Security policy is implemented;
- The mitigation of non-compliances must be automated (to the maximum) or documented in a work instruction/runbook;
- All Technical security baseline settings must be monitored and automatically remediated (preferred) or create an incident ticket to ensure that they do not change over time, resulting in reduced security;
- Technical security baselines compliance must create a report monthly;
- When using cloud native components (Vendor OS images or SaaS applications) Technical baseline security must be implemented;
- The Product Owner is accountable for continuous implementation of the Technical security baselines;
- Exception: Some Cloud Services aim at delivering an unmanaged environment (e.g. the customers maintain their own virtual servers which they acquire via the cloud service). In these cases, the customer is responsible for maintaining security and compliance for that cloud layer (e.g. OS management).

5.4.1 Flow chart step descriptions



Security Baseline Check *(DevSecOps Engineer)*
Technical security baseline verification (manually or automated) must be done monthly to ensure that the Technical security baseline is implemented on the platforms in scope.
This check must be done using automated tooling.

Analysis of Deviations *(Dev**SecOps** Engineer)*
Analyze deviations from security baseline.
Some deviations may be caused by products or service specifics; they are "because that's the way it works". Such well-known deviations must be documented once. In general, no changes will be needed to correct such deviations.

Issue Changes *(Dev**SecOps** Engineer)*
Issue change(s) to correct the deviations from the Technical security baseline.

Implement Changes *(Dev**SecOps** Engineer)*
Implement changes to correct the security baseline deviation.

Request Customer RAA *(Product Owner)*
A signed Risk Acceptance Agreement must be created when a Customer does not want to implement the advised Technical security baseline setting(s) (see Risk Acceptance process 5.12.1).

Mandatory evidence for Technical Security Baseline
- A report of the security baseline compliance must be available on at least a monthly basis (both on shared as well on per customer)
- Each unit reports trends showing the level of baseline compliancy and the progress over time.
- Evidence from Revision history that Baselines have been reviewed yearly (document control)
- Evidence of the deviation analyses must be available monthly
- Changes which are initiated by the process must able to retrieve
- Overview and details of the created RAA's

5.5 Security Incident Management

The following types of security incidents can be distinguished:

1. Service specific: (e.g. DHC Service, DCS Service). These security incidents originate often from automated security monitoring and logging (see next chapter) and relate to a single service. These are usually coordinated, recorded, and tracked through ATF, resolution follows the rules for incident management. Generally, the Computer Security Incident Response Team (CSIRT) is not involved in the resolution.
2. Security incidents not automatically detected by tooling which may affect multiple services delivered to multiple customers. These incidents are also usually coordinated, recorded, and tracked via ATF. Involvement of CSIRT depends on the possible impact.
3. Generic security incidents (not service related). Those do not directly affect a service to a customer. The GBU Chief Security Officer coordinate these security incidents

All three categories of security incidents can be promoted to major incidents via the standard procedures when required. When high risk security incidents cannot be resolved timely via the standard incident management process Atos CSIRT can be involved for further management. Involvement can be arranged via the assigned Quality, Security and Compliance Officers of the Practice/GBU.

In every AST for every customer a CSM (Client Security Manager) must be assigned. It is his task to define and execute together with the customer, based on Atos best practices, the breach notification process. The CSM is not part of the CES organization, although the two Practices will support the CSM e.g. for other processes such as Risk Acceptance.

In all cases reports on the security incidents must be available.

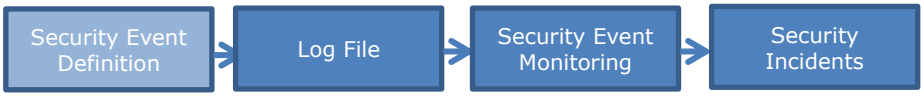
5.6 Security Monitoring & Logging

The goal of Security Monitoring and Logging is to timely detect malicious activities on the infrastructure and applications and to ensure that data for forensic investigation remains available.

