EVIDEN

For internal use

Operations Manual

Author(s)	:	**Gabriel Munteanu, Andrada Roman, Sophie Bertrand, Ralf Thomas, Aljosja Molenaar, Parag Deshpande, Pawel Korpowsky**
Document Number	:	**MSD-U02-0028**
Version	:	**1.0**
Status	:	**Final**
Source	:	**Eviden**
Document date	:	**20 October 2023**
Number of pages	:	**99**

Role	Names
Reviewers	Nicolas Tailhardat, Pankaj Bhadana, Vivek Jindgar, Rakesh Kumar, Josep Rodo, Steve Lawrence , John Cipolla, Simon Withers, Steve Midgley, Pawel Korpowsky, Magdalena Krajnik - Jaworska
Approvers	Santi Ribas, Rakes Kumar, Magdalena Krajnik - Jaworska
Document controller	Dorota Skonieczna
Document owner	Santi Ribas

Approver Name	Approved
Santi Ribas	20.10.2023
Rakesh Kumar	20.10.2023
Magdalena Krajnik-Jaworska	20.10.2023

Contents

List of changes

Version	Date	Description	Author(s)
0.1	10.10.2023	Copy of DevSecOps manual	Gabriel Munteanu
1.0	10.10.2023	CES practice name was replaced by OneCloud. Communication tool name was removed from the MIM process. Global Capacity Manager role removed. Removed capabilities and enablers from Scaled agile framework Removed L4D description Added Service Transition Manager and Project manager roles description Scope of document reworked to include BDS ; definition of devsecops removed Replaced L4d with Service Description Replaced Devsecops engineer with Operation engineer Removed workplanner role Replaced pro-active problem manager with normal problem manager description Adjusted process manager and major incident manager roles Added availability management CAPC link changed Added availability Management Service Transition chapter was added Project Management chapter was added Incident Management flow updated Updated Risk Management chapter Updated User Management chapter “Request Fulfillment and Configuration Management” updated as “Configuration Management”	Gabriel Munteanu

1 Introduction

This document defines the common way of working in the OneCloud organization and is used as a process reference for BDS Cybersecurity Services Global Delivery Organization. It is based on the following standards and with input from the following sources:

- **ESMM** (Eviden Service Management Model) which is extended towards the operational use of the processes.
- **ITCF** (Eviden IT Control Framework) 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")
- **Eviden Security Policy** which provide the framework for the security processes
- **COBIT 2019**
- **SAFe (Scaled Agile Framework)**
- **Norea DevOps study report**
- **ISACA controls** (Information Systems Audit and Control Association)

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

1.1 Scope

This Operations Manual is **mandatory** for all contracts and all teams within OneCloud .

For BDS Cybersecurity Services Global Delivery Organization applicable are chapters:

- 4 (excluding 4.1; 4.5; 4.7.5; 4.9)
- 7.6 & 7.7

*Out of scope

Out of scops are the Customer contracts where is clearly documented that Eviden OneCloud/BDS are obligated to use Customer processes or Eviden processes which need to be customized.

1.2 Target Audience

Group	Objective
Management and all Operational staff within OneCloud	To use the daily execution of the Operation and Development 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.
BDS Cybersecurity Services Global Delivery Organization	To simplify and streamline all the ESMM Processes to use in the daily execution and improve 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

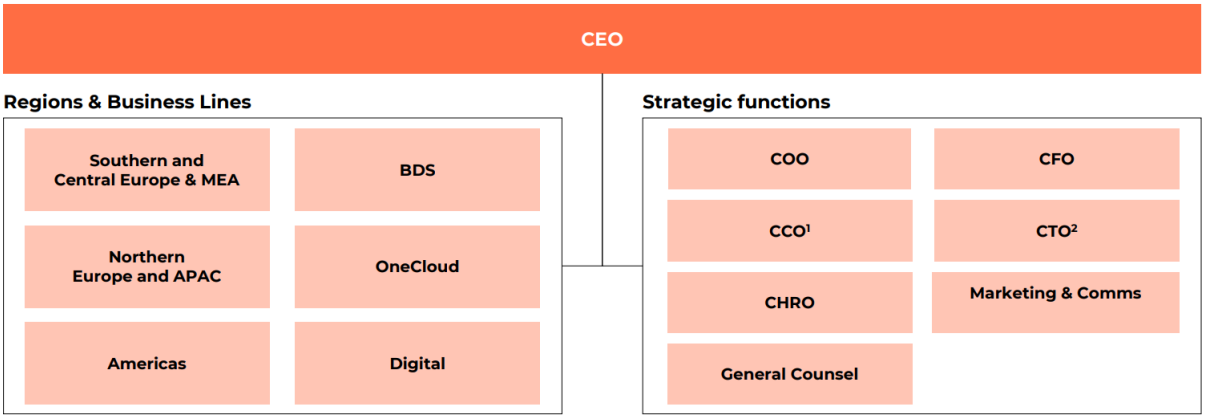
2.1 Organization and Roles

2.1.1 Organizational Setup

The Atos Group announced its intention to split its digital and big data businesses into two separate listed businesses in terms of technology activities in order to foster the development of company value. The split will result in two separate entities (new Atos Tech Foundations and Eviden) Atos tech foundation has become a private company. The split is expected to be completed by End of 2023.

Eviden is a global company that operates in three regions (RBU), three business lines (BL) and various strategic functions. This manual describes the policies and procedures for the Business Line of OneCloud and Big Data and Security (from hereof BDS), which provides cloud-based solutions to clients across all 3 Regions (RBU) and the Global Delivery Center (GDC). The manual covers the roles and responsibilities, quality standards and processes across Business Line OneCloud and BDS to be compliant with regulatory requirements of ISO and the Eviden internal IT-Control Framework.

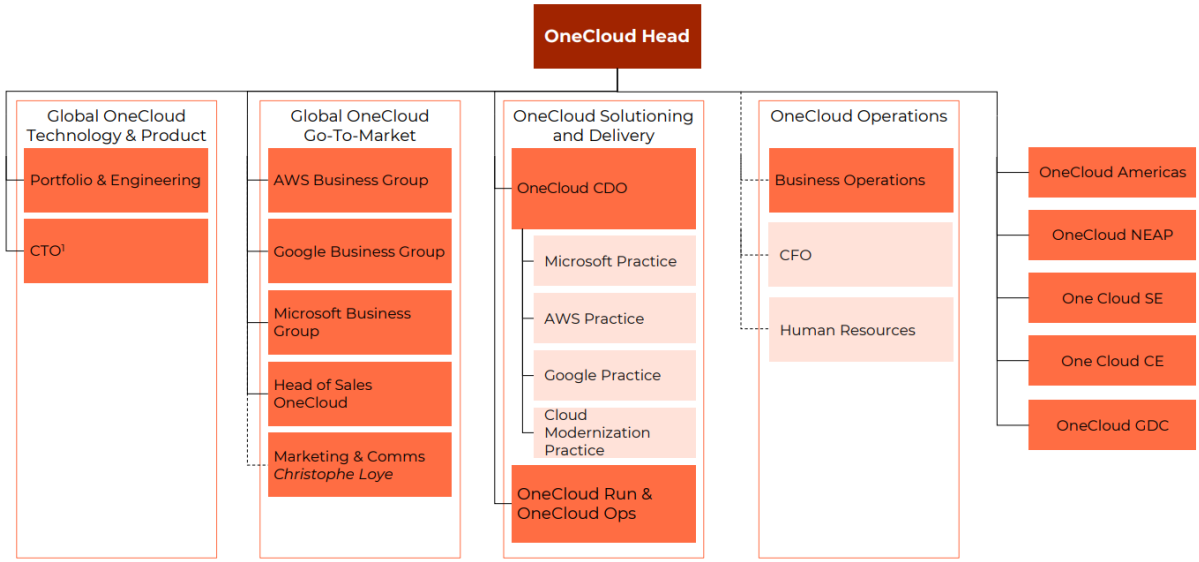
Eviden Day 1 organization – CEO N-1



Business Line OneCloud provides end-to-end cloud solutions for our customers across different regions and industries. We have four main functions within OneCloud: Technology & Product, Go-to-Market, Solution & Delivery and Operation. We also have four regional business units (RBUs) and three global delivery centres (GDCs) in India, Poland and Romania. The RBUs are responsible for account management, deal solutioning and sales management. The GDCs are responsible for delivery resources and staffing strategy. The global functions are responsible for developing and executing the Technology-, Product-, Solution-, Delivery- and Go-to-Market strategy in cooperation with the RBUs and GDCs. The Go-to-Market Organization is organized in Business Groups, which are aligned to our 3 main Hyperscaler Partner Microsoft, Amazon Web Services AWS and Google. The global Solution and Delivery function is organized in four Practices that align with our three Hyperscaler Partners: Microsoft, AWS, Google and the Practice Cloud Modernization.

Cloud Operation is responsible for supporting customers in daily operation in all our Cloud Managed Service Portfolio.

Eviden Day 1 organization – OneCloud



Microsoft, Azure, Google and Cloud Modernization are four practices that span across all Regional Business Units (RBU) and Global Delivery Centres (GDC) of our organization. These practices enable us to deliver innovative solutions and services to our clients, leveraging the latest technologies and best practices in the cloud domain.

Details regarding the organization can also be consulted on the official page under this link.

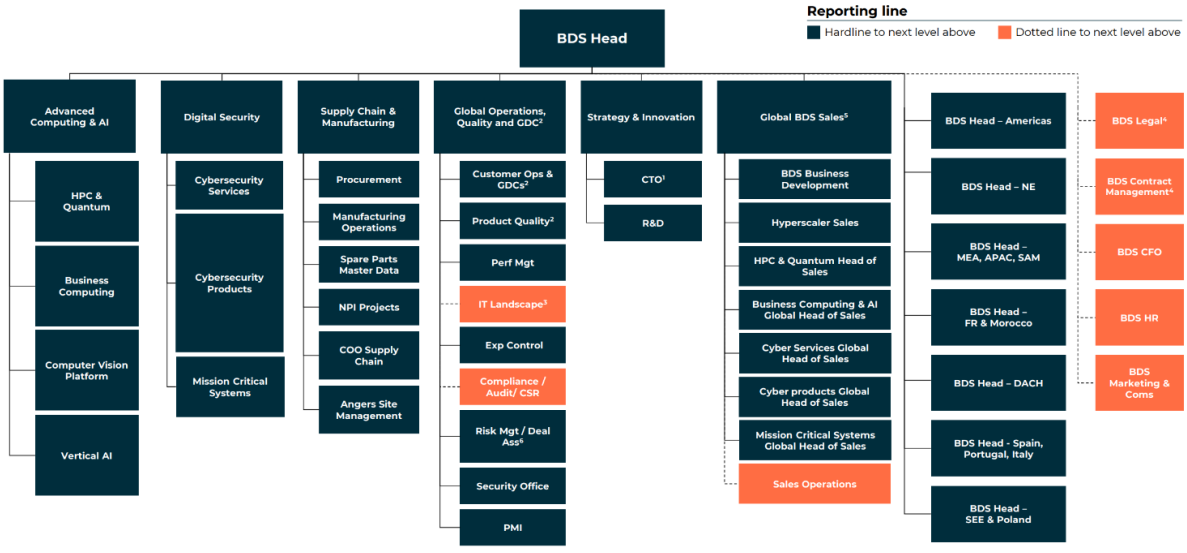
Eviden OneCloud – Target Operating Model

OneCloud				
Primary dimension / Secondary dimension	AWS Business	MS Business	Google Business	Cross OneCloud
General Mgmt, Transformation				General
Portfolio & Engineering, CTO Portfolio and Portfolio engineering development, incl. PMO				Portfolio and CTO
Marketing, Business Development & Global Accounts	GTM	GTM	GTM	GTM
Customer Solutions Design & Architecture	Design	Design	Design	Design
Customer Build PM, Transitioning & Transformation, Modernize, OneCloud Ready	Build	Build	Build	Build
Run CloudOps, Service Management, Escalation management	Run	Run	Run	Run

- Primary dimensions will include P&L reporting: OE, ER, PM and GM
- Based on the size of some geographies or strategy, some secondary dimensions can be empty or grouped if less than 5 people

Every Practice (Primary dimension) consists of main function "Go-to-Market", Design, Build and Run. All Run functions across Practices are organized in Cloud Operations.
The main responsibility of each Practice is to deliver solutions that meet the needs and expectations of our clients. This involves four main functions (Secondary dimension): Go-to-Market, Design, Build and Run. Go-to-Market is the process of identifying and engaging with potential customers, understanding their challenges and opportunities, and proposing value propositions. Design is the process of creating and validating the solution architecture, defining the scope and requirements, and planning the delivery. Build is the process of developing, testing, and deploying the solution, ensuring quality and compliance. Run is the process of maintaining, monitoring, and optimizing the solution, ensuring reliability and performance. All Run functions across Practices are organized in Cloud Operations, which provides centralized support and governance for cloud-based managed service business.
Portfolio is the function that oversees the design and delivery of OneCloud's core products and services for the global market. It works closely with CTO (Chief Technology Officer), the unit that sets the strategic direction of the portfolio based on market research and customer feedback.
The organization has defined and implemented quality gates for different types of deliverables, such as customer solutions, projects, new products and managed services. Quality gates are checkpoints that ensure the deliverables meet the agreed standards and requirements before they are transferred to the next phase or stakeholder. Quality gates help to improve customer satisfaction, reduce rework and errors, and enhance collaboration and communication across the organization.
Our teams are committed to delivering high-quality products that meet the needs and expectations of our customers. We ensure that all Practices (Primary dimensions) and all Functions (Secondary dimensions) are following the best practices of SAFe Agile framework and/or best practices of waterfall project management (like PRINC2 framework), depending on the nature and scope of each project.

