



FitSM Foundation

6-7 Nov 2023

Foundation training in IT Service Management according
to FitSM

Version 3.0.1



This work has been funded by the European Commission.
It is licensed under a [Creative Commons Attribution 4.0
International License](https://creativecommons.org/licenses/by/4.0/).



Purpose of this training



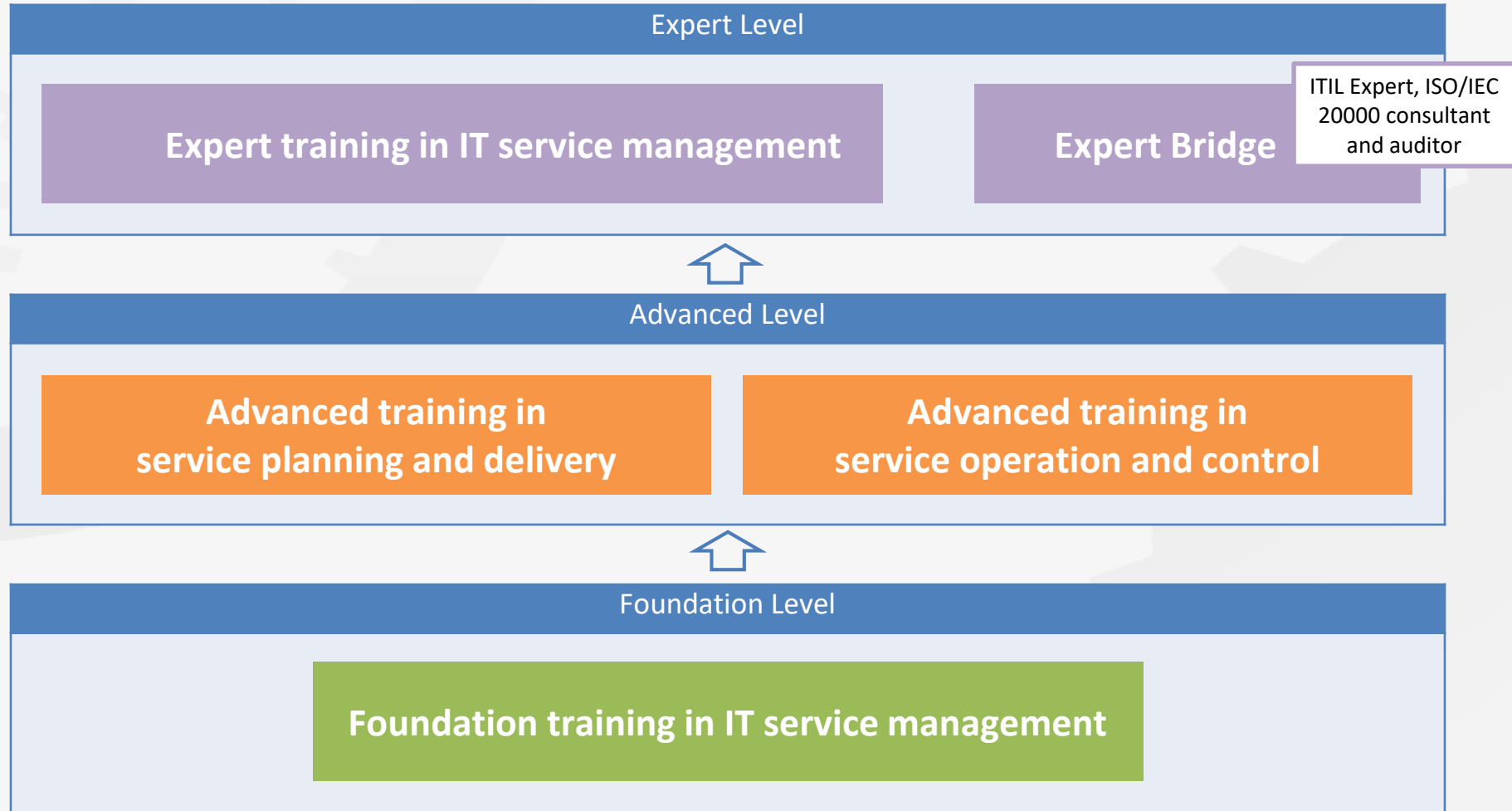
- Become familiar with
 - Basic IT service management concepts and terms
 - Purpose and structure of FitSM standards and their relationship to other standards
 - FitSM approach and key principles
 - Process framework underlying FitSM
 - Selected requirements defined in FitSM-1
- Achieve the ***Foundation Certificate in IT Service Management according to FitSM***

FitSM Foundation exam



- At the end of this training
- Closed book, i.e. no aids are allowed
- Duration: 30 minutes
- 20 multiple choice questions:
 - Four possible answers for each question: A, B, C or D
 - One correct answer per question
- At least 65% correct answers (13 of 20) are required to pass the examination

FitSM qualification program



Training agenda

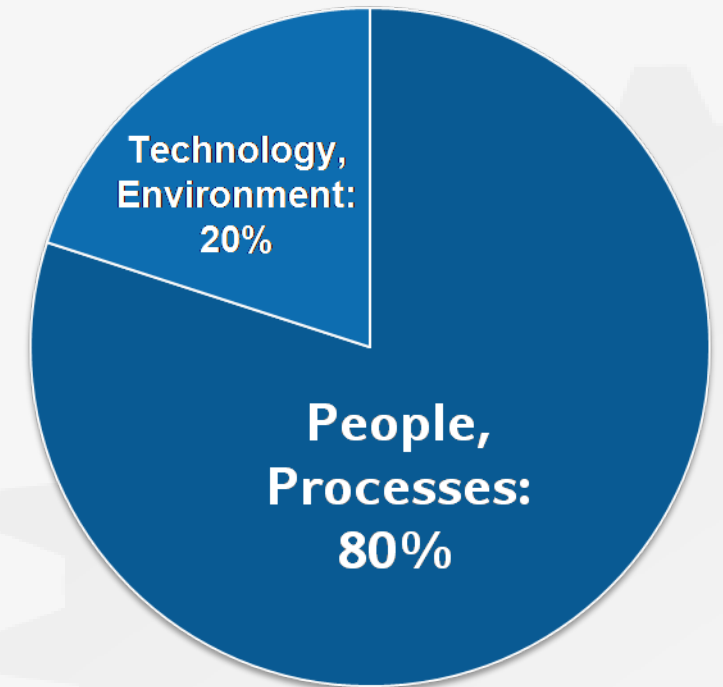
- IT Service Management: Introduction, Terms & Concepts
- The FitSM Approach & Standards Family
- IT Service Management – General Aspects
- IT Service Management – Processes
- Benefits, Risks & Challenges of Implementing IT Service Management
- Related Standards & Frameworks