Definitions & agreements

- Each Service must have an overview of security incidents (per technology layer) relevant for that Service; All components in the cloud service must send logging to the central (security) monitor solution of that Cloud Service from where incidents will be forwarded to ServiceNow.
- Monitoring must be implemented for the list of identified security events created during development. The minimum base is the security events defined in the Atos Information Security Policy ASM-SEC-0001 which can be found on the Atos Security Library; For every service monitoring must be implemented based on best practice and not limited to the events defined in the Security Policy.
- Where possible, event logs should record whether or not personal data has been changed (added, modified or deleted) as a result of an event and by whom. Log information should be deleted within a specified and documented period.
- Security incidents are recognizable in ATF by setting at least one of the three fields Confidentiality, Integrity, and/or Availability;
- Operational security incidents are handled via Incident Management;
- Security incidents not related to a specific Service or affecting Atos must be reported according to the Atos global security incident guideline;
- When requested, log files should be made available to customers if disclosure is within acceptable risks and access to the specific logs is strictly controlled.

5.6.1 Flow chart step descriptions



Security Event Definition, Log File, Monitoring and Incidents

This flow is expected to be fully automated and as a result of a security event it has to generate an ATF Incident request. This request will be handled according regular Incident Management procedures.

Mandatory evidence for Security Monitoring and Logging

- Overview of defined security incidents must be available
- Log files containing the selected log events must be kept for a minimum period of 12 months
- Reports of security incidents in ATF must be available

5.7 Antivirus Management

The goal of Antivirus Management is to protect systems from virus and related hacking threats.

The implementation fulfils the requirement that originate from the ISO27001 standard and the ITCF control **LS-13 Logical Security – Antimalware**.

- Antivirus software must be installed on systems commonly affected by Malware (e.g. Windows and Linux systems)
- Virus signatures must be kept up to date

- Regular checks must be executed that the Anti-Virus software is still active and added to the production plan.
- In case of anomalies, e.g. sudden higher volumes of viruses or viruses which require manual intervention for removal, a security incident should be registered in the requesting system

Mandatory evidence for Antivirus Management

- Overview that signatures are still current
- Overview that of required systems that antivirus software is current and still active
- Security requests when required.

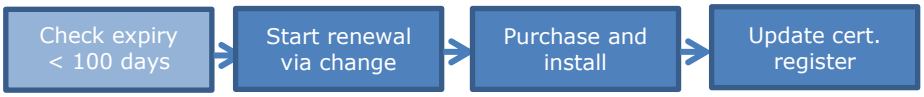
5.8 Security Certificate Management Process

The goal of Security Certificate Management is to ensure continued availability of services by means of timely renewal of certificates.

Definitions & agreements

- For every service a register must be maintained, or a central register used, which contains all used certificates, the purpose, the expiration dates and renewal dates
- A monthly check on security certificate expiration must be included in the Production Plan
- The certificate renewal process must be initiated 100 days before expiry of the certificate
- Public Certificates are required for Internet or Customer Facing services
- Public Certificate can have a maximum lifetime of **xxx** years
- Private (self-signed) certificates are allowed when closed environments not exposed to internet or customers.
- Private Certificates can have a maximum lifetime of **xxx** years
- Every Service must have a defined Standard Change for certificate renewal, including CIP and Workflow

5.8.1 Flow chart step descriptions



Check expiry *(Dev**SecOps** Engineer)*
A monthly check of the certificate register must be executed where certificates which will expire within the next 100 days must be selected for renewal.

Create change *(Dev**SecOps** Engineer)*
Issue a change request for certificates renewal. A standard change should have been defined for certificates renewal.

Purchase certificate *(Product Owner/Service Responsible Manager)*
Ensure that the required certificates are purchased and timely made available to the operations engineer.

Install Certificate *(Dev**SecOps** Engineer)*
Install the renewed certificates according to the work instructions as defined in the change request.

Update Certificate register *(Dev**SecOps** Engineer)*
Update the certificate register in order to reflect the new expiry date for the renewed certificate.