Eviden Day 1 organization – BDS



BDS is structured in 2 Strategic Business Groups (SBGs), combining 5 complementary businesses to help customers with trusted intelligent platforms:

- **Advanced Computing SBG**, composed of 2 Global Business Lines (GBLs):

    - Business Computing: uniquely powerful High-End Servers and Integrated AI/Edge solutions (Servers, Software, Services) to compute massive data flows and turn them into business outcomes;
    - HPC & Quantum: Hybrid Supercomputing & Exascale, AI/ML Supercomputing & Quantum Computing for computing, digital simulation and Artificial Intelligence.
- Digital Security SBG, composed of 3 GBLs:
    - Cybersecurity Products: sovereign solutions for Identity and Data protection or IoT security and encryption;
    - Cybersecurity Services: consulting, integration, managed services to build continuous up-to-date extreme security and sovereign cloud solutions;
    - Mission Critical Systems: highly efficient mission systems (esp. leading the defense industry) for organizations that ensure the wellbeing of people, protection of nations and integrity of infrastructures. They particularly address homeland security, defense, energy, aerospace and transportation sectors.

BDS relies on R&D teams whose expertise is recognized internationally and strongly contributes to the development of Eviden technology portfolio, from infrastructures to smart data platforms and industry solutions. BDS relies on R&D teams whose expertise is recognized internationally and strongly contributes to the development of Eviden technology portfolio, from infrastructures to smart data platforms and industry solutions.

Detailed for BDS organization can be found here.

2.2 Introduction to Agile and SAFe

2.2.1 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.

2.2.2 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
- 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.

2.2.3 Minimal Viable Product

A Minimum Viable Product (MVP) is a product which contains the features required to enable the service described in the Service Description, 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 Development and Operation teams 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

2.2.4 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

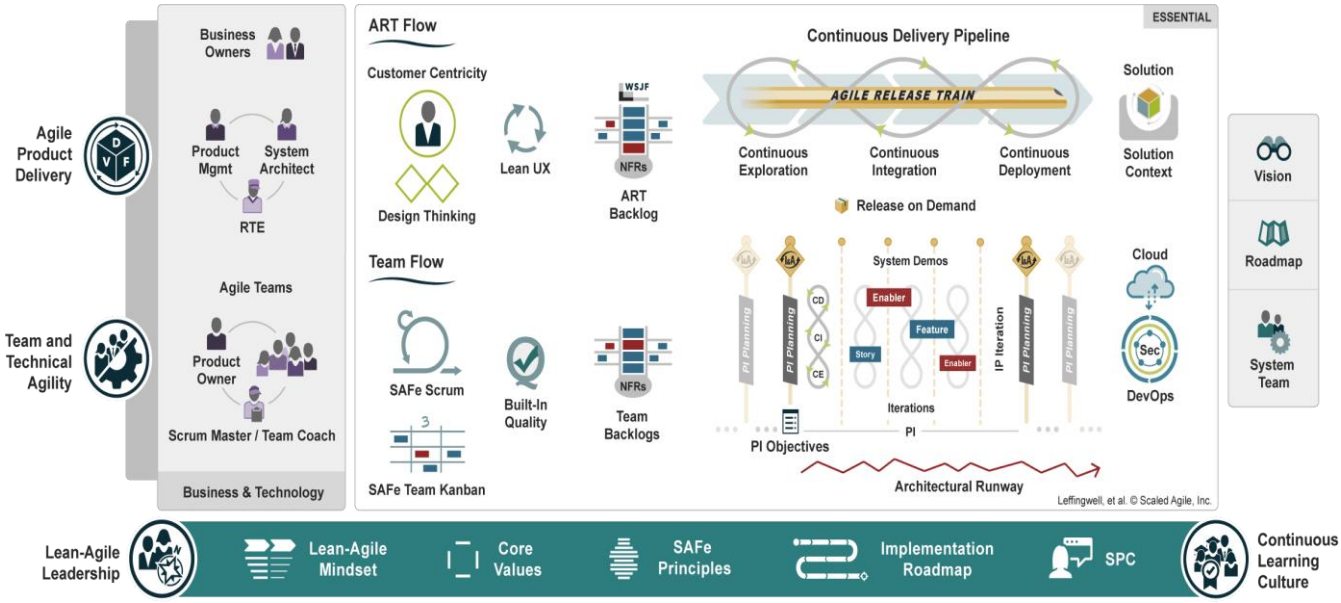
framework at all levels. The objective of SAFe is to create VALUE at the best quality by respecting the people and culture, having the right flow and optimizing sustainable value delivery, providing time and space for innovation and also taking in consideration relentless improvement.

The scalability of SAFE covers 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.

Program Backlog is the holding area for upcoming **Features** which are intended to address 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 behaviour 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	Non-functional Requirements (NFRs) define system attributes such as security, reliability, performance, maintainability, scalability, and usability. They serve as constraints or restrictions on the design of the system across the different backlogs.
Features	Feature is a service that fulfils 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 is 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.

2.3 Essential SAFe

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.

Operation Team

Product Owner
The Product Owner is responsible for defining user stories and prioritizing the team backlog, breaking down Portfolio Epics into Engineering feature. 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 development and operation teams 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.

Operation Engineer
The Operation Engineer writes and verifies code, fixes bugs, executes patch management, maintains asset and configuration repository and functions
He/she 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).

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 during design and build stages.

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.

2.3.1 SAFe Portfolio and Large Solutions

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 Service Description. 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

2.3.2 Other Roles

Global Process Implementation Architect
Responsible for the implementation of (technical) service management processes for all services.
Service Transition Manager
Responsible for the project management of Cloud Ops onboardings/off boardings. Coordinates the onboarding team and is ultimately responsible for taking contracts from signature to an operational managed service
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 OneCloud 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 OneCloud/BDS Process Owner

Responsible for defining processes based on Eviden (ESMM) 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 Operations 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.

Project Manager

- The Project Manager must plan, organize, and oversee the completion of specific projects while ensuring these projects are on time, on budget, and within scope
- The Project manager is responsible for defining the project scope, developing a project plan, and managing resources to successfully execute the plan
- Act as the primary point of contact for all project stakeholders & responsible for managing reporting/communication, risks, and changes throughout the project lifecycle.
- Decision-making authority within clearly defined boundaries and defined and documented scope of .
- Responsibility for structured communication in the project both to the project team of the own organization, as well as to the customer
- Continuous monitoring of SLAs/KPIs & enforcement of change processes
- ·Identification of open points/ deviations from the defined project scope and initiation of suitable measures
- Definition and coordination of external services of contractual partners
- Compliance with specified processes and methods
- Documentation of existing project results and experiences, review and / or lessons learned at the end of the project

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 centres (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 Centres.

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.

Problem Manager

Skilled technician which does pro-active and reactive 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 Operations

Concentrates on the definition and execution of Service Management Processes, based on ESMM.

Standard changes, Priority 1 incidents, Major Incident Management, Problem Management and Configuration Management. Also, responsible for assessing whether processes are executed according definitions.

. In the OneCloud Internal Contact List you'll find which services are already covered by OneCloud.

Major and Critical Incident Manager

Responsible for managing Major incident after incident has been promoted to Major Incident (MI).

For more information on the ESMM roles refer to ESMM 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 Business line Operations teams, in line with Eviden delivery standards, defined budged and planning.

Customer Landscape Owner (CLO)

End-2-end responsible for delivering Eviden services to a contract on technical integration of multiple Eviden services.

Client Security Manager

Every customer must have an assigned Client Security Manager in line with the Eviden 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.

2.3.3 Roles RACI

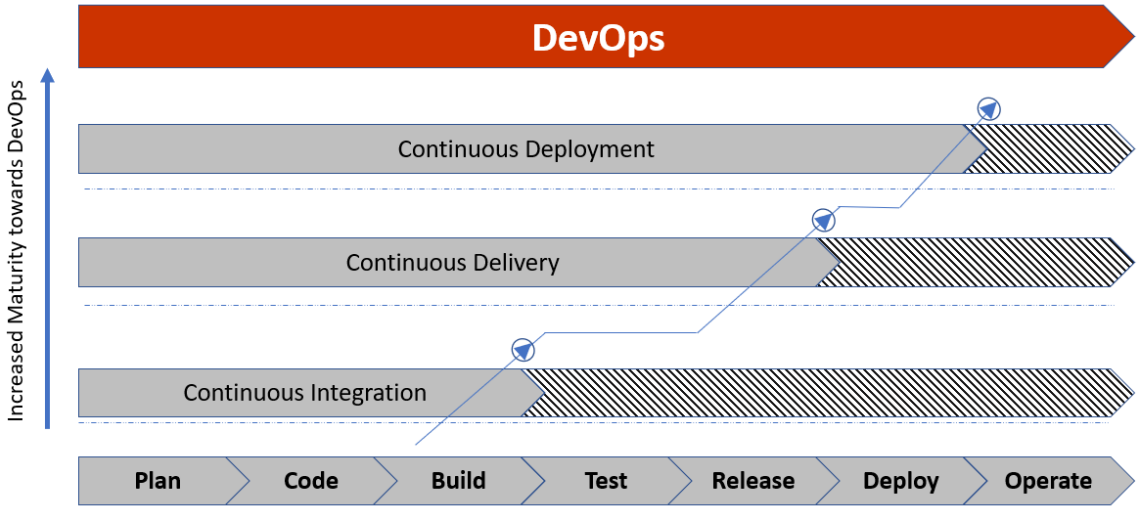
The Operations roles and their responsibilities are described per process in this Cloud Operations Manual, but for more details refer to the Excel version here on SharePoint.

3 Development Processes

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 the Operations 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 Operations 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.

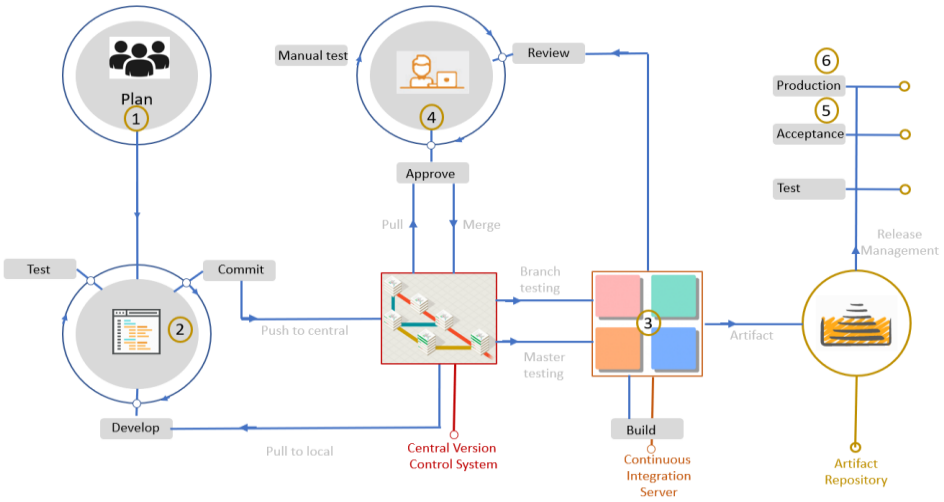
3.1.2 Operations Processes and Requirements

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 the Operations 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 Operations 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.