IT Service Management: Introduction, Terms & Concepts

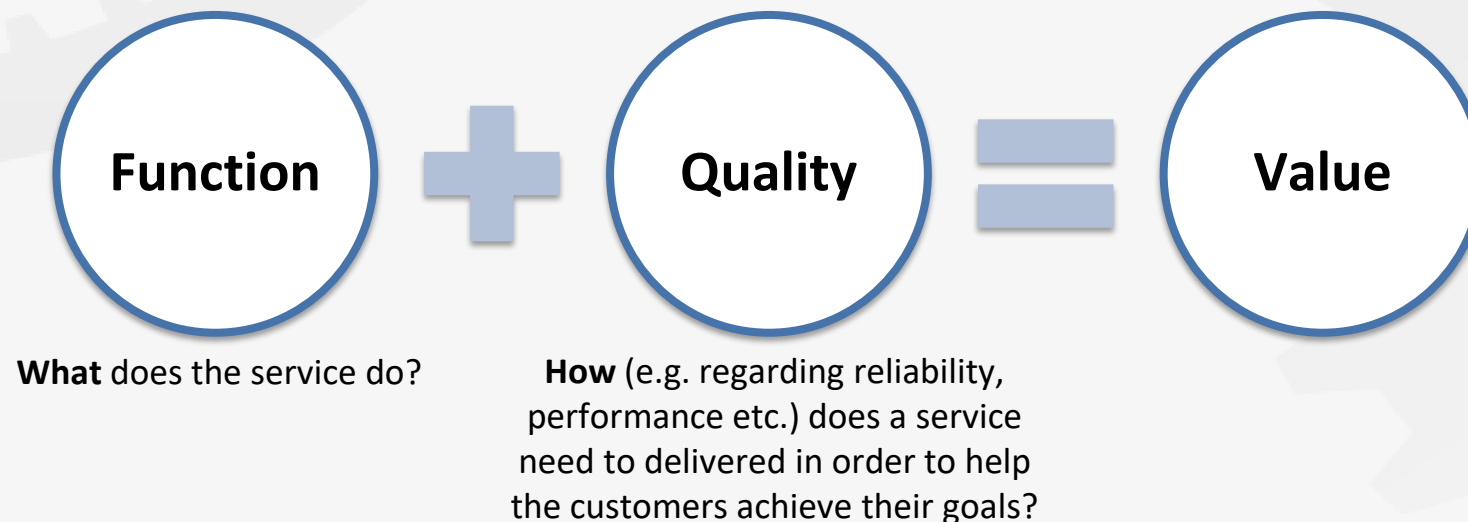
Why IT service management is needed

- Why IT service management (ITSM)?
 - A majority of IT service outages originate from "people and process issues"
 - Duration of outages and degradations significantly dependent on non-technical factors
- IT service management ...
 - ... aims at providing high quality IT services meeting customers' and users' expectations
 - ... by defining, establishing and maintaining service management processes.



Reasons for service outages

- Service is...
 - ... an intangible good that is delivered by a **service provider** to **customers**
 - ... something that provides **value** to the customers by helping them achieve their goals.
 - ...typically can be delivered / taken / ordered on its own



What is a service?

Definition following FitSM-0:

Service:

A way to provide *value* to a *user / customer* through bringing about results that they want to achieve

Examples of IT services:

- Provision of standard desktop workstations
- Connectivity: E-Mail, LAN, internet access
- Provision of computational resources
- Provision of standard and special applications
- Storage, backup, archival storage

Definition following FitSM-0:

Service provider:

Organisation or *federation* (or part of an organisation or *federation*) that manages and delivers a *service* or *services* to *customers*

What is a process?

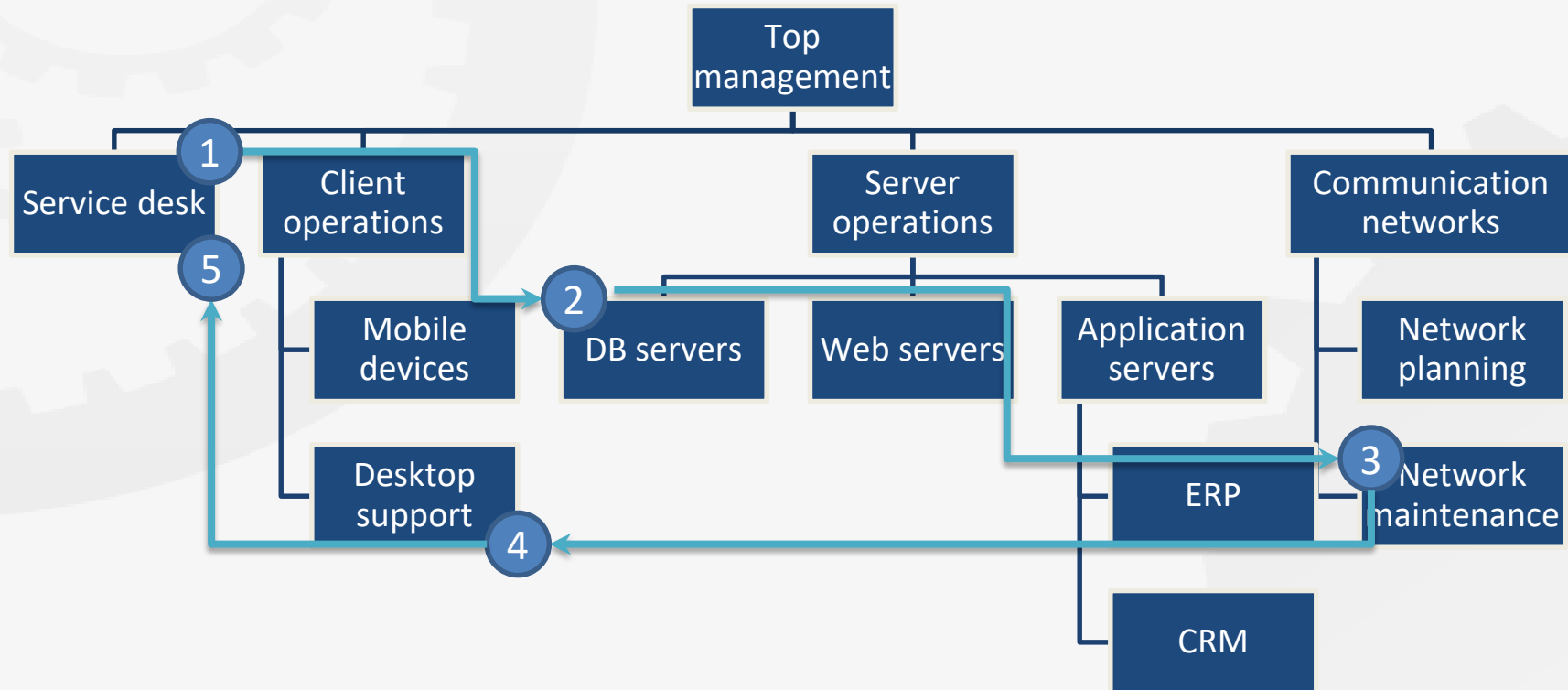
Definition following FitSM-0:

Process:

Structured set of *activities*, with clearly defined responsibilities, that bring about a specific objective or set of results from a set of defined inputs

- Key facts about ITSM processes:
 - ITSM processes support the delivery of IT services.
 - To provide one IT service to a customer, often several processes are needed.
 - An IT service being successfully delivered is the result from many processes successfully operating and interacting.
- The ITSM processes of an IT service provider are part of the **service management system (SMS)**.