5.9 Encrypted Communication

All web communication must be encrypted with strong encryption methods. Weak encryption is not allowed.
Secure Socket Layer (SSL) is a generic name for the protocol used for secure communications between two systems. There are five protocols in the SSL/TLS family: SSL v2, SSL v3, TLS v1.0, TLS v1.1, and TLS v1.2. The older versions are known to contain deficiencies:

- SSL v2 and SSL v3 MUST be switched off on all systems and interfaces
- TLS 1.0 is recommended to be switched off. It MUST be disabled on systems handling sensitive data or performing critical operations over internet

Within the encrypted protocols Cipher Suites are used. A cipher suite is a named combination of authentication, encryption, authentication code and key exchange algorithms used to negotiate the security settings for a network connection.

In order to ensure that only strong cryptographic ciphers are used the systems MUST be configured to disable the use of weak ciphers and to configure the ciphers in an adequate order (the strongest ciphers at the top). In any case, at least the following Ciphers must be disabled:

- Disable cipher suites that do not offer encryption (eNULL, NULL)
- Disable cipher suites that do not offer authentication (aNULL). aNULL includes anonymous cipher suites ADH (Anonymous Diffie-Hellman) and AECDH (Anonymous Elliptic Curve Diffie Hellman)
- Disable export level ciphers (EXPORT are legacy weak ciphers that were marked as exportable by US law)
- Disable ciphers using DES
- Disable the use of SHA1 and MD5 as a hashing mechanism
- Disable the use of IDEA Cipher Suites
- Disable RC4 cipher suites

5.10 Network Vulnerability Scans

The goal of Network Vulnerability Scans is to detect security risks on Internet Facing infrastructure or on the Atos Service Network (ASN).

The implementation fulfils the requirement that originate from the Cloud Security Policy and ISO27001. In 2020 a new Global Vulnerability Management (GVM) scanner (Tenable) was introduced and all ATOS owned IP addresses on internet and in the Internal Service Networks must be scanned on vulnerabilities.

Definitions & agreements

- Network Vulnerability Scans are performed regularly to check whether an IT component is vulnerable from attacks over the network. In view of the increasing number of attacks that are carried out over the network, these scans are becoming increasingly more important;
- Network Vulnerability Scans are performed on the Internet Facing Infrastructure (IFI) as well as on the Atos Service Networks (ASN);
- All ATOS owned Cloud Services Internet Facing IP addresses must be included in the vulnerability scanners. (must be added during new service implementation (TOS/TOP));
- All Cloud services IP addresses facing towards the Atos Service Network (ASN) must be included in the vulnerability scanners;
- All recorded IP addresses in the vulnerability scanner must be added to the Tenable Asset Group of the supporting the Practice and maintained by the Quality, Security and Compliance Officer. This will enable Cloud dedicated reporting and control;
- The Internet Facing Infrastructure (IFI) and ASN scans run every week; Execution of these scans is coordinated by Atos Global BDS;
- Vulnerabilities are classified Critical, High, Medium and Low.

- All Critical and High vulnerabilities must be eliminated; Vulnerabilities with a medium and low rating must be mitigated next.

Issue change to mitigate *(**DevSecOps** Engineer)*
Take the vulnerabilities from the GVM report and issue changes to mitigate those vulnerabilities or follow up with owners.

Implement Change *(**DevSecOps** Engineer)*
Implement changes to mitigate vulnerabilities or follow up with owners.

Mandatory evidence for Network Vulnerability Scans
- Changes requests for mitigation stored in ATF
- Analyses and status of the internet facing vulnerabilities
- Analyses and status of the vulnerabilities in Atos network (ASN) facing IP-addresses
- Provide an overview of internet facing IP addresses in the vulnerability scans
- Provide an overview of internal networks addresses in the vulnerability scans

5.11 Add devices to the Atos Service Network

The goal of the process to add devices to the Atos Service Network is to ensure that no new vulnerabilities are introduced on critical Atos Infrastructure

The process is described in the procedure Adding devices to the ASN: MSD-U02-0020 - Adding devices to the ASN