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 and 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 and 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 and 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 and 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 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

Approved and tested deliveries are (automatically) deployed to the production environment. Automatic and continuous deployment requires a mature organization having all previous steps in place. As long as the Operations 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 Operations 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 Operations Team (e.g. Jira).

In case of major release the Global Business Line 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

In Prepare and Plan the Program Increment (PI) planning takes place and Definition of Done is defined and agreed by the Product Owner, Operations 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

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

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

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)

Deploy to Production

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)

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.
- . For Cloud Ops services, this must be approved by Service Transition (ST) team. ST will in turn will complete a verification checklist to be used as evidence of service readiness for operations
-

Definitions and Agreements

- Deployment Quality Assurance Process should be initiated at the early possible stage of deployment.
- It is a mandatory process for all OneCloud 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.
- Any deployment which will subsequently be managed by Operations team under Cloud Ops must go via the Service Transition team

Service Transition will accept the handover of the environment, and align an onboarding resource to complete and verify Cloud Ops onboarding

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

Quality Records can be represented by the following locations, depending on the service: Quality and Compliance Homepage, OneCloud Sharepoint, local repository agreed with the (G)OSCO upfront.

3.3.1 KPI

During the Development & Operations of services, for various actives as listed below, applicable SLAs/KPIs are tracked & reported as a part of Eviden OneCloud Dashboard:

- Service Development
- Incident Management
- Request Management
- Change Management

Detailed definition & description of individual SLA/ KPI is specified in the dashboard information page:

Reference	Eviden OneCloud Dashboard

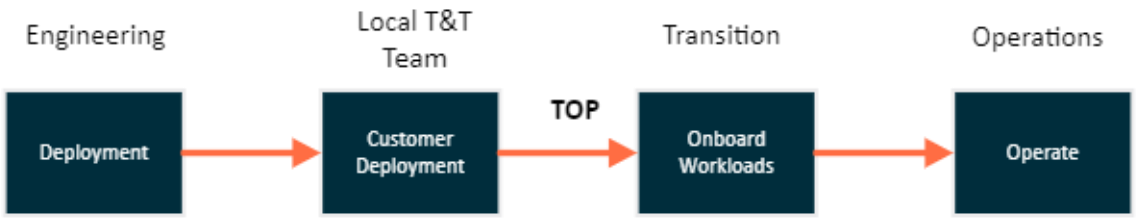
3.3.2 Customer Requested Requirements on existing services

Definitions and agreements on Non-Standard Customer Request on existing services

- 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.), Operations 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 Operation 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 OneCloud 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 Development and Operations teams; 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 Eviden(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 Implementations – Exceptions

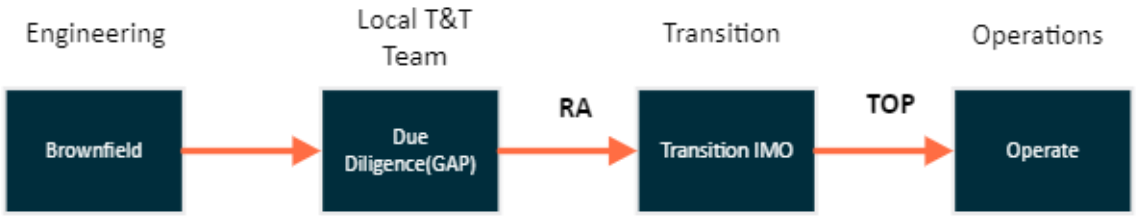
Exceptions occur only when there is a strong business justification to move a Cloud Service into operations while Service Acceptance has not passed. This is applicable for both Global Portfolio Services as well as Local Services. Note: These stages were named Early Life Support (incomplete TOS) or Intermediate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

Onboardings of Brownfield environments to Cloud Ops managed services are coordinated by Service Transition team

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 Eviden 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 Eviden 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 Eviden can take full accountability for operations in TOP.

4 Service Delivery Processes

4.1 Support Group and Categories

Definitions and 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 OneCloud 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.
- The Specific Primary Category for BDS Services must be " Security Management"

Naming Conventions

For OneCloud:

- 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

For BDS:

- Naming convention regarding the new support groups created is mandatory as follows:
    - Country.Security.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 OneCloud Business line, please respect the following guidelines when creating the support group:

- OneCloud Business Line
    - Business Lines one of the following – relevant for reporting: CTO-GDC" for services managed by India, Poland or Romania
    - "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"

    - “Process Management”
- Business Line for BDS groups is: CyberSecurity (CyS)
- OneCloud Naming convention regarding the new categories created in ATF 2 is mandatory as follows:
    - Incidents Events and Problems: Cloud.<Platform><Service>
    - Changes: Cloud.<Service Number>.<Description>

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

4.2 Event Management

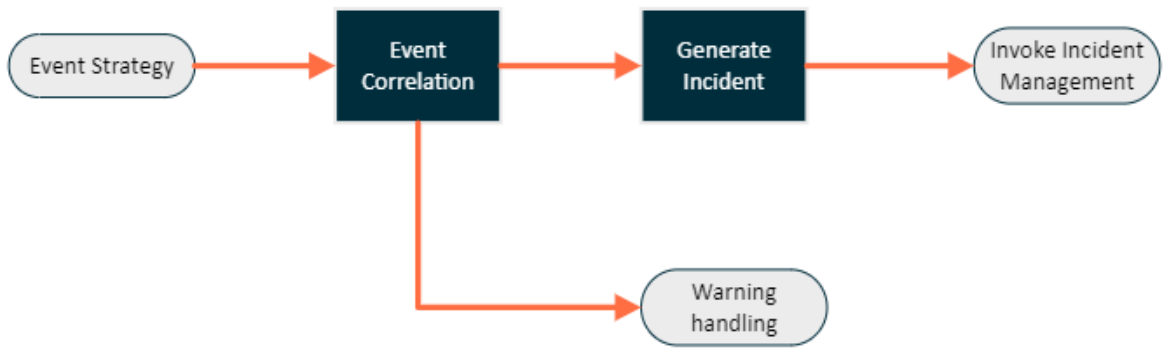
The goal of Event Management is to ensure proper handling of events generated by automated systems. Event handling can lead to a generated incident based on the event data.

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

Definitions and 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 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.

Flowchart and Description



Event Strategy

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

Based on the correlation rules implemented the need of an incident creation will be defined.

Warning Handling

Check generated events (activity triggered from Production Process) and act according to work instructions.

Generate Incident

Tooling creates Incident Request in ITSM tool (e.g. ServiceNow).

Invoke Incident Request

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**.

Definition and Agreements

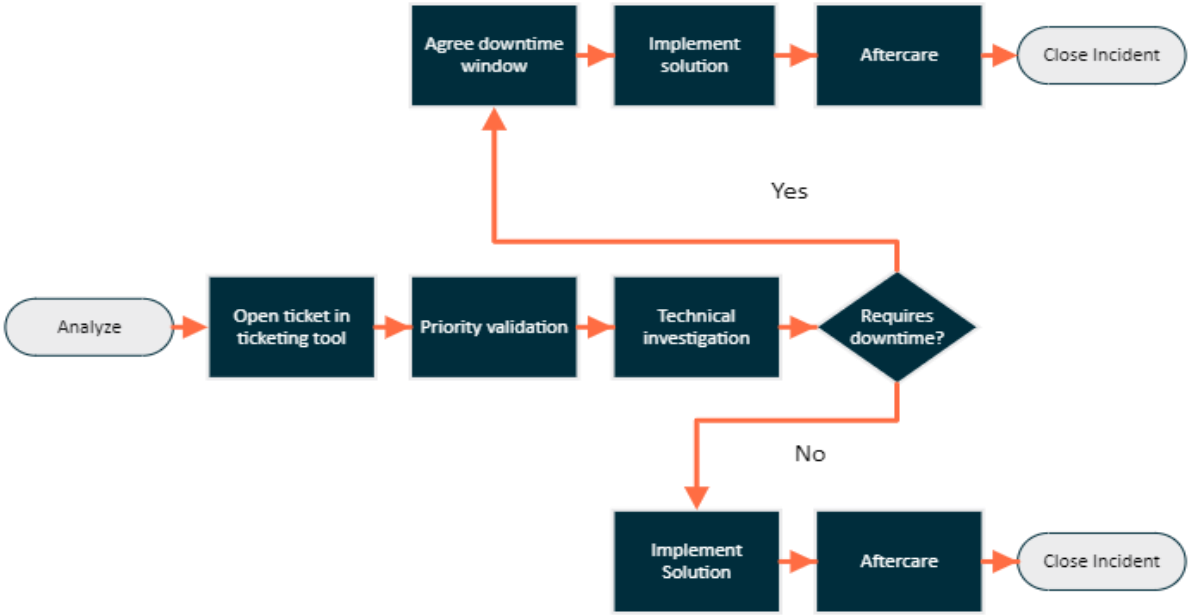
- Operation team must be involved in Incident Management Process in order to achieve process improvement and be able to:
    - Plan responses to potential incidents upfront by identifying weaknesses in the system
    - Develop automated priority selection
    - Develop automated resolution

- Priority of an incident request indicates the Eviden 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 Engineer
    - from the automated solution implemented by the 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 Eviden Management).

- A Major Incident is any incident which requires Eviden 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 Eviden Management) are logged and regular status updates are sent via the agreed communication tool.
- The Service Responsible Manager will take the role of Technical Escalation Lead during Critical Incidents.
- For every Priority 1 or Major Incident the Operations team must be engaged.

Flowchart and description



- To open the incident request and to be able start the investigation mandatory information are required : Is there sufficient information to start working? Right Customer, right and existing CI; correct support group; enough information supplied?
- If additional information from the Requester is needed, the Team/person assigned to the incident contacts the Requester. The Team/assigned person will keep the request on his own support group, fills the call back date where required and change status of the request to “on-hold clock stop”.
- If due to any circumstances the requester cannot be contacted involve Service Responsible Manager 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 Service Responsible Manager or SDM.
- If all above is ok, the Incident request is assigned to an Engineer to be worked upon. In case of a Priority 1 or Major Incident always inform the Service Responsible Manager, the Service Delivery Manager or Cyber Security Delivery Manager (if such a role exists for Customer and incident is related to BDS Cybersecurity Services) 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.
- Status of the incident request can be changed from “in progress” to “on hold – clock stop” for below scenarios:
    - Team/person assignees to the request is waiting for additional, mandatory information.
    - Team/person assignees to the request is waiting for change executive.
    - New resolution time is agreed with requester.

Only Team/person assigned to the request can modify it.

Analyze

- Start analyzing the reported disruption.

Open ticket in ticketing tool

- If the conclusion of the analysis results in identifying a disruption or potential disruption open a ticket and assign it to the Support Group. It can be done directly by Customer, Account, Service Responsible Manager, Service Desk, or Technical Teams, it depends on the service model setup.
- Escalate to Service Responsible Manager when the result of the analysis leads to the conclusion that the priority must be changed. If Service Responsible Manager agrees that priority should be increased, new ticket with proper priority must be open to not breach the SLA for initial request (initial request should be added to the new one as a child and priority should be lower to 5).

Priority Validation

- Management team validates prioritization categorization and availability of all information needed during ticket intake.

Downtime

- Downtime window has to be approved by the CI Owner before implementing the fix additional approval can be required if there is clear and written Customer requirement.