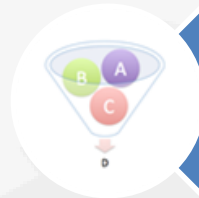
Organisational structure vs. process



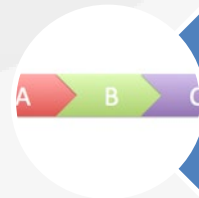
Most important elements of a process



Goal(s), objectives



Clearly defined inputs, triggers and outputs

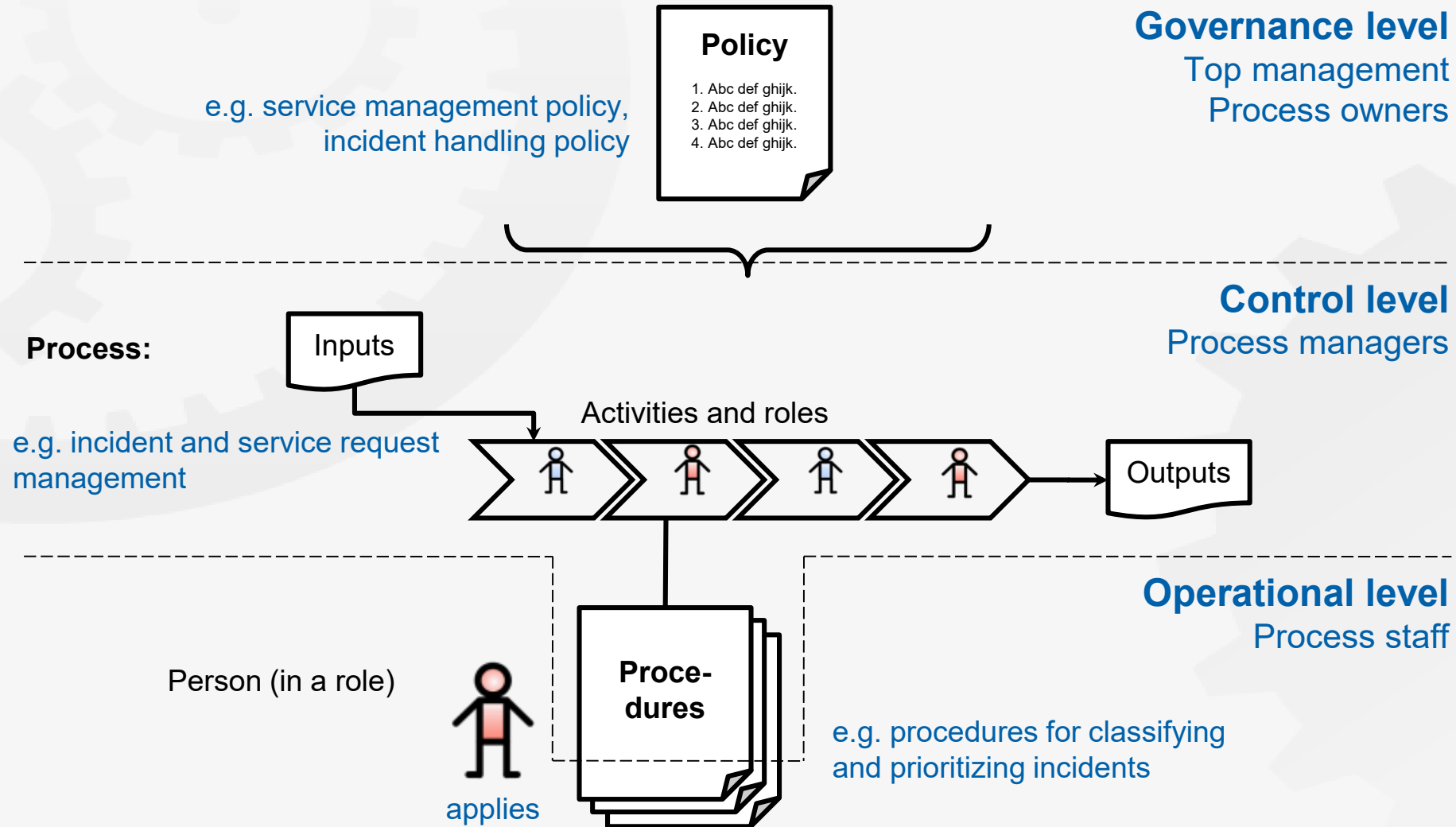


Set of interrelated activities
(across different functions)



Roles and responsibilities

Service management system (SMS): Overview



Service management system (SMS): Key terms



Definition following FitSM-0:

Service management system (SMS):

Overall *management system* that controls and supports management of *services* within an organisation or *federation*

Definition following FitSM-0:

Policy:

Documented set of intentions, expectations, goals, rules and requirements, often formally expressed by *top management* representatives in an organisation or *federation*

Definition following FitSM-0:

Activity:

Set of actions carried out within a *process*

Definition following FitSM-0:

Procedure:

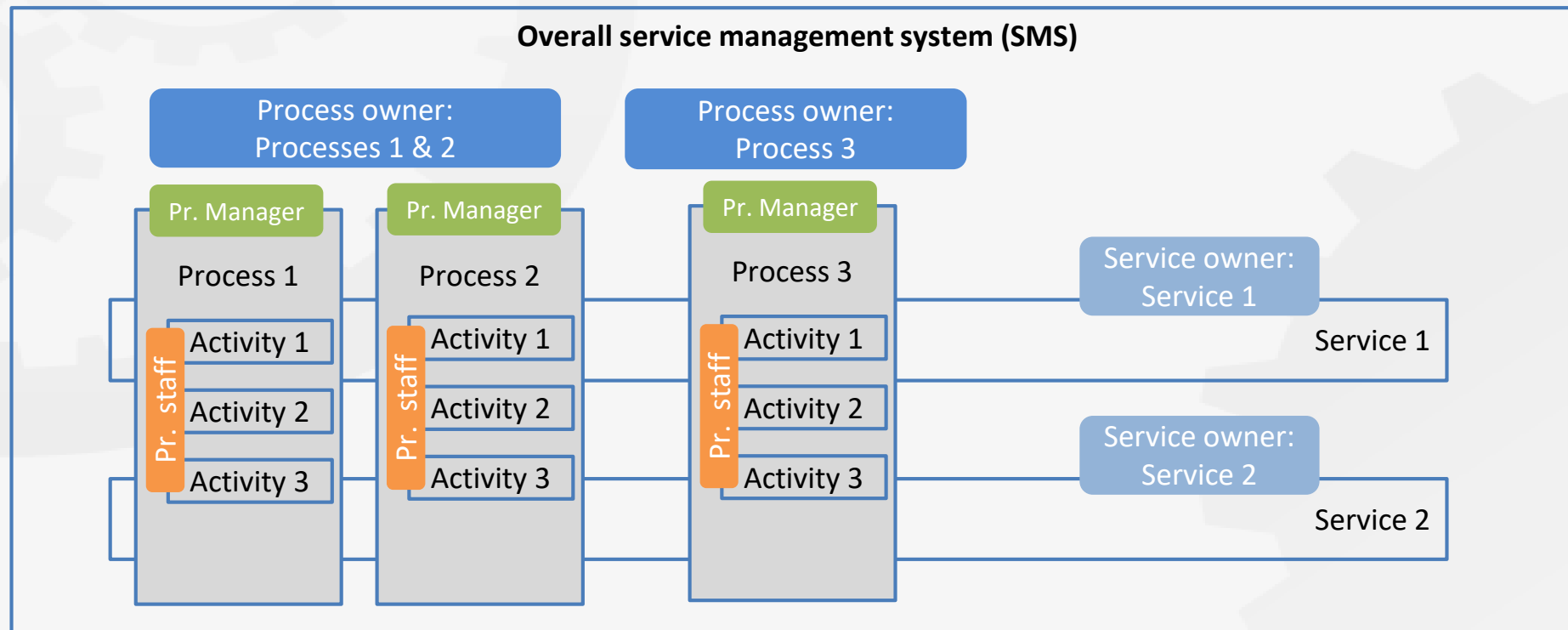
Specified set of steps or instructions to be carried out by an individual or group to perform one or more *activities* of a *process*

Service management system (SMS): Key roles



- Service owner:
 - Overall responsibility for a service
 - Maintains the service definition (in the service portfolio)
 - Acts as primary contact point and expert for this service
- Process owner:
 - Overall accountability for a process
 - Defines process goals, monitors their fulfillment
 - Has authority to provide / approve resources
- Process manager:
 - Responsible for the operational effectiveness and efficiency of a process
 - Reports to the process owner
- Process staff member:
 - Responsible for performing a specific process activity
 - Escalates exceptions to the process manager

Service management system (SMS): Key roles





The FitSM Approach & Standards Family

What is FitSM?