Definitions & agreements
- The process is required as a mandatory process by Atos Global Security (RACG)
- It is applicable for any type of device connected to the Atos Service Network by Cloud Services
- An approval of the Global Security and Compliance Officer is required to be requested via the functional mailbox (see procedure)
- The IP-address of the device must be included in the appropriate Asset Group of GVM (Tenable) to ensure continuous reporting of vulnerabilities

5.12 Risk Management Process

The objective of this risk management process is to ensure that risks which threaten the Cloud Service which ATOS delivers to customers are visible and managed at an appropriate level. Risk management provides a systematic method for identifying major risks and removing them where possible, or otherwise adopting all the control measures and precautions that are reasonable and practical in the circumstances. The Risk Management process for Global Cloud Services is described in MSD-U02-0025.

Definitions & agreements
- For customer risks as risk letter must be send to the customer and recorded in the Atos ART tool; The various input fields must be used in the way and with the name convention described in the Risk Management Process.
- Global Risks (not dedicated to one customer) are registered in the internal risk register.
- Global Risks are reported to RACG.
- A formal review should occur at least quarterly in a dedicated Risk meeting with relevant members of Core MT:

- Monitor implementation dates on action plans to assess if work planned is on target
- Add new risks that have emerged
- Change the risk rating of risks that have been successfully reduced
- Monitor the overall ongoing progress towards risk reduction
- Ensure stakeholders are informed of risks identified

5.12.1 Risk Acceptance Agreement for Customers

The goal of a Risk Acceptance Agreement is to transfer legal risks, which are a result of customer decisions to deviate from Atos guidelines and advices, to customers.

The implementation fulfils the requirement that originate from the ITCF controls are initiated from other processes which have the ITCF relations described.

Risks related to deviations from security standards (e.g. deviations from Security Baselines, patch advices or Atos security policies) resulting in a lower security level must be registered in the Global Atos Risk Tool (ART) and communicated with and understood by the Customer.

Definitions & agreements

- Deviations from security standards (e.g. deviations from Technical security baselines, patch advices or Atos security policies) resulting in a lower security level must be formally accepted by the Customer via a signed Risk Acceptance Agreement (RAA). The registration of the risk must be done in the ART tool;
- Deviations from contractual agreements which result in significant risk on service delivery may also require a RAA;
- The ART tool contains the repository of the risks and the status of the acceptance;
- The Client Security Manager (or the SDM if no CSM appointed for the customer) is responsible for managing the risk, defining the criticality of the risk and the communication to the customer.

Prepare RAA *(DevSec**Ops** Engineer)*
The DevSecOps Team prepares the RAA, with an explicit description of the risk related to the deviation from the security standard. The SRM approved RAA is entered in ART.

Customer signs RAA *(Client Security Manager)*

- The Client Security Manager defines the criticality of the risk and decides whether the risk can be accepted internally or needs to be accepted by the customer. Note: for shared components of the shared cloud services the CSM does not define the criticality of the risk.
- During the period that the RAA is not yet signed, the Client Security Manager keeps in contact with the Customer and maintains records, preferably in meeting minutes, to ensure that the
- Customer is aware of the risks.
- The Client Security Manager maintains the status in the ART tool.

Mandatory evidence for Risk Acceptance Agreement

- RAA reported from the ART tool per service
- Internal Global Risk Register.

5.13 Software as a Service (SaaS) Management Process

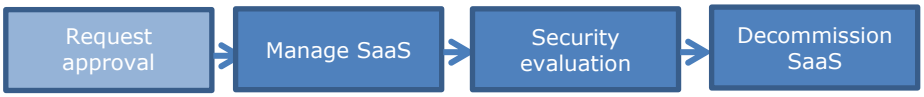
The goal of the SaaS Management process is to manage all external Cloud (IaaS, PaaS, SaaS) based services that are engaged by Atos Business Unit(s) to provide services. And to ensure that Vendor is providing the External Cloud based Services from a secure environment (physical, logical, network, etc.).

The implementation fulfils the requirements that originate from the policy "Policy on using external based cloud solution".