Implement Solution

- Implement the identified solution

Aftercare

- Monitor for an agreed time the current solution to avoid reoccurrence
- Obtain final confirmation for the implemented solution from the requestor or stakeholder

Close request

- The basic principle is to close a request immediately after solving it

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 communication tool, 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 – for OneCloud only
- Documented automated implemented solution in source code – for OneCloud only

4.4 Problem Management

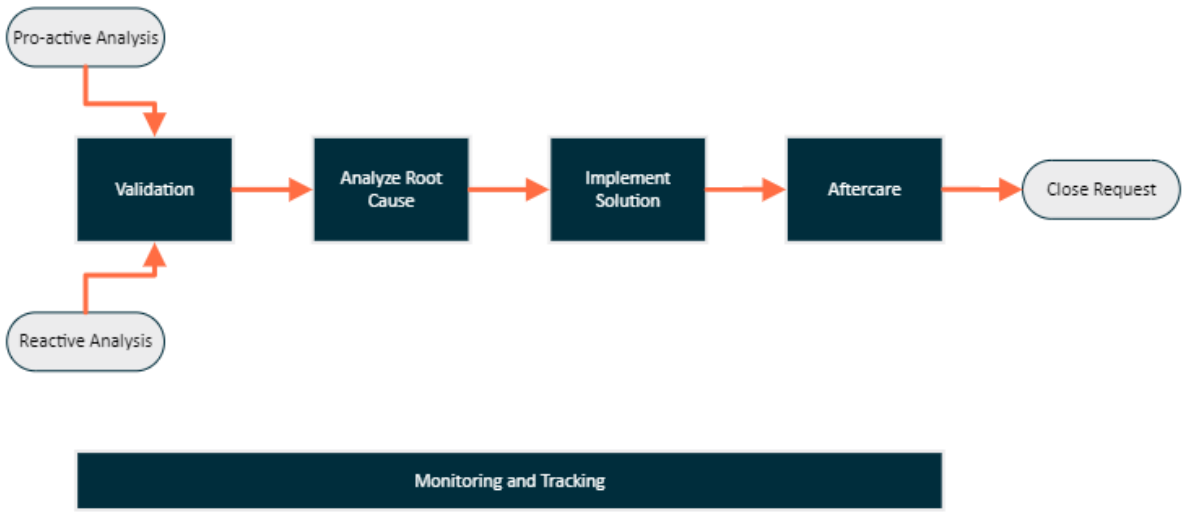
The goal of Problem Management is to prevent (re)-occurrence of incidents by eliminating their root cause.
The implementation fulfils the requirement that originate from the ITCF controls **PM-01 Problem Management** and **PM-02 Problem Management – Major Incidents**

Definitions and agreement

- Mandatory Problem Management Process triggers:
    - A valid P1 incident or Major incident.
    - The mandatory periodic incident analyses by a technical 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 operations 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 OneCloud 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.

Flowchart and description



Pro-active Analysis

- This step must be a mandatory action in the Production Plan.
- Review incident trends and reasoning reports and identify potential problems.

Reactive Analysis

- This applies after a P1/Critical Incident or MI has been resolved.

Validation

- 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

- 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.

Implement Solution

- 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 Business Line of customer via normal procedures.

Aftercare

- 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 or SDM to close the problem based on above evidence.
- Upload the final RCA document on the agreed platform and provide the URL into the problem ticket.

Close

- Check RCA lifecycle status.
- Set request to status Closed.

Monitoring and Tracking

- 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: Quality and Compliance Homepage, OneCloud 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.

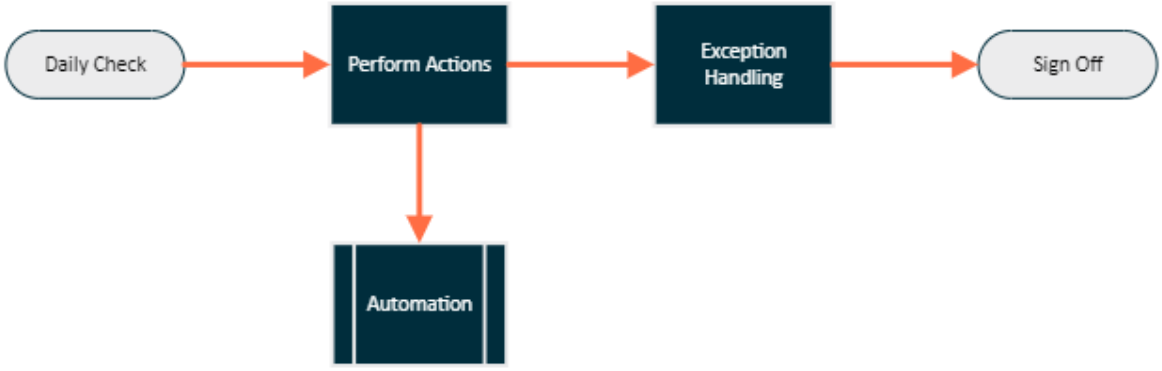
The implementation fulfils the requirement that originate from the ITCF controls **LS-13 Antivirus / Malware, IM-02 SLA threshold monitoring, LS-15 Cryptographic Key Management, DB-02 Backup Monitoring** and **OP-02 Operations Monitoring**

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)
    - Besides these activities the production plan needs to be completed with service specific activities.
    - Development and Operations have an important role in the automation of the operational activities.

Flowchart and description



Daily Check

- 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

- Perform actions according plan and according associated work-instructions

Automation

- Define automation actions to improve the execution of the activities
- Propose the actions to the Product Owner for them to be included in the Team Backlog

Exception Handling

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

Sign-Off

- Provide mandatory evidence

Mandatory evidence for Production Management

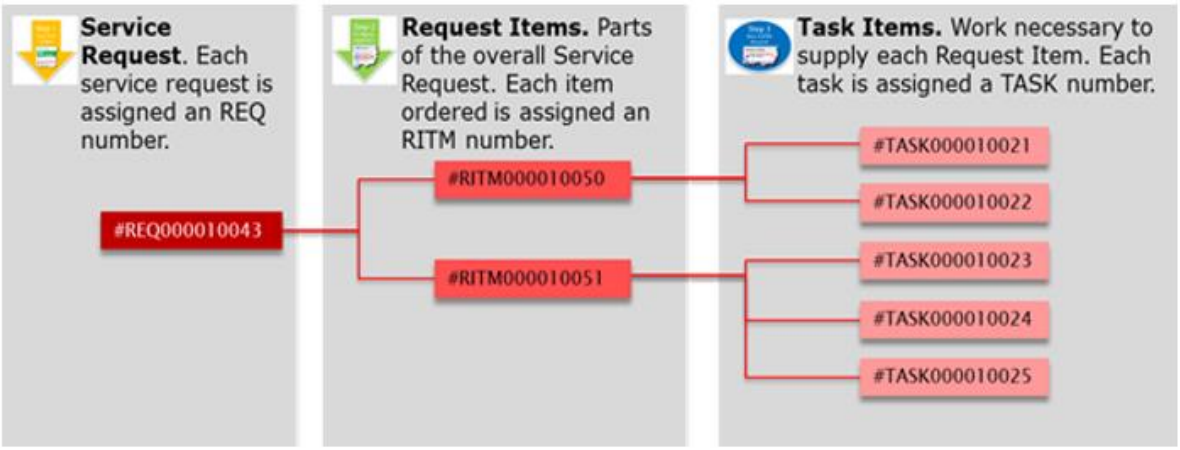
- Finalized and approved Production Plan
- Sign-Off your checking activities by means of registering this in a production plan log which is stored on Quality Records Environment. In case incidents are raised because of your check, name incident request numbers in the log-file.
- Quality Records Environment can be represented by the following locations, depending on the service: Quality and Compliance, OneCloud 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 Fulfilment

The Request Fulfilment 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 Fulfilment.
- 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 fulfilment.

Mandatory evidence for Request Fulfilment - Generic

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

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/BDS 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.
- For OneCloud are defined in the Global Cloud Change Activity Production 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.

Flowchart and description

Validate Change

- 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

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

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.

Aftercare

Make sure aftercare activities are done as described in the work instructions and/or workflow tasks. Also, store change evidence where applicable.

Close Change

Set Change ticket status to closed

Mandatory evidence for Change Management – Standard Change

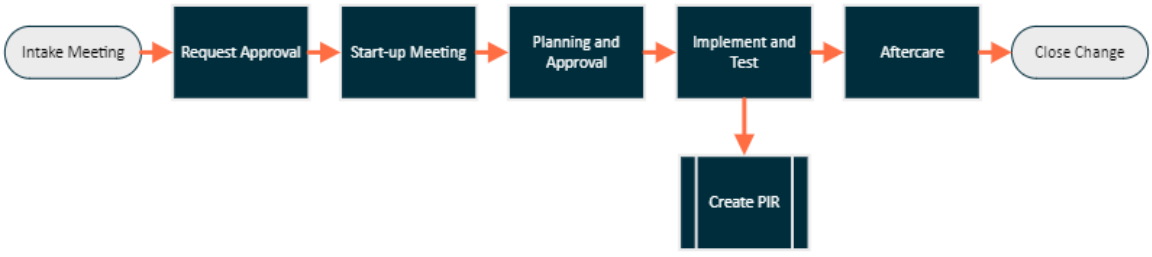
- Work instruction, CIP and BIG or Blueprint Design stored on a known location agreed with Document Control for every standard change
- Categories described in the Global Change Activity Production Catalog (CAPC) are implemented in ITSM Tool (if applicable, but tooling constraints must be discussed prior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

4.7.2 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/BDS 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 OneCloud is the owning change manager and requests approval internally in OneCloud and applicable AST CABs. (request is assigned to acting change manager)
- For Shared Cloud Services all non-standard changes to be handled by Global Cloud Change Manager and grant Global One Cloud 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)

Flowchart and description



Intake Meeting

Organize intake meeting to discuss the non-standard change.
Attendees;
Technical Service Architect, Service Responsible Manager, Product Owner, Requester (e.g. CLO), 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.

Request Approval

Gather approval from Service Responsible Manager or Service Delivery Manager. Store email approval on Quality Records Environment.

Start-up Meeting

Organize Startup meeting with Technical Architect, TSM, Product Owner, 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

- For OneCloud - Make sure the CIP is filled by the Operation team and a ticket request is issued with pre-defined Non-Standard workflow available for all customer contracts:
- ServiceNow: Cloud.<Platform>.GenericWorkflowNonStandardChange.
- Include all Business Lines and Account teams which are involved in this change and describe the impact per Business Line or Customer.
- Address request and CIP to Th Responsible Change Manager. Required CAB attendees are: Change Manager, Service Responsible Manager, Product Owner and Requester. For Medium (Significant) and Large (Major) changes, Account Team approval is mandatory.
- In case of a non-standard change type 'Large (Major)', also address the change to the Eviden Global Delivery CAB. Send CIP and request information to the Global Process Owner for Change Management (mailbox) and request for approval.
- Store all approvals Quality Records Environment.
- After approval has been granted, agree on implementation date (store implementation date in Ticketing tool request) and inform the responsible 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/Account Team approval not mandatory)
- Medium (Significant) change; 4 weeks (customer/Account Team approval mandatory)
- Large (Major) change; 6 weeks (customer/Account team approval mandatory)

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

Implement and Test

- 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.

- 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

- Make sure aftercare activities are performed as described in the CIP.
- For instance;
- Update CMDB and set the 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

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

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: Quality and Compliance Service Delivery Centre, OneCloud Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.

4.7.3 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'.

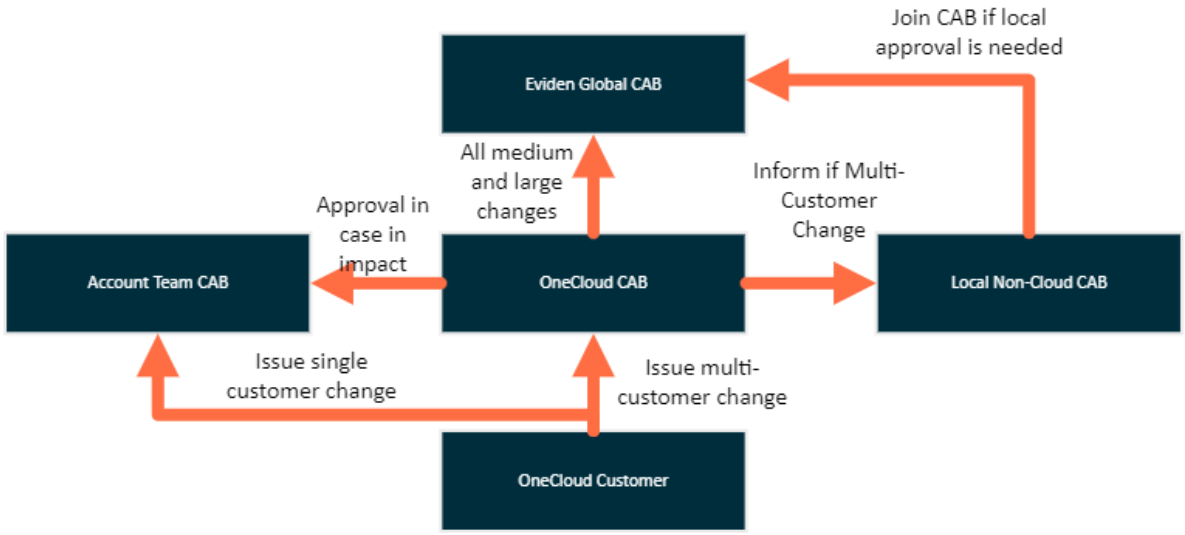
Emergency change preparation recognizes the same procedural steps as a non-standard change. However Senior Management (OneCloud/BDS and AST) and Emergency-CAB approval is required, mandatory documentation may be written afterwards. Emergency CAB is applicable in case of prevention of a priority 1 or 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 OneCloud/BDS and AST Senior Management approval on Quality Records Environment
- Quality Records Environment can be represented by the following locations, depending on the service: Quality and Compliance, OneCloud Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.
- All other Non-Standard change evidence (see 4.7.3)

4.7.4 Change Advisory Board Structure - For OneCloud only

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 OneCloud 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.