- A family of standards for lightweight IT service management
- Suitable for IT service providers of any type and scale
- Main design principle: Keep it simple!
- All parts (and this training material) freely available under Creative Commons licenses:

www.fitsm.eu



The development of the FitSM standards was supported and funded by the European Commission through the EC-FP7 project “FedSM”.

The FitSM approach



The key principles of the FitSM approach to managing IT services:

Practicality

Consistency

Sufficiency

Extendibility

The foundation for systematic IT Service Management:

Service- and
customer-orientation

Process-orientation

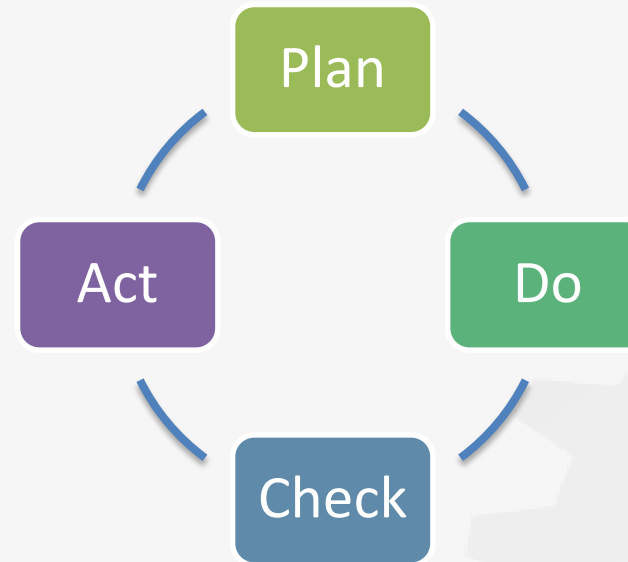
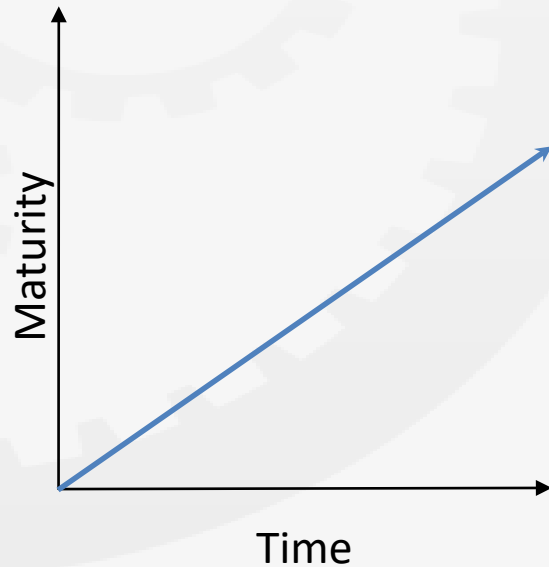
Continual
improvement

ITSM principles



Principle	Explanation
Service- and customer-orientation	<p>IT-driven solutions provided to customers and users are arranged as services and provided according to clearly defined service levels.</p> <p>Services are aligned to the needs and expectations of (potential) customers. Both the service provider and customer are aware of agreed service targets.</p>
Process-orientation	<p>Activities required to plan, deliver, operate and control services are carried out as part of well-understood and effective processes.</p>
Continual improvement	<p>The entire service management system follows the plan-do-check-act approach.</p> <p>All processes and activities necessary to manage IT services as well as the services themselves are subject to evaluation, aimed at identifying opportunities for improvement and taking appropriate follow-up actions.</p>

ITSM principles: Plan-Do-Check-Act cycle (PDCA)



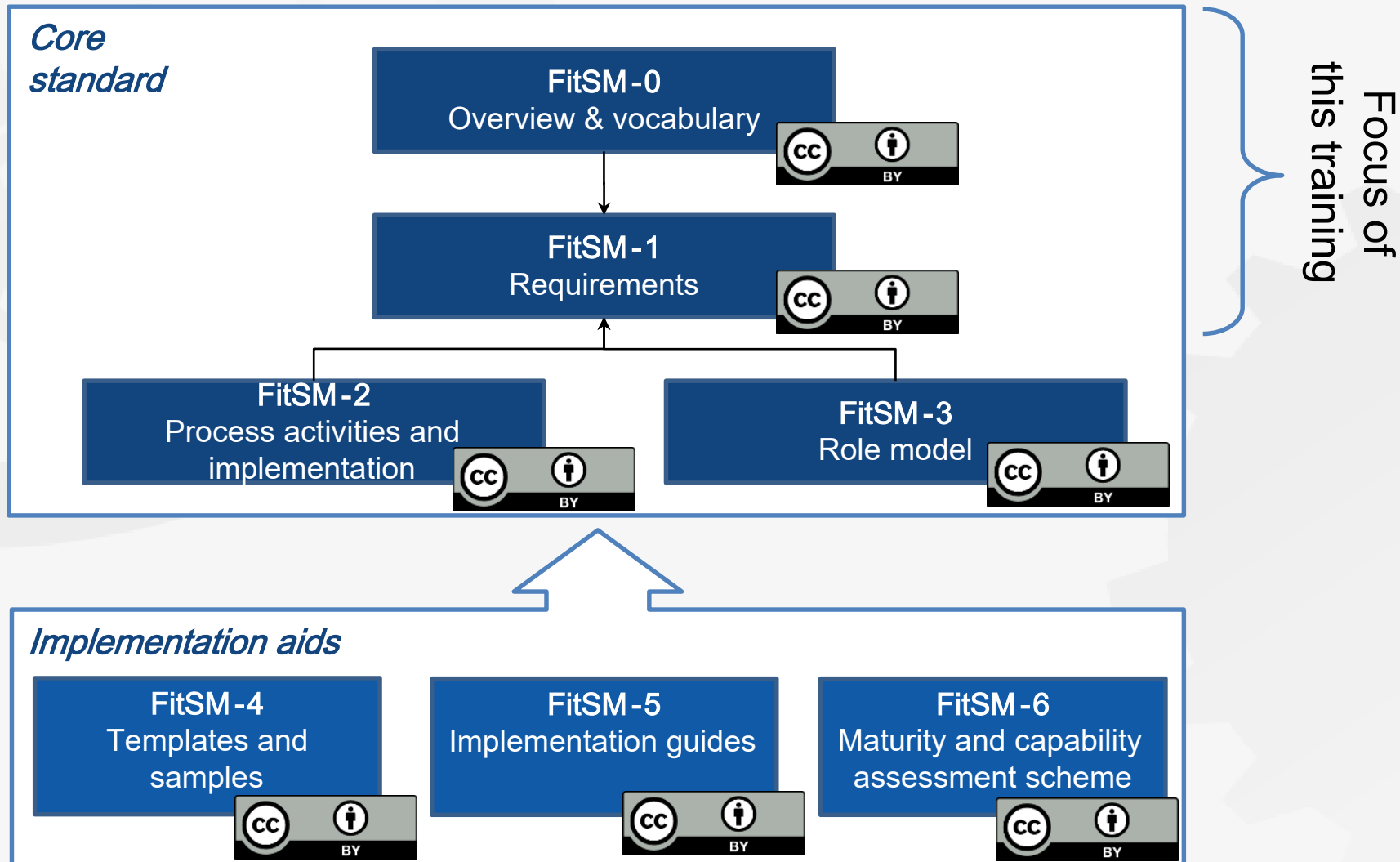
- Quality management approach according to W. E. Deming
- Key principle: continual improvement
- Plan-Do-Check-Act can be applied to the whole service management system