Definitions & agreements

- Global IT or Global Operation is made aware of the Atos Business Unit's intention to engage the Vendor for External Cloud based Services.
- Atos Business Unit MUST seek approval of Global IT/Global Operation for engaging the Vendor to utilize their External Cloud based Services.
- Global IT or Global Operation gets the opportunity to evaluate the Service and/or Vendor from IT Landscape fitment perspective. Global IT or Global Operation also gets the opportunity to evaluate the Service and/or Vendor from a Security perspective. Atos Information Security Policy and Atos Security Requirements for Partners and Suppliers SHOULD be the baseline for evaluation. Alternative solutions / Vendors may be proposed by Global IT or Global Operation.
- Every SaaS must be integrated with the operations processes and compliant to ATOS Policies:
  - Access management as described in chapter 5.3, User Authorization Management.
  - ITSM as described in chapter 4.7, Change Management.
  - Monitoring
- Any Public Cloud Solution that Atos Business wants to use for its employees must enforce Atos 2FA authentication or an alternative 2FA authentication validated by GIT/Global Operation and Group Security. For public Cloud solutions limited to small number of users (e.g. 50) and for which the provider can't enforce the 2FA, an exception may be granted by Group security.
- Any specific criteria / control that Global IT/Global Operation wants the Vendor to implement can be identified to the Functional Owner.
- Global IT/Global Operation maintains a list of all the external Cloud Services / Vendors approved by the Security Officer of Global IT/Global Operation.

5.13.1 Flow chart step descriptions



Request approval to Global IT *(Product Owner)*
Product Owner must request the approval from Global IT to the functional owner including the cloud Security Evaluation (for multiple deliveries). Or request approval to Global IT with the Cloud Security Evaluation.

Manage SaaS *(**DevSecOps** engineer)*
For the execution of operational processes the Product Owner is accountable. Below process must be executed compliant to the ATOS policies during "Manage SaaS":

- Access management as described in chapter 5.3, User Authorization Management. Service Delivery processes (please see Chapter 4)
- Monitoring
- Hardening

Security Evaluation *(Product Owner)*

The Vendor MUST provide a periodic (at a minimum annually) / event driven assurance in form of a formal written communication, sharing of security reports.

Decommission SaaS *(Product Owner)*

In the event it is decided to cease taking the services from Vendor; adequate controls should be implemented to ensure secure closure.
The secure closure of services will include (but not limited to):

- Return of Data by Vendor which is specific to Atos Business Unit
- Removal of any documentation from Vendor's environment related to Atos Business Unit
- Removal of instance / configuration by Vendor which is specific to Atos Business Unit
- Removal of access by Vendor for Atos Business Unit to Vendor's environment

6 Monitoring – (Management) Controls

6.1 Controls (monitoring)

The goal of management process monitoring is to maintain compliance to legislation and applicable standard by means of management ownership and continuous improvement.

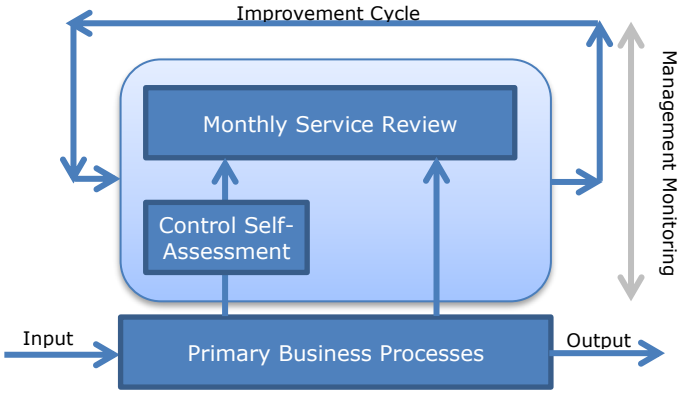
The implementation fulfils the requirement that originate from the ISO27001 standard and monitoring of ITCF controls Service Review including Compliance Self-Assessment.