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 Eviden 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.

Eviden 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.

4.7.5 Continuous Integration and Continuous Development

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 Operations 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 Eviden 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 Operations 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 Configuration Management

The goal of Configuration Management Process is to support the Eviden 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

- 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.

4.9 Release Management and Service Lifecycle 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;
- Operation 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 Operations team.
- In principle a customer cannot decline a Life Cycle Management update. In exceptional cases a decline is allowed only when a Risk is agreed with the customer (see operational risk management). 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.

Flowchart and Description

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

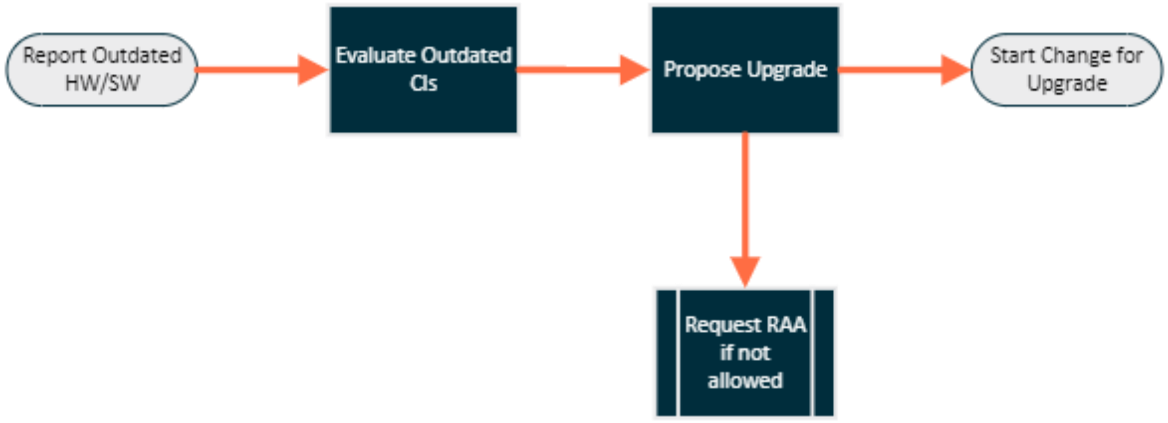
The goal of Technology Refresh and Obsolescence Management is to ensure that systems (hardware) remain supported and do not cause security or availability risks.

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 Operations 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.

Flowchart



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: Quality and Compliance Homepage, OneCloud 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
- Registered, communicated and accepted risk (see operational risk management process) 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 service levels.
- If the contractual agreed SLA's are different that the SLA's defined in the Service Design, an upfront agreement is required.
- Monthly reporting and reviewing of delivered agreed service levels (KPI's) is mandatory;
- If to deliver OneCloud/BDS Service Manager the Customer ITSM Tool is used the Customer is obligated to deliver mechanism which will allow SLA real-time monitoring, measurement and reporting
- The Service Delivery Manager is accountable for the continuous monitoring of the agreed Service levels (KPI's) with the customer;

- The OneCloud Technical Service Manager (TSM) /BDS Service Manager is accountable for the continuous monitoring of the agreed Service levels (KPI's) for service within his/her Business Line.
- 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 OneCloud Business Line, 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 must 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 OneCloud 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 OneCloud/BDS 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 Fulfilment 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: Quality and Compliance Homepage, OneCloud 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.

Definitions and Agreements

Capacity management in terms of technical and information resources for the account is managed by the Account Management roles in line with the contract eg. based on the ASMM Capacity Management Process

- TECHNICAL

Technical Capacity on a Service level (owned and managed by CyberSecurity Team) is the responsibility of the support team with technical experts and service managers who monitor and report the status based on Account Team or Contract requirements. Capacity Management of the cloud infrastructure during operations is executed by the hyperscalers and is not applicable for Eviden public cloud operations. Capacity Management of resources in the cloud infrastructure (eg. VMs, ...), and related cost management, is the responsibility of the customer. Any capacity monitoring during operations will be managed as part of event management and is not considered capacity management. Any changes of resource capacity during operations can be requested, and is executed, via change management and is not considered capacity management.

- HUMAN

Human capacity management covers aspects of planning and delivery of human resources in line with Workforce Management process. People/Team/Operations Managers etc. plan the resources vs. current and forecasted workload demand taking into consideration the service requirements as regards service levels, availability and continuity.

Mandatory Evidence for Capacity Management

Not applicable for Eviden public cloud or BDS environment .

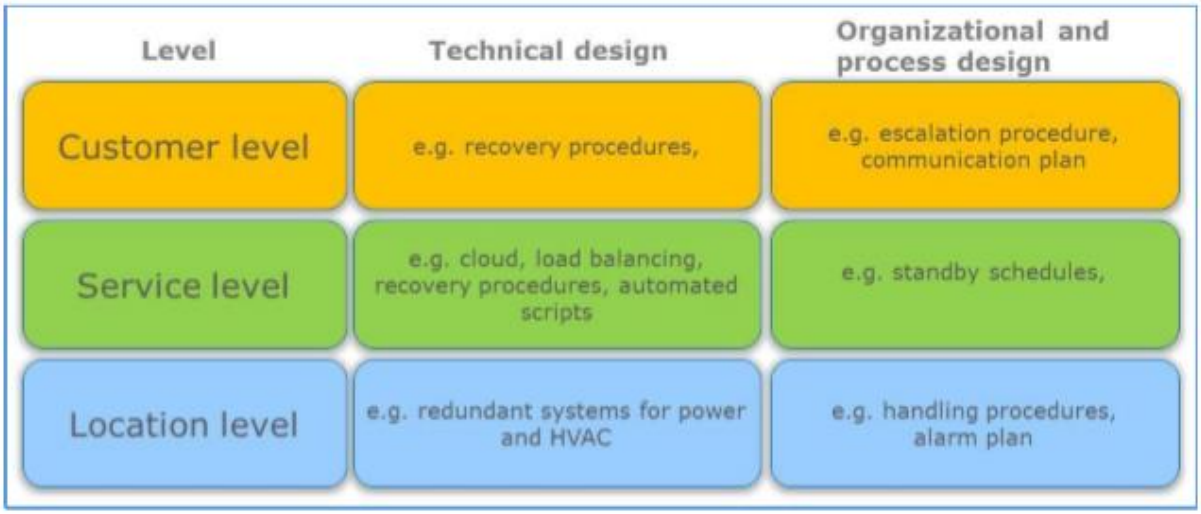
4.13 IT Service Continuity Management and Disaster Recovery

IT Service Continuity Management & Disaster Recovery (ITSCM & DR) aim to ensure that the cloud component of Eviden'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 for OneCloud

- Continuity Plans are needed to fulfil requirements of ISO22301, ISO27001, ISAE3402
- OneCloud Management has the role of Business Continuity Owner for OneCloud
- The Global Business Continuity Coordinator, is responsible for defining OneCloud Services Continuity processes based on Eviden 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 OneCloud;
- 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 OneCloud is defined for the service level. Customer Level must be settled by the AST, location level by the corresponding (internal) services. (See next picture)



Definitions and Agreeements for BDS

- BDS Service Continuity Plans are needed to fulfil requirements of ISO20001, ISO27001, ISAE3402

- Head of BDS Cys GDCs have the role of Business Continuity Owner
- The BDS GDC Security Officer is responsible for defining below key documents:
  - Business Continuity Plan (or Service Continuity Plan for CyS location in Poland) for BDS GDCs
  - Recovery Procedure for Human Resources in each BDS GDC location
  - Disaster Recovery Plans and Tests for BDS GDC locations

  based on Eviden standards and assessing whether processes are executed according to definitions.
- There are two dimensions of the Service Continuity Management:
  - Location Level - Service Continuity Management for the Global Delivery (particular GDC) site covering aspects related with continuity of services delivered from that particular site and managed on the BDS GDC level.

Service Level - Service Continuity management on operational level (operational resilience) for the service covering technical and service management aspects related with IT Configuration Items availability, security, and related service documentation, focusing on effective implementation of Eviden Security Policies, maintenance and backup activities for Eviden critical assets - IT technical infrastructure elements in the scope of BDS GD CSS responsibility that are critical to the service deliver in line with the agreed Service Availability Levels.

4.13.1 Define Service Continuity – for OneCloud

Flowchart and Description

Define SCP (Global Business Continuity Coordinator)

A Service Continuity Program defining the Service Continuity Management activities for OneCloud, 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 and Operate – for OneCloud

Flowchart and Description

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 must 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 OneCloud organization, tools will play a key role in order to create fit for purpose documentation for SCP Process.

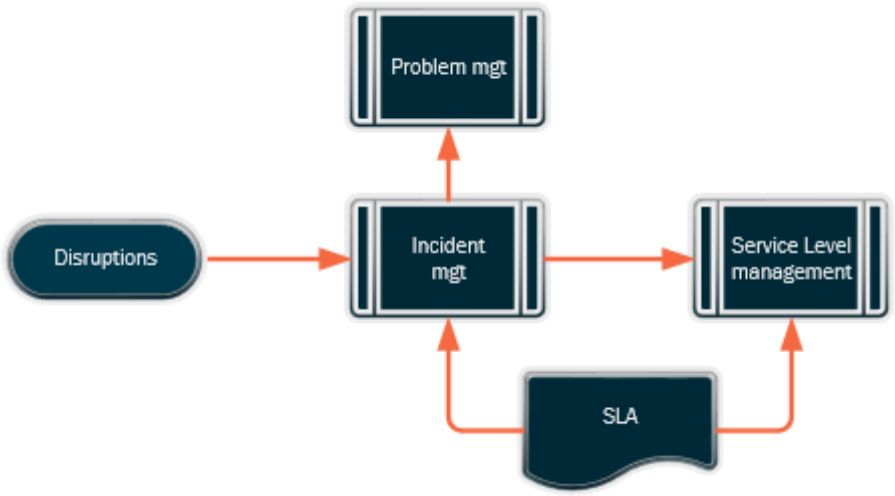
4.14 Availability Management

The objective is to understand the Availability requirements of the business and to plan, measure and monitor to improve the availability of the IT Infrastructure, services, people, resources and supporting organization to ensure these requirements are met consistently. Availability Management should ensure the agreed level of availability is provided.

Definitions and agreements

- For public cloud services the availability of the physical IT infrastructure is managed by the Hyperscaler.
- The service availability requirements are defined in the customer contracts (SLA) and implemented during onboarding of the service for the specific customers.
- During operations the availability of the IT infrastructure, and response by service organization to disruptions, is monitored and measured
- Any disruptions in IT infrastructure are managed via event and incident management process.
- Problem management process is executed after priority 1, or major, incidents to analyse the root cause and define corrective/preventive measures.
- On a monthly basis the service levels are reported (internally & to customers), and reviewed, as part of the service level management process.

Flowchart



Mandatory Evidence

- Incident management, see paragraph 4.3.
- Problem management, see paragraph 4.4.
- Service level management, see paragraph 4.11.