FitSM key principles

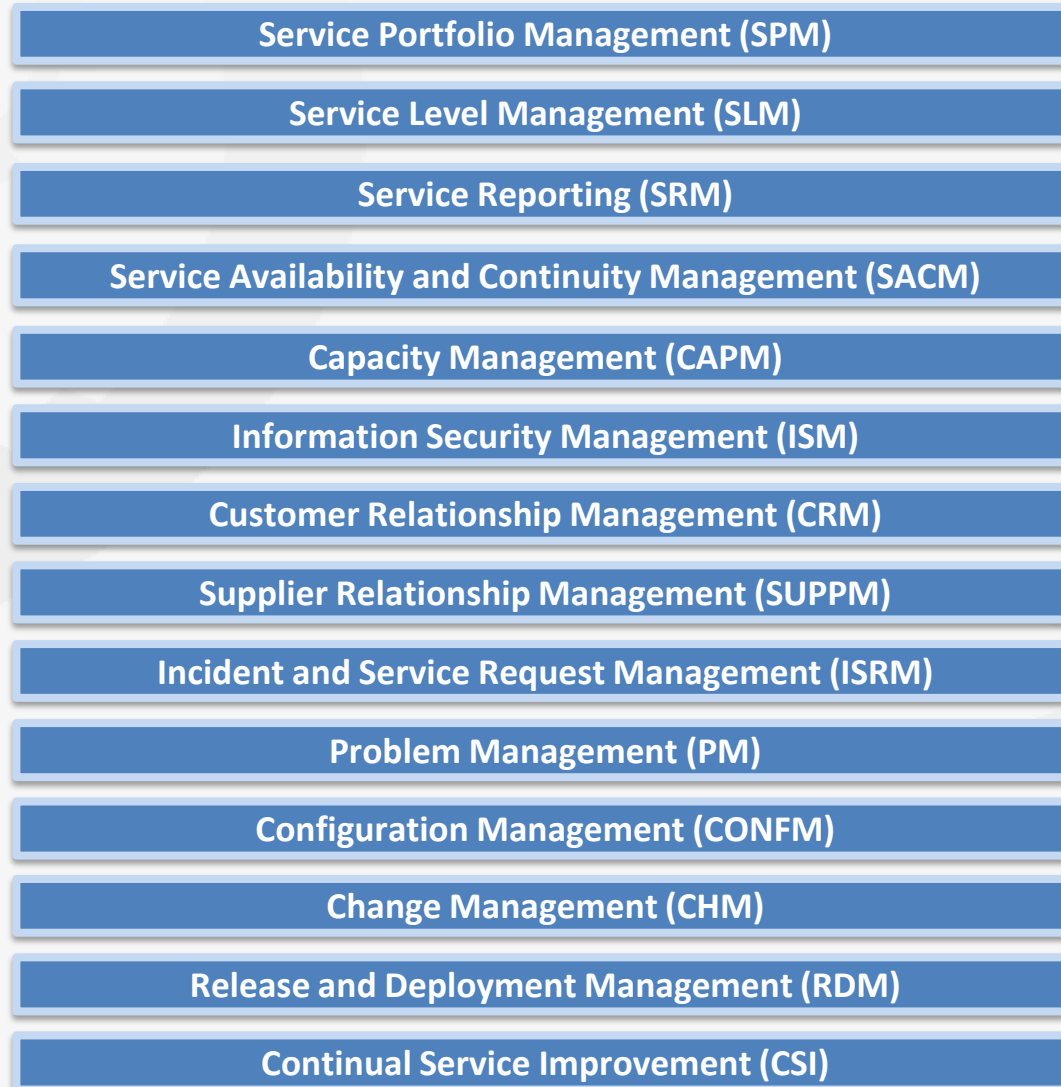


Principle	Explanation
Practicality	Apply simple, proven guidance instead of drowning in theoretical best practices
Consistency	Repeatable performance before detailed documentation
Sufficiency	Good enough and working over seeking the perfect solution
Extendibility	Leverage many sources of knowledge rather than live in a walled garden

FitSM parts



FitSM process model



A possible grouping of the FitSM processes



Two main topic areas:

Plan & Deliver

- SPM
- SLM
- SRM
- CRM
- SUPPM
- SACM
- CAPM
- ISM

Operate & Control

- CONFM
- CHM
- RDM
- ISRM
- PM
- CSI

FitSM-0: "Overview & vocabulary"



- FitSM-0 defines 80 important terms from the IT service management context – in alphabetical order:

- | | | | |
|--|-----------------------------------|-------------------------------------|-------------------------------------|
| – Activity | – Effectiveness | – Management review | – Service acceptance criteria (SAC) |
| – Assessment | – Efficiency | – Management system | – Service catalogue |
| – Audit | – Emergency change | – Maturity level | – Service component |
| – Availability | – Escalation | – Nonconformity | – Service level agreement (SLA) |
| – Availability of information | – Federation | – Operational level agreement (OLA) | – Service lifecycle |
| – Capability level | – Federation member | – Operational target | – Service management |
| – Capacity | – Federator | – Policy | – Service management plan |
| – Change | – Improvement | – Post implementation review (PIR) | – Service management system (SMS) |
| – Classification | – Incident | – Priority | – Service portfolio |
| – Closure | – Information security | – Problem | – Service provider |
| – Competence | – Information security control | – Procedure | – Service request |
| – Confidentiality of information | – Information security event | – Process | – Service review |
| – Conformity | – Information security incident | – Record | – Service target |
| – Configuration | – Integrity of information | – Release | – Supplier |
| – Configuration item (CI) | – IT service | – Release and deployment strategy | – Top management |
| – Configuration management database (CMDB) | – IT service management (ITSM) | – Report | – Underpinning agreement (UA) |
| – Continuity | – Key performance indicator (KPI) | – Request for change | – Underpinning contract (UC) |
| – Customer | – Known error | – Risk | – User |
| – Demand | – Major change | – Role | – Value |
| – Document | – Major incident | – Service | – Workaround |

FitSM-1: "Requirements"



- FitSM-1 defines 82 requirements that should be fulfilled by an organisation (or federation) offering IT services to customers.
- Compliance with the 82 requirements can be regarded as a "proof of effectiveness".
- The 82 requirements are structured as follows:
 - 17 general requirements (GR)
 - 65 process-specific requirements (PR)
 - Consideration of the 14 IT service management processes from the FitSM process model
 - Between 3 and 6 requirements per process