In order to be able to monitor the processes for Cloud Services a Control Self-Assessment (CSA) is implemented. The results are incorporated in the monthly services reviews where the status and improvements actions are discussed.

Definitions & agreements

- 'IT compliance' is the adherence to legislation and applicable IT framework standards. It deals with working according to standards and regulations; e.g. Cloud Security Policy, Sarbanes-Oxley (SOX) law, privacy law;
- The ISAE 3402 standard requires a "written statement of assertion". The assumption is that Management of a Service organization effectively utilizes "monitoring" as a key principle in assessing the effectiveness of IT controls;
- The compliance self-assessment procedures (CSA) are used to support the audit readiness and preparation for ISAE3402 audits. This is done by means of a self-assessment by management for major delivery and security processes. The goal is to create ownership at management level for the correct execution of these processes;
    - This ownership is enforced by means of electronic monthly signatures by the Service Responsible Manager in the Compliance Self-Assessment tool (CSA). When processes are not at the expected level, management must take actions in order to get back in control.

The results of the CSA and SLA Results are incorporated in the monthly services reviews where the status and improvements actions are discussed and recorded.



Mandatory evidence for Service Reviews

- Signatures by the Service Responsible Manager in the Compliance Self-Assessment tool
- Service review PowerPoint presentation document available on the Quality Records Environment. This document contains KPI's for Customer Satisfaction, Service Operation, Service Change and Service Assurance. Service Review Template to be found here
- Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.

- Recorded action points maintained during the service reviews in the Service Review documentation

6.2 Document Control

The goal of Document Control is to setup and manage a Document – and Record Management system to comply with ISO requirements.
Control of Documented Information Process is part of business lifecycle and Atos Integrated Management System (AIMS). It belongs to Governance Risk and Compliance (GRC) activities, which are embedded in each Key Transversal Process defined by Atos Group.

Definitions and Agreements

- Document control is based on the Atos control of documented information process;
- A document can be a controlled document or an evidence document:
    - **Evidence** is documentation which represents a status of a fixed timeframe. Documents are not re-used anymore (e.g. reports, checklists, TOS checklists etc.). Documents are written/created only once and will never change.
    - **Controlled Document** is documentation which is re-used by multiple persons and need proper control on changes. (e.g. procedures, work instructions, designs etc.);
- There are two levels of controls for controlled documents:
    - **Standard control**
        - Recommended registration in a list of project or service documents
        - Unique identification (title/ file name)
        - Version control (e.g. SP versioning)
        - Ownership indicated (individual person, function/role, unit, etc.)
        - Reviewed for adequacy prior to use
        - Security classification
        - Document (release) date
        - Reviewed as per needs (so standard controlled documents will never be overdue)
        - Compulsory storage in EDMS
        - Atos office template should be used, if not, Atos brand rules must be followed.
    - **Strict control**
        - Mandatory listing in the master index
        - Unique identification (title/ file name and Document Reference)
        - Strict version control (indicated in master index and in the document)
        - Named individual document owner
        - Reviewed for adequacy prior to use
        - Approved for adequacy prior to use
        - Security classification
        - Document (release) date
        - Reviewed ≤ 2 years (next review date indicated in master index)
        - Compulsory storage in EDMS
        - Atos office template should be used, if not, Atos brand rules must be followed.
- Both standard and strict controlled documents are managed by the Document Controller.
- Documents managed under standard control are stored in the Cloud Services Document Library on SP or on the Cloud Version Control System;
    - Cloud Version Control System requirements:
        - Versioning option available
        - Publishing procedure agreed with Document Controller
        - Clear access options
        - Readable format for documents
        - Clear work instruction on how to find documentation.
- Documents managed under strict control are published in the Published Storage following the steps under Document Management SP location.