5 Project Management

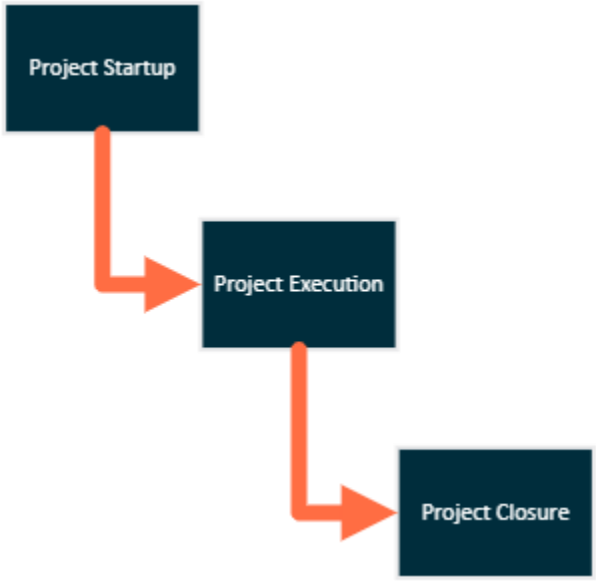
5.1 Project Management Overview

For any new contract, a project manager gets allocated to ensure project execution is done in accordance with the customer obligations.

Project Manager is responsible for project execution according to the contractual agreements / SOW, project execution life cycle & associated processes :

- Planning, management & resource control of multidisciplinary projects.
- Decision-making authority within clearly defined boundaries & scope of project. Responsible for ensuring compliance with specified processes and methods.
- Coaching of project participants regarding the application of project management processes & methods.
- Responsibility for structured communication with several divergent stakeholder groups from the project startup phase till project closure. Control of necessary decision-making processes and changes.
- Establishing reporting in accordance with the agreed structure & management of risks/mitigation actions.
- Measurement & evaluation of project performance within the contractual obligation of budget, schedule & quality requirements. Ensure stakeholder Satisfaction.
- Identification of deviations from the defined project scope and initiation of suitable measures including enforcement of change management processes. Responsible for management of risks and mitigation actions.

Project Execution life cycle is broadly categorized in three phases:



1. Project Startup

During project startup phase, project manager performs & co-ordinates below startup activities & deliverables, along with the project team & various stakehodlers :

- Handover from Bid/Sales to Delivery
  - Contract obligations – Scope , Deliverables , Milestones & Acceptance criteria.
- Kick-Off with customer
- Project start up activies :
  - Setup organization chart & roles/responsibilities.
  - Staffing & resource onboarding plan
  - Setup Governance
    - Internal & external governance meetings & reporting
    - Communication plan & escalation matrix
    - Risk & Issue management
  - Project Planning
  - Setup Project in the appropriate tool (e.g. WBS code) & reporting
  - Identify Quality milestones/gates
  - Identify & setup KPIs
  - Setup Invoicing schedule
  - Change management setup
  - Document Mgmt setup

2. Project Execution

During project execution phase, project manager performs below project tracking & monitoring activities along with the team & stakeholders , in order to fulfill contractual obligations with regard to schedule , budget & quality .

- Project schedulling & tracking
  - Effort estimation / re-estimation
- Resource Management
- Internal & external governance meetings
- Internal & external reporting , including :
  - KPI reports
  - Risk & issue tracking
- Execute Quality gates
- Obtain customer acceptance for the deliverables.
- Hypercare/Warranty (as applicable) – Planning/tracking & obtaining customer signoff
- Provide inputs for invoicing, as per the contractual milestones.
- Change Requests– Tracking & Monitoring
- Document Management

3. Project Closure

Main activities performed during project closure:

- Validate fulfillment of contractual obligations

- Resource release / offboarding
- Obtain financial closure
- Conduct project closure meeting

5.2 Change Management in Projects

A change is every event in project/program that impacts the scope, budget, time, quality or a combination of these. There are two types of changes:

- Changes covered by external revenue (mostly initiated on request of the customer)
- Changes not covered by external revenue (also known as exceptions or cost of non-quality)

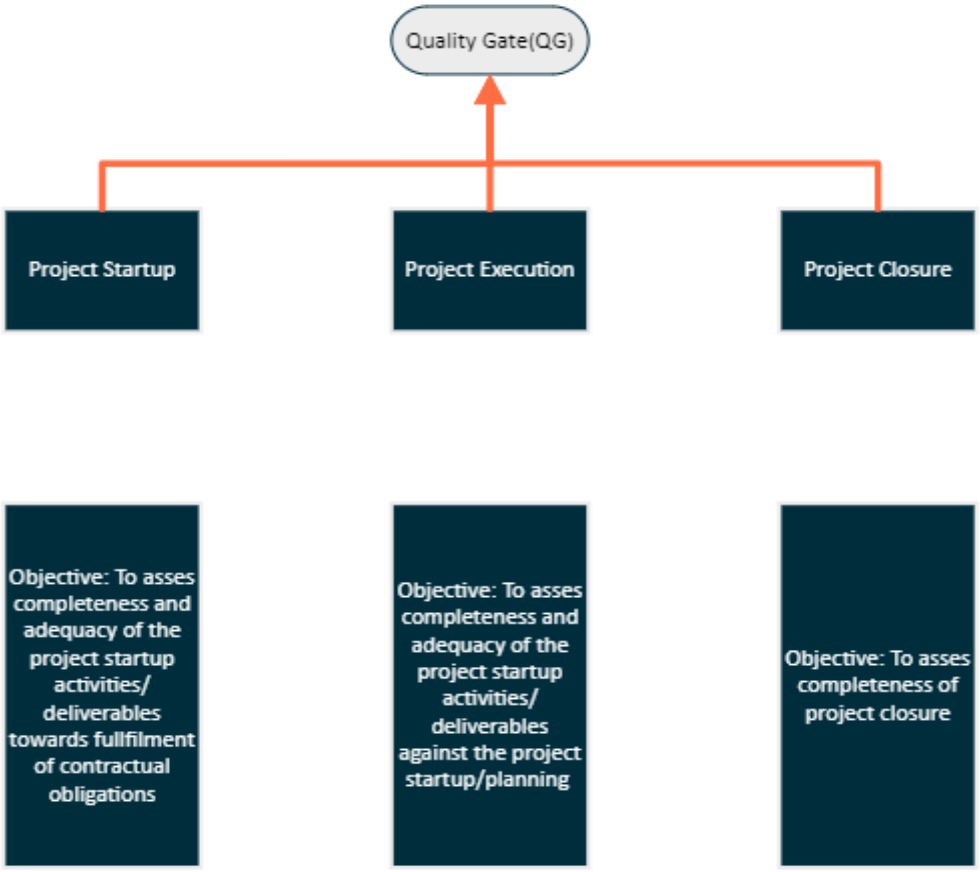
Change request gets assessed based on the level of its impact:

- Project Manager -if the change itself keeps within the delegated project boundaries of time/budget/quality.
- Program Manager - if the change itself keeps within the delegated program boundaries of time/budget/quality.
- Steering Committee/Board - if the change does not keep within the delegated program boundaries of time/budget/quality.

Out of Scope: Change Management in Operations (i.e., The process of handling changes in the maintained production environment)

5.3 Quality Management in Projects

During project startup phase, Project Manager plans quality management activities & quality Gates, along with the stakeholders. Quality Gates are planned in line with the phases of project execution life cycle.


Quality Gate(QG)
Project Startup
Project Execution
Project Closure
Objective: To asses completeness and adequacy of the project startup activities/ deliverables towards fullfilment of contractual obligations
Objective: To asses completeness and adequacy of the project startup activities/ deliverables against the project startup/planning
Objective: To asses completeness of project closure

5.3.1 Quality Gate Process

Phase	Input	Activity	Output	Responsibility
Project Startup Phase	**Project plan** established , based on Contract obligations – Scope, Deliverables & Milestones	**Quality Gate Planning:** Based on contractual obligations & project plan, project manager plans the quality gates, through involvement of project stakeholders & QM. Quality gates are planned at different phases of the project management lifecycle, namely: **1.Project start up – Quality Gate** **2.Project exection – Quality Gate :** Based on the contractual milestones , as appropriate , multiple quality gates are planned during project execution phase. **3.Project closure - Quality Gate**	**QG plan**	**Responsibility-**PM **Supported by** - QM & other stakeholders

Phase	Input	Activity	Output	Responsibility
Project Startup, Execution & Closure	QG plan	**Prepare for Quality Gate**: Ensure preparation for quality gate, as per the quality gate plan. Informs other stakeholders about the quality gate. Collates the required the evidence & updates the QG template or formats. Ensure readiness for conducting QG meeting, by submitting all the necessary evidence to QM & other stakeholders	**Evidence required for QG are submitted**	**Responsibility-**PM **Supported by** - QM & other stakeholders
Project Startup, Execution & Closure	**QG evidence** submitted by PM	**QG -Readiness check:** QM evaluates evidence & status against various criteria/checkpoints & obtains clarifications (if required) from the PM.	**QG evidence - evaluated**	**Responsibility QM** **Supported by** - PM

Phase	Input	Activity	Output	Responsibility
Project Startup, Execution & Closure	QG evidence-evaluated	**Conduct QG Meeting (attended by PM, QM & other stakeholders)** On the basis of evaluated status of various criteria/checkpoints of QG, a joint meeting is held (between PM, QM & other stakeholders) in order to decide whether project fulfils the objective of QG and to make a decision i.e., GO/ GO with actions / NO GO – Rework & Recheck 'Customer Engagement Manager / head of Customer Delivery' is consulted, in case if there is no consensus in the meeting on QG decision.	**QG Decision:** GO/ GO with actions / NO GO – Rework & Recheck	**Responsibility QM** **Supported by** - PM, 'Customer Engagement Manager / head of Customer Delivery'

5.3.2 Quality Gate - Assessment Criteria

Assessment criteria of Quality Gate , provides explicit requirements against which the appropriate evidences could be submitted & objectively evaluated.

Purpose of the Project startup - Quality gate' checklist is to provide criteria/checkpoints to assess completeness & adequacy of project start up activities/ deliverables , towards the fulfillment of contractual obligations with respect to schedule, budget & quality .

No#	Project startup -QG Criteria	
1	**Handover from Bid/Sales to Delivery**	Contract obligations – Scope, Deliverables, Milestones & Acceptance criteria is well recognized by Delivery team.
2	**Contract Walkthrough**	Walk-through of customer signed contract & SOW, is conducted with all relevant stakeholders: (i.e.; Contract Related risks, Assumptions, Internal service agreements, Agreements with external vendors, etc. are recorded)
3	**Kick-off with Customer**	Client Kick-off meetings performed with the required Agenda.

		Minutes are produced and shared with stakeholders.
4	**Deliverables List**	Contractual Deliverables mapped in the project plans & project schedule.
5	**Organization Setup**	Delivery organization including, roles and responsibilities, and customer roles (where appropriate), are documented & shared with stakeholders.
6	**Internal Kick-off**	1.Internal Kick-off meetings conducted 2. Minutes are produced and shared.
7	**Acceptance Criteria**	Acceptance Criteria is defined for all the Deliverable & agreed with the customer. Hypercare/Warranty period is agreed with customer & incorporated in project plan/schedule.
8	**Resource Capacity Plan**	Resource plan established & resource capacity allocation done accordingly.
9	**Resource Onboarding & Training Plan**	Onboarding & Training needs have been identified and trainings are planned.
10	**WBS and Scheduling**	Delivery Schedule is defined along with Critical/Major milestones. (at appropriate level i.e. Phase/ Sprint or Program Increment level etc .)
11	**Governance & reporting**	1.Client Steering Group meeting (including, participants, format of Agenda, Minutes of meeting etc) agreed with the customer. 2.As per Contract terms, other project level governance & reporting requirements are agreed with Customer. 3.Escalation procedure agreed with customer.
12	**Communication Plan**	All stakeholders of a project are identified and covered in the communication plan agreed with the customer.
13	**Risk Management (Risks, Issues, Assumptions & Dependencies Log)**	Risk Management is initiated, including Risk Management process setup with the customer. - Key risks & mitigation actions are defined. External risks shared with the customer. - Issues Log is in place - Assumptions/dependencies are defined and monitored.
14	**Quality Management**	Quality Milestones/Gates are identified. Quality Milestones/Gates are planned & incorporated in project schedule.