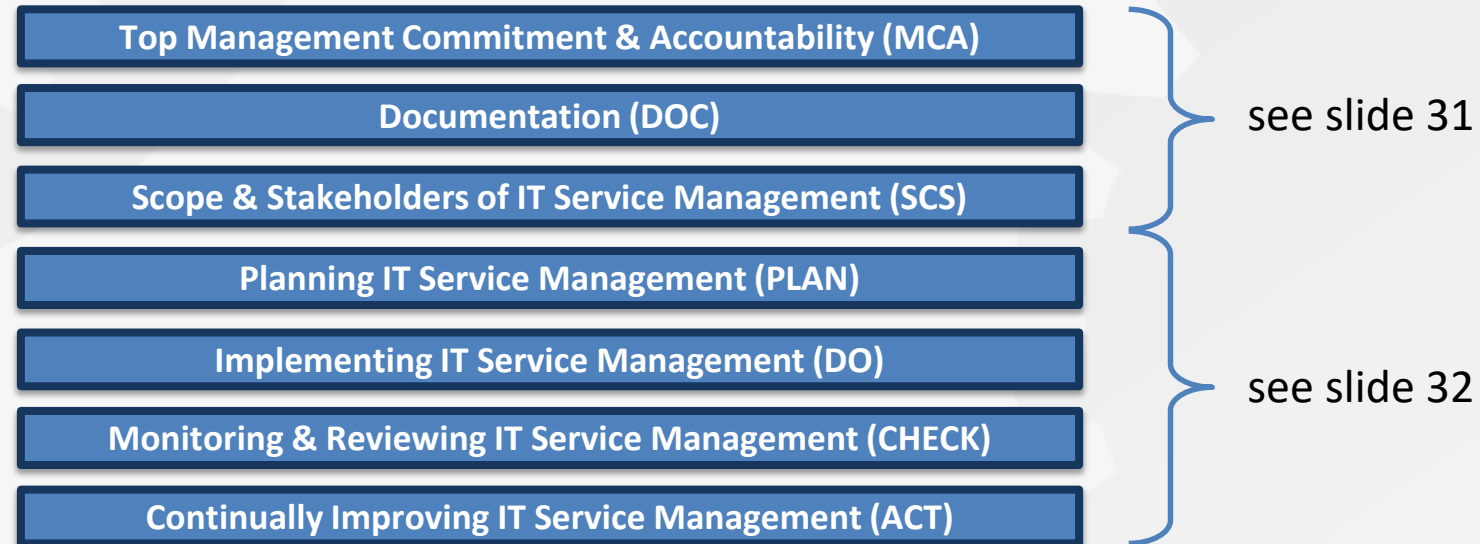


IT Service Management – General Aspects

General aspects: Overview



- General aspects of a service management system (SMS) cover all topics that are not directly related to a specific ITSM process.
- Topics to be considered:



ITSM – General aspects: Top management



GR1 MCA

- Top management commitment & accountability:
 - Assign one individual to be accountable for the overall SMS
 - Define and communicate goals
 - Define a general service management policy
 - Conduct management reviews

GR2 DOC

- Documentation:
 - Documentation to the extent necessary to support effective planning, including:
 - General service management policy
 - Service management plan and related plans (see GR4)
 - Definitions of all service management processes (see PR1-PR14)
 - Control of documentation, addressing as applicable:
 - Creation and approval
 - Communication and distribution
 - Review
 - Versioning and change tracking

PDCA applied to the SMS: Key concepts



GR3 SCS

GR4 PLAN

- Planning IT service management:
 - Define the scope of the SMS
 - Set the timeline for implementing service management processes (service management plan)

GR5 DO

- Implementing IT service management:
 - Implement processes as planned
 - Support and enforce practical application of defined processes

GR6 CHECK

- Monitoring & reviewing IT service management:
 - Monitor key performance indicators (KPIs) to evaluate effectiveness and efficiency
 - Perform assessments and / or (internal) audits to determine the level of compliance
 - Assess the organisational maturity

GR7 ACT

- Continually improving IT service management:
 - Identify nonconformities and deviations from goals
 - Take action -> Manage improvements through the CSI process (see PR14)

General aspects: Summary

- Most important things to remember:
 - Management buy-in is vital to the success of IT service management
 - Serious buy-in = mandate, resources, communication!
 - A certain level of documentation is necessary for effective processes
 - Only write documents that someone is going to read!
 - Embed the principles of continual improvement in the SMS, leveraging the PDCA approach



IT Service Management – Processes



Service Portfolio Management (SPM)

Objective

To maintain the service portfolio and to manage services through their lifecycle

What is a service?

Definition following FitSM-0:

Service:

A way to provide *value* to a *user / customer* through bringing about results that they want to achieve

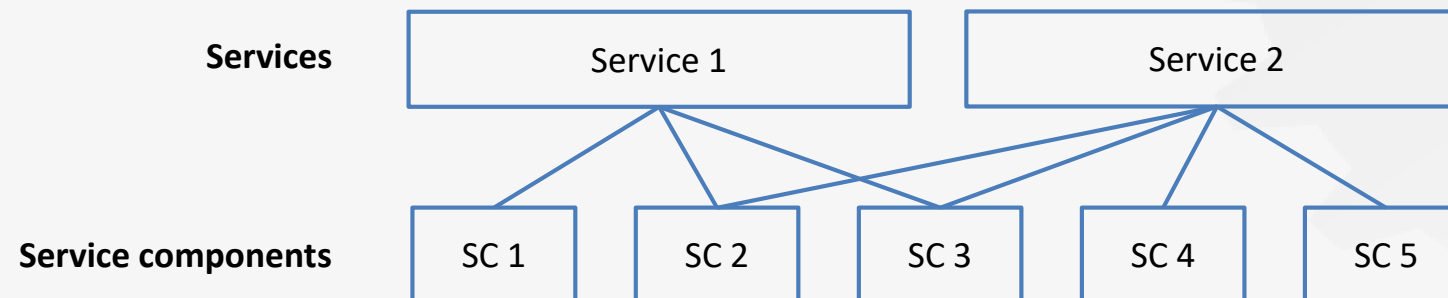
Definition following FitSM-0:

Service component:

Logical part of a *service* that provides a function enabling or enhancing a *service*

Note 1: A service is usually composed of several service components.

Note 2: A service component is usually built from one or more configuration items (CIs).



SPM: Important terms



Definition following FitSM-0:

Service portfolio:

Internal list that details all the *services* offered by a *service provider*, including those in preparation, live and discontinued

Definition following FitSM-0:

Service lifecycle:

The series of phases a *service* may move through in its lifetime

Note 1: Specific service lifecycle phases are typically defined for each organisation, depending on the complexity needed. These may include initial idea, proposal, design, development, deployment, production and retirement.

SPM: Requirements according to FitSM-1



PR1 Service Portfolio Management (SPM)

REQUIREMENTS

- PR1.1 A service portfolio shall be maintained. All services shall be specified as part of the service portfolio.
- PR1.2 Proposals for new or changed services shall be evaluated based on predicted demand, required resources and expected benefits.
- PR1.3 The evolution of services through their lifecycle shall be managed. This shall include the planning of new services and major alterations to existing services. Plans shall consider timescales, responsibilities, new or changed technology, communication and service acceptance criteria.
- PR1.4 For each service, the internal and external suppliers involved in delivering the service shall be identified, including, as relevant, federation members. Their contact points, roles and responsibilities shall be determined.

SPM: Key concepts



- The service portfolio lists and defines the services that a service provider offers or plans to offer in the future.
- The service portfolio is an "internal tool" for the service provider.
- Each service in the service portfolio follows a lifecycle consisting of different phases.
- The transition between service lifecycle phases requires coordination.



Service Level Management (SLM)

Objective

To maintain service catalogues, and to define and evaluate agreements on service quality with customers and suppliers

SLM: Important terms

Definition following FitSM-0:

Service catalogue:

Customer-facing list of all live services offered along with relevant information about these services

Definition following FitSM-0:

Service target:

Reference / target values for a parameter used to measure the performance of a *service*, listed in a *service level agreement (SLA)* related to this *service*

Note: Typical service targets include availability or resolution time for incidents.