- The owner of the document decides what is the type of control needed for the document. It must be applied if it contains shared, need-to-know information that requires version control;
- Evidence documents are stored on each service's Quality Records SP space, accessible via the Quality Records Environment. Quality Records Environment can be represented by the following locations, depending on the service: Global Cloud Services Homepage, CES Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.
- Note that there is a distinction between Service specific documents (named MSx-Sxx) and Unit generic documents (named MSx-Uxx). Only use generic document ranges when you document covers multiple services;
- Always use the latest Atos PowerPoint -, Excel - and Word templates available on the Communication Toolkits site;
- Never change macro settings and/or fieldnames of the template;
- Documents under strict document control must be reviewed by default within 2 years after publication unless a different period is agreed upfront;

Signature convention

- Signatures (for standard depending on the owner, for strict is mandatory) on documents authorizes content for official usage and evidence of approval;
- Official Management documents such as Strategies, Policies and Procedures (xx**M**-xxx-…. and xx**P**-xxx-….) must be signed by the Document Owner, the QA function (Document Controller) and as many reviewers as the owner deems necessary;
- Both strict and standard controlled documents can include the table with approvals/signatures – as per Document Owner's decision
- A signature always consists of the name in print, the signature and the date of signing;
- Use the Word template sign block to collect signatures for approval;
- Approvers sign the document in ascending order of authority: first all reviewers, then the QA function, then the document owner and finally the senior Manager(s) (if applicable);
- Approvers can approve documents with electronic signature or by e-mail. E-mail approval to be documented and represented by Document Control in the official document by adding "approved by e-mail" note.
- Original e-mails with approvals are stored by the Document Controllers together with the electronic versions of the document, preferably in PDF format.

Create Document *(Anybody)*
Fill in: title, document number, version, status, document date, owner, and security classification;
Write the content and update the change list;
Deliver the document for review and approval.

Publish Document (Document Control)

STANDARD CONTROL
The Document Control team will publish your documents in non-editable PDF format (for Word docs) as follows:

- For Service/Product documentation please send an email to CSESO-Doc-Control-requests@atos.net (instead of raising a ticket via SDM) and attach completed Doc Control Request Form
- For Unit documentation raise a request via ServiceNow and use Service catalog -> Atos Internal Service Catalog -> Doc Control -> Generic service request

STRICT CONTROL

- For document under strict control follow the steps under Document Management SP location.

Inform Target Readers *(Document Author)*
Inform your target readers about new or changed version of the document.

Mandatory evidence for Document Control
Document control process, per service, documented and aligned with the Document Controller. All documents which required document control stored on the right location agreed in the defined process.

6.3 Training, Qualification and Certification

The goal of Training, Qualification and Certification is to ensure a high quality of service with appropriately skilled staff.

Definitions and Agreements
- The Product Owner is accountable for the training and qualification of his employees;
- Employees must be qualified for their role or function;
- Each DevSecOps team maintains a training plan that defines the training requirements for its employees and a training registration sheet as evidence;
- An annual qualification check must be held to ensure that all employees are still qualified;
- The training plan must be evaluated annually;
- If a trained subject has changed, employees need to refresh their qualification status, e.g. in case of new releases. This is based on an impact / risk analysis;
- The training and qualification of employees is regularly audited;
- Work instructions should contain the required qualifications to execute a task;
- The Product Owner use the staff qualification status for the scheduling of work;
- Training agreements are documented in the individual development plan (IDP).

Available Process training material
- Security Awareness training available on My Learning for all staff (Mandatory).

Mandatory evidence for Training, Qualification and Certification
- Unit training plan & training registration sheet
- Stored evidence of annual qualification check

6.4 Employee Screening

Reliability and integrity are the key elements for Service supply to our Customers. Atos has a standard (pre-employment) screening procedure for all employees and, temporary resources working on behalf of Cloud Services.

Definitions and Agreements
- Pre-Employment screening must be executed in accordance to the Atos generic policy
- This procedure is executed only with written permission of the employee involved:
  - Check on the correctness of the Curriculum Vitae;
  - Check on identity papers, degrees, certificates;
  - Reference check at former employers;
  - Check governmental waiver for good behavior.
- In all cases, the Contract manager is accountable for additional screening to be performed in the scope of the contract;

Mandatory evidence for Employee Screening
- Registration of the screening documents (confidential) in line with local country policies

6.5 Quality Management and Audits

Structure and trends

The Control Self-Assessment (CSA) is used to monitor quality, security and compliance of a service over time.