15	**Project KPIs**	Project KPIs are agreed with the customer and incorporated in the Reporting Schedule.
16	**Invoicing Schedule**	Invoicing schedule, associated KPIs and arrangements are agreed.
17	**Change Management**	Change control process (including Change request Form, Change request Log) agreed with the customer.
18	**Document Management**	Suitable Document management repository (e.g., SharePoint) is set and made accessible to team.

- Project Execution – Quality Gate

Purpose of 'Project execution - Quality gate' is to provide criteria/checkpoints to assess completeness & adequacy of project execution activities/ deliverables, as against the project startup/ planning which includes contractual obligations/baselines regarding schedule, budget & quality aspects.

No#	Project exection - QG Criteria	
1	**Planning & Scheduling**	Detail Project plan/ schedule is tracked & monitored at the appropriate level (i.e. Phase/ Sprint or Program Increment level etc .) as identified during project startup phase .
2	**Resource Management**	Resource allocation & management is performed, based on the resource capacity plan which is established during project startup phase.
3	**Governance & reporting**	A. External governance meetings are conducted & External reports are produced/published, according to the agreement with Customer done in project startup phase. B. Internal Governance meetings are conducted & internal reports are produced/published , according to plan defined in project startup phase.
4	**Risk Management**	Risks, Issues, Assumptions & dependencies are identified, tracked & reported, according to the practices planned during project startup phase.
5	**Project KPIs**	• External KPIs are reported, according to the contractual obligations (and concerned agreement with customer done in project startup phase)

		• Internal KPIs are reported, according to planning & setup done in project startup phase. • Based on the KPI performance , corrective/preventive actions are planned & tracked.
6	**Quality Management**	Quality Management activities & deliverables are performed in a project, according to the contractual obligations & applicable 'Delivery Model/Methodology' of the services in the scope. i.e.: • Fulfilment of 'Acceptance criteria for deliverables', is validated & its records are maintained, prior to the customer delivery/deployment in the production. Customer signoff is obtained . • Fulfilment of 'Acceptance criteria of Warantee/Hypercare phase' (if applicable) is verified & customer signoff is obtained . • As applicable - Record of peer/SME reviews of intermediate deliverables e.g.: Assessment / Design / Code etc • As applicable - Records of the defects & its closure status for concerned test phases (i.e., Unit test, integration/system test, UAT etc.) with in the project
7	**Change Management**	Change Management: • As appropriate, Change requests are identified (to execute the project within the contractual obligations of schedule , budget, & quality) • Record of all the change request is maintained along with its approval & implementation/closure status.
8	**Invoicing**	Inputs for invoicing are provided, as per the contractual milestones.

- Project Closure – Quality Gate

Purpose of 'Project closure - Quality gate' is to provide criteria/checkpoints to assess completeness of project closure activities/ deliverables .

No#	Project closure -QG Criteria	
1	Governance	All contractual deliverables are completed & signed-off by customer.
2	Governance	Formal acceptance of a project is received from customer.
3	Change Management	All Change requests are closed - Change request log is updated.
K4	Financials	All payment milestones are invoiced.
5	Governance	All Project related WBS codes closed.
6	Resource Management.	Offboarding of all the resources is done, in accordance with Offboarding process. i.e.: 1. Removal of concerned access. 2.Offboarding communication sent
7	Governance	Project Closure Meeting conducted & all stakeholders are informed about project closure.
8	Best Practices	Project specific 'Best Practices' are collected & reported (to enable organization wide continuous improvement)
9	Lessons learned	Project specific 'Lessons learned' are collected & reported (to enable organization wide continuous improvement)
10	Customer Satisfaction Survey	Customer Satisfaction Survey conducted (as applicable , based on contractual obligations/ internal practices) & results are communicated to the stakeholders.

5.4 Project KPIs

KPIs get identified & reported, to manage a project efficiently within the quantifiable contractual obligations of schedule, budget & quality.

Activities of KPI identification, monitoring & reporting are performed across the three phases of project execution lifecycle:

- Project Startup Phase - KPI identification & setup
  - Project manager is responsible for planning of applicable internal & external KPIs along with the concerned stakeholders . KPIs are identified primarily based on the two inputs :
    - External KPIs: These are the KPIs which required to be reported due to contractual obligations i.e. KPIs defined in the customer contract/SOW.
    - Internal KPIs: Internal KPIs are recommended to be captured for efficient governance of any project , with in the organization. Internal KPIs coves primarily the two aspects of project delivery.
- Project Execution Phase - KPI Monitoring, reporting & continuous improvement:
  - During project execution phase, project manager is responsible for monitoring & reporting of internal & customer KPIs .
  - Project manager provides facilitation to the project team & stakeholders (towards identification of appropriate corrective/preventive actions) in order to achieve continuous improvement in KPI performance of project .

Reference	Location
RAINBOW	Rainbow Process Presentation.
Eviden – Best Practices	Eviden Program Management Centre - Artefacts
Eviden -Customer Delivery Global Project Summary info.	Customer Delivery Global Project Summary Info.xlsx
Cloudreach Project – Best Practices	Delivery Processes - Customer Delivery - Confluence (jira.com)

6 Service Transition

Service Transition is a global team within the Operations organization, responsible for the onboarding/offboarding of services under the Cloud Managed Services portfolio. Service Transition team reports to the Head of Service Assurance

6.1 Scope and Objectives of Service Transition

- The onboarding/offboarding of Cloud Managed Services portfolio, as well as any changes to existing services
- The improvement of onboarding/offboarding processes and functions
- The retirement of service and the transfer of services between service providers and Eviden
- Plan and manage the changes in service efficiently and effectively.
- Act as an escalation point during transition activities.
- Manage the risks related to newly introduced, modified, or discontinued services.
- Deploy the service releases into environments that support them adequately.
- Set the appropriate expectations for the performance and usage of new or changed services.
- Make sure that the service changes create the expected value for the business.
- Provide the necessary knowledge and information about services and service assets.

6.2 IT Services in Service Transition

Change Management Process: To control the lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT services.

Change Evaluation Process: To assess major Changes, like the introduction of a new service or a substantial change to an existing service, before those Changes are allowed to proceed to the next phase in their lifecycle.

Project Management (Transition Planning and Support) Process: To plan and coordinate the resources to deploy a major Release within the predicted cost, time and quality estimates.

Release and Deployment Management Process: To plan, schedule and control the movement of releases to test and live environments. The primary goal of Release Management is to ensure that the integrity of the live environment is protected and that the correct components are released.

Service Validation and Testing Process: To ensure that deployed Releases and the resulting services meet customer expectations, and to verify that IT operations can support the new service.

Configuration Management Process: Setup information about Configuration Items required to deliver an IT service, including their relationships and handover to operations

Knowledge Management Process: To gather, analyze, store and share knowledge and information within an organization. The primary purpose of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge.

6.3 Flowchart and Description

- To define the complete strategy for transitioning including the policies, roles and responsibilities, standards, frameworks, and the criteria for success.
- Make the necessary preparations for service transition along with the review and acceptance of inputs, raising a request for making changes, checking the readiness for transition, and baselining the configuration.
- Plan and coordinate the transition of services which includes the generation of plans for service transition, reviewing and coordination of plans which are ready for release and deployment.
- To provide adequate support for the transitioning process which includes providing advice and assisting in administration, monitoring of progress, and reporting.

6.4 Quality Checks

Any Service Transition process can only be considered completed once the deployment of the service is verified by an Operations lead who was not assigned to the onboarding project. The Service Delivery Manager also reviews the internal knowledge-share before the service is live.
The following artefacts are created and completed as part of onboarding:

- Customer Action Checklist
- Technical Onboarding Checklist
- Service Onboarding Verification Checklist
- Internal documentation:
  - Onboarding Intake workbook
  - Workload workbook
  - HLD/LLDs if infrastructure is built by Eviden
  - Completed TOP if handed over from Deployment Manager
  - Customer wiki, created from the above

7 Quality Security and Compliance

7.1 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 Eviden policies and regulations and for Security in his Operations team.
- The Product Owner is accountable for Security and Compliance awareness and mandatory trainings for an Operations team.
- The security processes are mandatory for every Cloud Service and Operations team;
- Information Security management is integral part of all ASMM, Operations teams, security and production processes and is part of everyone's daily work;
- Eviden is certified for ISO27001. External auditors perform regular surveillance audits; Audits on ISO27001 are guided via the GBU's;
- Eviden 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 Eviden My Learning site.

7.2 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 Eviden global patch policy.
- 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 Eviden 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 Operations 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 centre 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 Operations
- For DPC version N or N-1 Operations Team will test the patch and provide a work instruction for deploying the patches.
- For previous DPC releases Operations 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 Operations team.

- The Operations team maintains overviews of implemented and recommended patches per Customer and Service under their responsibility;
- The Operations 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;
- Risks must be addressed via operational risk management when the Customer does not want to implement the advised patches. Not allowed in case of Eviden owned shared CIs;
- RACI on Patching is included in the overall RACI.

Flowchart and description

Evaluate and Prioritize (Patch Manager)

Evaluate and prioritize the Supplier and Eviden 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 Operations patch manager tracks the progress in a patch tracker. The tracker must contain:

- The patch advisories from vendors or Eviden patch advisories;
- Patch advisories with on the backlog for testing;
- Patches (changes) with on the backlog for deployment;

Create Change(s) (Operations 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.

Operational Risk Management (Operational engineer, Service Delivery Manager)

Operational risk management needs to be initiated in case a customer wants to skip a patch cycle.

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
- Registers, communicated and discussed risks 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)

7.3 User Authorization Management

The goal of User Authorization Management is to ensure the correct Eviden 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**

7.3.1 Main principles

Authentication:

- Only individual User IDs must be used. Sharing IDs is not allowed.
- Eviden DAS IDs, or email addresses, must be used if possible.
- MFA, especially Eviden/Atos PKI, must be used if technology allows this.
- Passwords, if used, must comply to password policy requirements.
- Authentication must be disabled within 5 business days in case employee leaves the company.

Access rights:

- Access is granted/kept on a need to have basis with least privileges required to perform the assigned task.
- Role based access model (incl. using user groups) must be used if technology allows this. Cloud services should have a documented authorization matrix.
- Vendor/technology best practices, benchmarks and architect frameworks should be taken into consideration when implementing access rights.
- Extra (attention to) access controls must be implemented for access to (personal) data, utility programs (capable of bypassing normal operations or security procedures), secret authentication information and log information.
- Any newly granted access must be approved and approval records are stored for compliance purposes.
- Number of people having rights to manage access should be limited to the bare minimum.

- System logging must be enabled to log granting, updating and removing access rights activities if technology allows this. If not possible, an alternative solution should be available to demonstrate which access rights changes have been executed in a period of time (note: retain as long as needed).
- Access rights should be disabled/removed as soon as possible when there is no need to have (due to leaving or transfer of employee).
- Leaving employee access rights must be removed within 5 business days in case authentication cannot be disabled within that time-frame.
- Access rights must be reviewed at least quarterly.

Governance:

- User management procedures, and RACI, must be documented and agreed upon.
- The product owner is accountable for setup of service's user management.
- Management is accountable to initiate timely revocation of authentication and access rights in case their employees leave the company.
- A security incident should be raised in case user access has been compromised.
- Deviations from the principles and policies, which increase the security posture of the environment, must be addressed via risk management.
- Customer specific requirements, or responsibilities, need to be documented and agreed upon.