Definition following FitSM-0:

Service level agreement (SLA):

Documented agreement between a *customer* and *service provider* that specifies the *service* to be provided and the *service targets* that define how it will be provided

SLM: Important terms



Definition following FitSM-0:

Operational level agreement (OLA):

Documented agreement between a *service provider* and an *internal supplier* that specifies the underpinning *service(s)* or *service component(s)* to be provided by the *internal supplier* or *federation member*, together with the related *service targets*

Definition following FitSM-0:

Underpinning agreement (UA):

Documented agreement between a *service provider* and an *external supplier* that specifies the underpinning *service(s)* or *service component(s)* to be provided by the *supplier*, and the *service targets* that define how it will be provided

Note: A UA can be seen as a service level agreement (SLA) with an external supplier where the service provider is in the customer role.

SLM: Requirements according to FitSM-1



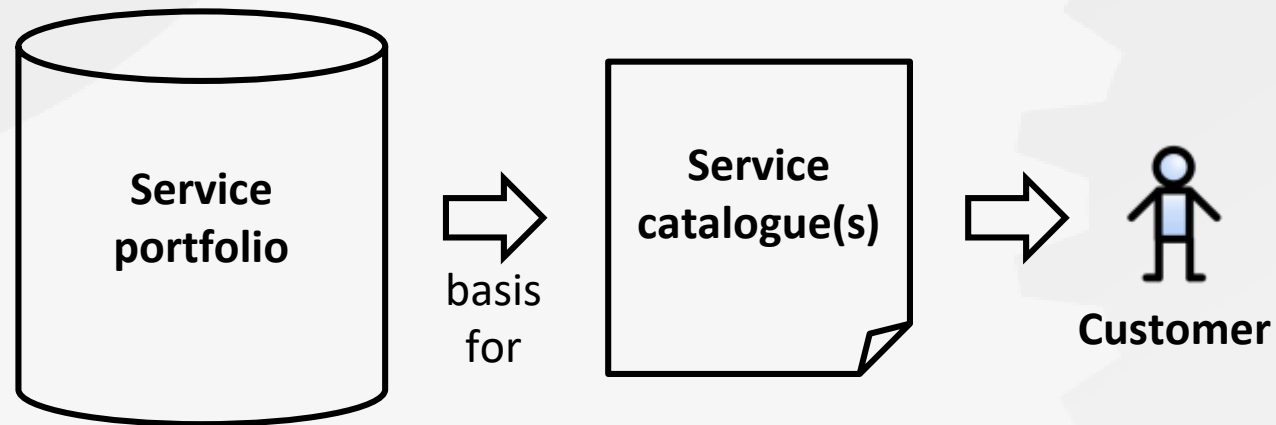
PR2 Service Level Management

REQUIREMENTS

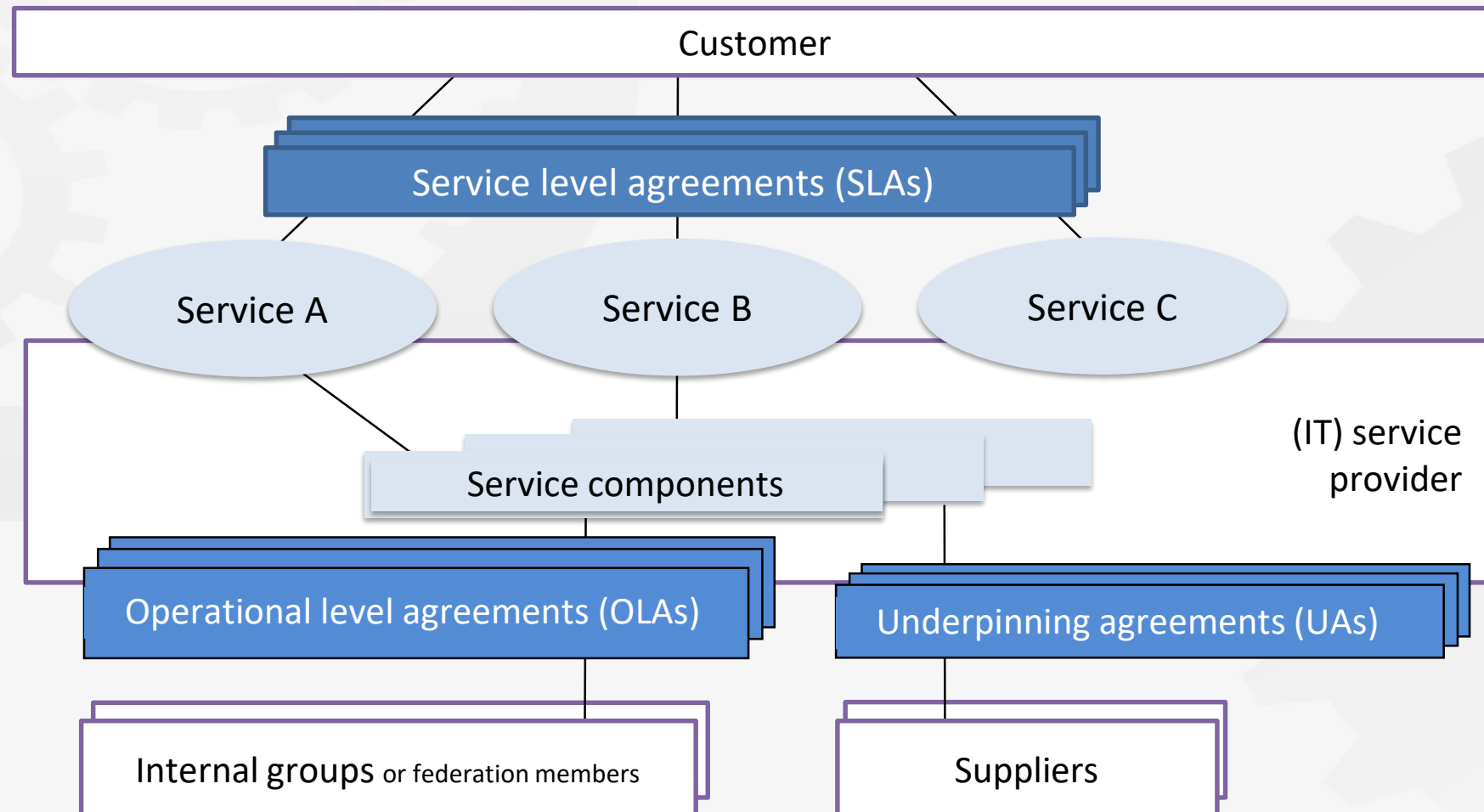
- PR2.1 A service catalogue shall be maintained.
- PR2.2 For all services delivered to customers, service level agreements (SLAs) shall be in place and reviewed at planned intervals.
- PR2.3 Service performance shall be evaluated against service targets defined in SLAs.
- PR2.4 For supporting services or service components, underpinning agreements (UAs) and operational level agreements (OLAs) shall be agreed as needed and reviewed at planned intervals.
- PR2.5 Performance of supporting services and service components shall be evaluated against targets defined in UAs and OLAs.

SLM: Key concepts – Service catalogue(s)

- While the service portfolio is an "internal tool" for the service provider, the service catalogue(s) is (are) facing the customer.
- The service portfolio is the basis for any service catalogue.



SLM: Key concepts – Types of service agreements and their relationships



SLM: Key concepts – Summary

- Produce a service catalogue for the customers and agree SLAs with customers.
- Agree OLAs and UAs with supporting parties and suppliers to ensure service targets in SLAs can be met.
- Evaluate service performance based on SLAs.
- SLAs provide information (e.g. service targets) vital as a basis for the execution of many other processes.