- The KPI's (scores) in the CSA tool must always be based on evidence. And evidence to be used in audits.
- Evidence must be recorded in the Cloud Services Quality Records Community as defined in the DevSecOps Manual.

6.5.1 Atos Integrated Management System (AIMS)

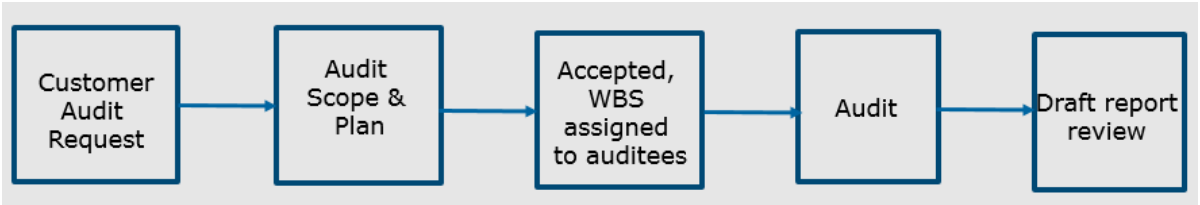
- The AIMS defines the Atos Governance and contains a Management System Manual (MSM) and a Management System Overview (MSO). The Quality Management System (QMS / ISO9001) and Information Security Management System (ISMS / ISO27001) are described in the MSO and are the basis for our Global ISO multi-site certification. The GBU MS MSO defines how MS is organized and how it is managed. All units have to comply with this MSO.

6.5.2 ISO and Compliance Audits guided by the yearly global program

- The Atos **IT Control Framework** describes the most important steps in the (ASMM) processes and is used as basis for audits. This Operations Manual covers all relevant controls of this framework;
- **External ISO auditors** execute, on a regular basis, a **surveillance audit** on the ISO9001 (quality) – and ISO27001 (security) multi-site certificates;
- **Generic compliance audits** are conducted by independent third party auditors and result in a formal (**ISAE3402 or SSAE16) Generic assurance report** for customers. Relevant controls from the Atos IT control framework are audited. Documented evidence has to be provided to proof that Atos is in control of the operation of the Customer IT infrastructure;

6.5.3 All other (Customer) Audits

Every other audit not being part of the yearly overall program has to be agreed upon upfront. These can be customer requested audits, audits as defined in contracts and also other internal audits. Examples of these audits are PCI-DSS, Pentesting, Hi-Trust or a customer agreed framework.



Related to these types of audits de following rules apply.

- Audit costs are never part of the service. These costs - including the costs of the operational teams for evidence requests, interviews, explanation, result review, etc – will be charged on a WBS which must be made available before any audit activity starts;
- In order to execute an audit for a service the agreed framework must be implemented. E.g. a PCI audit can only be executed if during implementation the controls were implemented in operation and the additional operational activities agreed and priced;
- Before an audit start an audit plan must be provided. This audit must contain the scope of the audit consisting of the description of the audited services or parts thereof, the controls which will be audited and the audit timeline;
- This audit plan must be accepted by a representation the Cloud Services Core Management Team.

6.5.4 Audit findings

- **Deviations** from the prescribed way-of-working are called **"findings"**;
- Findings are **classified** with
    a) finding **impact** (high, medium or low),
    b) finding **conformance** (major nonconformity, minor nonconformity or observation) and
    c) a **target resolution date;**
- Findings are **assigned** to Service Responsible Managers (also known as Finding Responsible Manager) and, when accepted, registered. The SRM is **accountable** for the timely and accurate resolution of the assigned findings;
- A finding **resolution plan** how to resolve the finding should be available within 2 weeks after registration of the finding;
- A Finding is **completed** when all assigned **actions** are closed;

Mandatory evidence for Quality Management and Audits

- All Audit and assessment reports