7.3.2 Workflow changing access rights

Request and authorized access rights

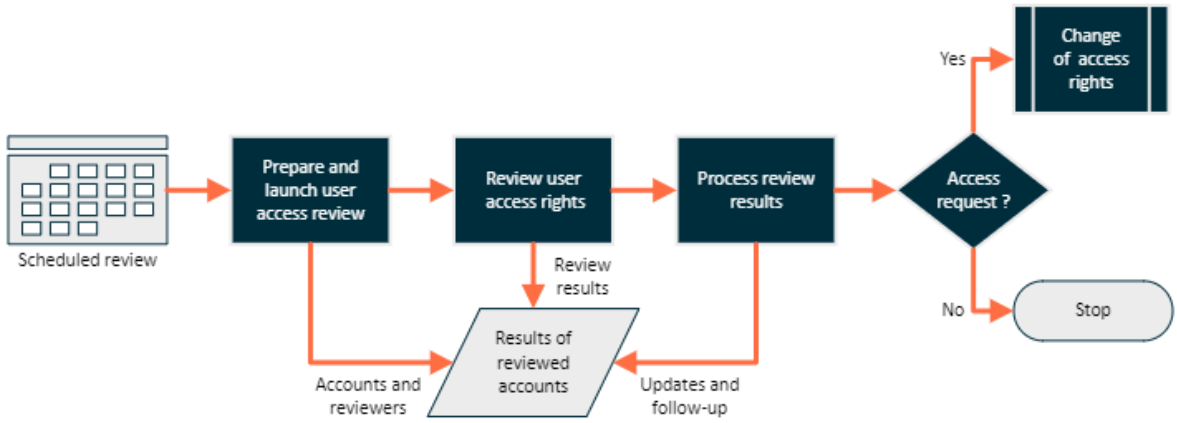
- Access is requested via defined way of working by authorized requesters.
- Depending of the way of working the approval needs to be done upfront or as part of the request. Check also any other requirement (eg. screening or geographical restrictions, segregation of duties).
- It is advised to use tooling (native functions or ticketing tool) for registration and approvals of access requests.
- Requests and approvals records need to be available for (retrospective) audits purposes.

Execute access request changes (designated user administrator team)

- Check for validness of the requested access and pre-requisites to execute it (approval, positive screening results, geographical restrictions, ...).

- Inform requester (and manager) when request is executed.

7.3.3 Workflow quarterly review of access rights



Prepare and launch (designated user administrator team, service responsible manager)

- By default this is executed by the designated user administrator team unless agreed otherwise.
- The Service Responsible Manager, of team needing the access, is accountable that the user review takes place, unless agreed differently.
- All user access rights in scope should be taken into account.
- It is advised to use (native) tooling to manage the review and store the results. See mandatory evidence.

Review user access rights (Service Responsible Manager or any designated reviewer)

- Review the user access request as requested within the requested time-frame.

Process review results (designated user administrator team, service responsible manager)

- Check if access has been reviewed and chase reviewers if not.
- Initiate access revocation request if access need to be revoked manually.
- Finalize and store user review evidence.

7.4 Mandatory evidence

The following evidence must be available, either documented or in systems/tooling:

- Applicable access model and authorization matrix.
- Applicable user management procedure and RACI.
- Approvals of granted access rights.
- List of granted, updated and removed access rights (incl. details) of (at least) last 15 months. Preferable system generated.
- List of employees, having access, who left the company in (at least) last 15 months.

- Per quarter an overview of all reviewed access rights, who performed the review, the review results per access right and any follow-up actions (eg. revocation of the access rights). User review results, including details and follow-up actions, of each quarter.

7.5 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 Eviden 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 Eviden 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).

Flowchart and description

Security Baseline Check

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

Analyse 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 Change

Issue change(s) to correct the deviations from the technical security baseline.

Implement Change

Implement changes to correct the security baseline deviation.

Request RAA

A signed Risk Acceptance Agreement must be created when a customer does not want to implement the advised technical security baseline setting

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 be able to retrieve
- Overview and details of related risks for deviations (see operational risk management).

7.6 Security Incident Management

The following types of security incidents can be distinguished:

- Service specific: These security incidents originate often from automated security monitoring (which is part of service) 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, it depends on the security incident criticality, complexity and contract agreements)

- Computer Security Incident Response (CSIRT) incidents reported by authorized caller are managed as part of separate BDS CSIRT Service, which may affect:
    - Multiple services delivered to multiple customers.
    - Single Customer who has contracted BDS CSIRT Service.
    - Single Customer who does not have contracted BDS CSIRT Service but requests for "ad hoc BDS CSIRT Service Support".

Those incidents are recorded via ITSM but tracking is done via dedicated CSIRT Reports which are stored in safe SP location where only authorized people have access
Coordination of:

- P1/P2 Security Incidents is under Security Incident Management Team (SIM Team) responsibility (for BDS CSIRT Customers)
- P3/P4 Security Incidents ais under CSIRT Management responsibility.
- Manage Detection and Response (MDR) Security Incidents coming from automated security monitoring deliver by AIsaaC solution, managed by separate BDS MDR Service. MDR Security incident can be triggered by :
    - Use Cases build-in AIsaaC Platform
    - Security Alerts coming from another security solutions integrated with AIsaaC.
    - MDR Security Incidents can be escalated to the CSIRT Team if proper criteria are met, Customer or another authorized person can do that if Customer has contracted CSIRT Service or there is agreement from availability and financial perspective to use "ad hoc BDS CSIRT Service Support." MDR Security Incidents are part of the MDR Security Threat Management Process described here.
    - Generic/local security incidents (not service related). Those do not directly affect a service to a customer. The GDC Security Officer coordinate those security incidents . Security Incident Reporting process is decreased in the Information Security Awareness Information Security Awareness

All 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 defined security incident management process (related to security incident types 1,3,4) Eviden CSIRT can be involved for further management. Involvement can be arranged via the assigned Quality, Security and Compliance Officers of the Business Line/GBU or another authorized person. In every AST for every customer a CSM (Client Security Manager) or SDM (Service delivery Manager) must be assigned. It is the task to define and execute together with the customer, based on Eviden best practices, the breach notification process. Internal Eviden communication/notification process is managed by Security Incident Management (SIM) Team in case of high priority security incidents. The CSM is not part of the OneCloud/BDS GDCs 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.

7.7 Security Monitoring and 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 – for OneCloud

- 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 Eviden Information Security Policy ASM-SEC-0001 which can be found on the Eviden 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 ITSM 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 Eviden must be reported according to the Eviden 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.

Flowchart and description

Security Event Definition, Log File and Security Even Monitoring

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

Definitions & agreements for BDS GDCs

Security Monitoring is delivered via:

- Service security functionality which is build-in in the service design to monitor security alerts on the service specific level.
- Standard portfolio BDS Service (Managed Detect and Response Service) to monitor security alerts coming from External and Internal Customers who have contracted MDR Service
- Non-standard BDS Services (delivered via non-standard SOCs and SIEM platform Teams) to monitor security alerts coming from External Customers who have contracted non-standard SOC/SIEM Service

Security Monitoring needs to be described in the service specific processes or procedures."

7.8 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.

7.9 Security Certificate Management

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

Flowchart and description

Check Expiry date

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.

Start Renewal

Issue a change request for certificates renewal. A standard change should have been defined for certificates renewal.

Purchase and Install

Ensure that the required certificates are purchased and timely made available to the operations engineer. Install the renewed certificates according to the work instructions as defined in the change request.

Update Certificate

Update the certificate register in order to reflect the new expiry date for the renewed certificate.

7.10 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

7.11 Network Vulnerability Scans

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

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 Eviden 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 Eviden Service Networks (ESN);
- All Eviden 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 Eviden Service Network 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 Business Line and maintained by the Quality, Security and Compliance Officer. This will enable Cloud dedicated reporting and control;
- The Internet Facing Infrastructure (IFI) and Eviden Network scans run every week; Execution of these scans is coordinated by Eviden 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.

Flowchart and description

Issue Change to Mitigate

Take the vulnerabilities from the GVM report and issue changes to mitigate those vulnerabilities or follow up with owners.

Implement Change

Implement changes to mitigate vulnerabilities or follow up with owners.

Mandatory evidence for Network Vulnerability Scans

- Changes requests for mitigation stored in ITSM
- Analyses and status of the internet facing vulnerabilities
- Analyses and status of the vulnerabilities in Eviden Network 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

7.12 Add Devices to Eviden Service Network

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

Definitions & agreements

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

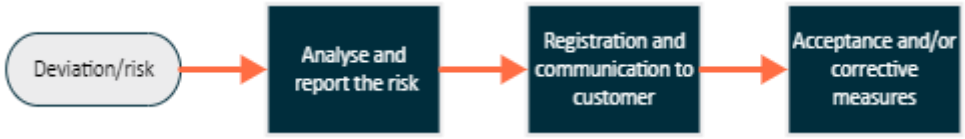
7.13 Operational Risk Management Process

This paragraph is related to managing risks during cloud operations. The objective of risk management is to identify, classify and address risks. In most cases these operational risks occur when there is a requested deviation from the contract or security standards. Eg. freeze patching for a group of servers. Therefor there are several ITCF controls referring to risk management in case of deviations.

Main principles

- Risks must be registered in a risk management tool (Eg. ART, MyRisks, ...).
- Risks must be communicated to the customer in case it concerns the security of the customer environments/data or our ability to adhere to the contractual agreements (or any other regulation).
- Communication of risks to customers must be formalized and documented.
- High risks should be formally accepted by customers by signing a risk letter or any other formal acceptance.
- Risk Acceptance Agreement (RAA): risk communicated to, and discussed with the customer. Formal acceptance in case of high risk.

Process flow



Activity	Ops engineer / TSM	Account Service Team	Customer
Analyse and report the risk.	R	A/I/C	
Register (and classify) the risk in risk management tool.	I	R/A	
Communicate risk to, and discuss with, the customer.		R/A	I/C
Accept the risk (formal if high).		C	R/A
Define corrective measures (if needed).	C	R	R/A

Mandatory evidence for Risk Acceptance Agreement

- Registered, and classified, risks in risk management tool.
- Documentation that risks are communicated to, and discussed with, the customer.
- Formal acceptance by customer in case of high risk.

7.14 Software as a Service Management Process

The goal of the SaaS Management process is to manage all external Cloud (IaaS, PaaS, SaaS) based services that are engaged by Eviden 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 Eviden Business Unit’s intention to engage the Vendor for External Cloud based Services.

- Eviden 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. Eviden Information Security Policy and Eviden 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 Eviden 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 Eviden Business wants to use for its employees must enforce Eviden 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.

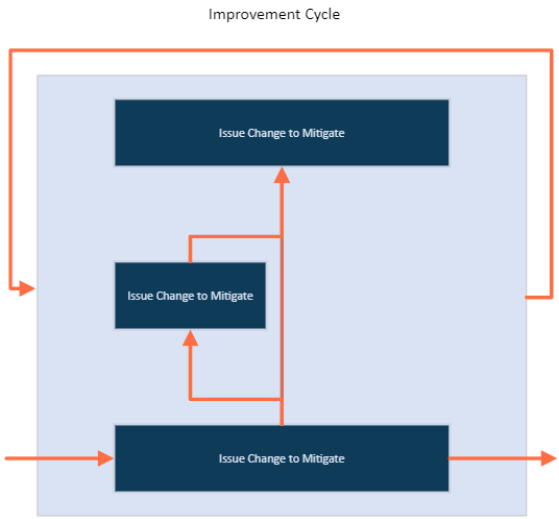
8 Monitoring – (Management) Controls

8.1 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 and BDS 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.
- Quality Records Environment can be represented by the following locations, depending on the service: Quality and Compliance Homepage OneCloud Evidence Repository (SDCC), local repository agreed with the (G)OSCO upfront.
- Recorded action points maintained during the service reviews in the Service Review documentation

8.2 Document Controls

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 Eviden Integrated Management System (EIMS). It belongs to Governance Risk and Compliance (GRC) activities, which are embedded in each Key Transversal Process defined by Eviden Group.

Definitions and Agreements

- Document control is based on the Eviden 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
        - Eviden office template should be used, if not, Eviden brand rules must be followed.
    - Strict control
        - Mandatory listing in the master index
        - 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
  - Eviden office template should be used, if not,Eviden 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, OneCloud 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 Eviden 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

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.

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 catalogue -> Atos Internal Service Catalogue -> 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.

8.3 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

8.4 Employee Screening

Reliability and integrity are the key elements for Service supply to our Customers. Eviden 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 Eviden 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 behaviour.
- 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

8.5 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 Operations Manual.

8.5.1 Eviden Integrated Management System

The AIMS defines the Eviden 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.

8.5.2 ISO and Compliance Audits guided by the Yearly Global Program

- The Eviden **IT Control Framework** describes the most important steps in the (ESMM) 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 Eviden IT control framework are audited. Documented evidence has to be provided to proof that Eviden is in control of the operation of the Customer IT infrastructure;

8.5.3 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, Pretesting, 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.

8.5.4 Audit Findings

- **Deviations** from the prescribed way-of-working are called **“findings”**;

- Findings are **classified** with
- finding **impact** (high, medium or low),
- finding **conformance** (major nonconformity, minor nonconformity or observation) and
- 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