Service Reporting Management (SRM)

Objective

To specify reports on services and processes and ensure they are produced and delivered

SRM: Important terms

Definition following FitSM-0:

Report:

A structured *record* communicating results gathered through measurement, monitoring, assessment, *audit* or observation

Note: A common report generated from a service management system is a service report targeted to customers of a service that details the performance of that service versus the service targets defined in a service level agreement (SLA).

SRM: Requirements according to FitSM-1



PR3 Service Reporting

REQUIREMENTS

- PR3.1 Required reports shall be identified. Reporting shall cover performance of services and processes against defined targets, significant events and detected nonconformities.
- PR3.2 Reports shall be agreed with their recipients and specified. The specification of each report shall include its identity, purpose, audience, frequency, content, format and method of delivery.
- PR3.3 Reports shall be produced and delivered to their recipients according to specifications.

SRM: Key concepts



- Reports are important to support decision-making.
- Reports can be useful to demonstrate the level of service quality that has been achieved.
- Specify and agree the reports and their purpose, audience, frequency, content, format and method of delivery with the report stakeholders / recipients.
 - Reports agreed with customers are often set out in Service Level Agreements (SLAs)

Service Availability & Continuity Management (SACM)

Objective

To ensure sufficient service availability and continuity to meet service targets

SACM: Why availability AND continuity?



Availability

Goal: Service is available frequently enough to meet customer needs ☐ continuous operation

Guard against: downtime/unavailability through 'normal' failures and issues

Input: SLA

Output: Plans

Continuity

Goal: Sufficient disaster protection to ensure continual operation of key services under all circumstances

Guard against: downtime/unavailability through 'exceptional' failures, disasters and crises

Input: SLA, risk assessment

Output: Plans

SACM: Important terms



Definition following FitSM-0:

Availability:

The ability of a *service* or *service component* to fulfil its intended function at a specific time or over a specific period of time

$$\text{Availability [\%]} = \frac{\text{Agreed service hours} - \text{downtime}}{\text{Agreed service hours}} \times 100$$

Definition following FitSM-0:

Continuity:

Property of a *service* to maintain all or parts of its functionality, even in exceptional circumstances

Definition following FitSM-0:

Risk:

Possible negative occurrence that would have a negative impact on the *service provider's* ability to deliver agreed *services* to *customers*, or that would decrease the *value* generated through some *service*

SACM: Requirements according to FitSM-1



PR4 Service Continuity & Availability Management

REQUIREMENTS

- PR4.1 Service availability and continuity requirements shall be identified and reviewed at planned intervals, taking into consideration SLAs.
- PR4.2 Service availability and continuity risks shall be assessed at planned intervals.
- PR4.3 Appropriate measures shall be taken to reduce the probability and impact of identified availability and continuity risks and meet identified requirements.
- PR4.4 Availability of services and service components shall be monitored.

SACM: Key concepts

- Identify service availability and continuity requirements (e.g. from SLAs).
- Identify availability and continuity risks and plan to reduce their probability and impact.
- Produce service availability and continuity plan(s).
- Monitor service availability.



Capacity Management (CAPM)

Objective

To ensure sufficient capacity and service performance to meet service targets

CAPM: Important terms



Definition following FitSM-0:

Capacity:

Maximum extent to which a certain element of the infrastructure (such as a *configuration item*) can be used

Note: This might mean the total disk capacity or network bandwidth. It could also be the maximum transaction throughput of a system.

CAPM: Requirements according to FitSM-1

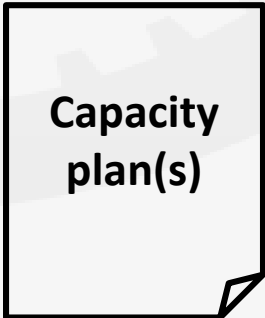


PR5 Capacity Management

REQUIREMENTS

- PR5.1 Service capacity and performance requirements shall be identified and reviewed at planned intervals, taking into consideration SLAs and predicted demand.
- PR5.2 Current capacity and utilisation shall be identified.
- PR5.3 Future capacity shall be planned to meet identified requirements, considering human, technical and financial resources.
- PR5.4 Performance of services and service components shall be analysed based on monitoring the degree of capacity utilisation and identifying operational warnings and exceptions.

- Service performance depends on sufficient capacity.
- Plan the resources required to fulfil the performance requirements (from SLAs) and produce a capacity plan.
- Key output from this process:

A rectangular icon with a folded bottom-right corner, containing the text "Capacity plan(s)".

**Capacity
plan(s)**

Typical contents:

- Agreed / required capacity and performance targets
- Planned capacity upgrades, downgrades and re-assignments of resources
- Requirements for capacity monitoring and related thresholds

- Monitor utilisation of key resources and evaluate service performance.

Information Security Management (ISM)

Objective

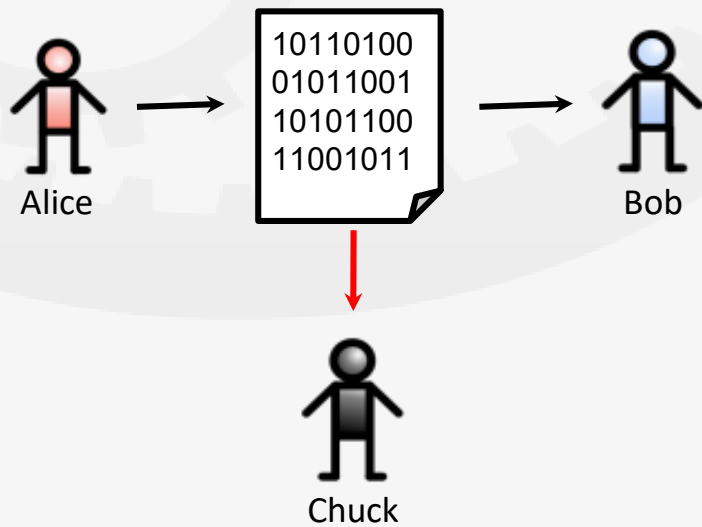
To preserve confidentiality, integrity and availability of information related to managing and delivering services

ISM: What is information security?

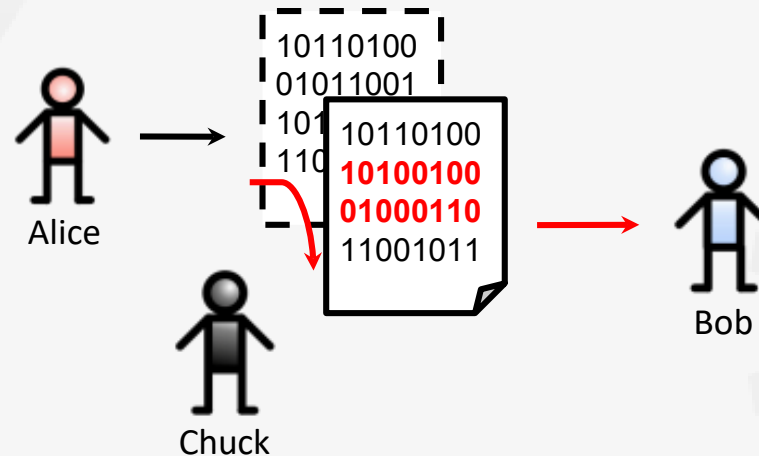
- Information security key aspects:
 - **Confidentiality**
 - **Integrity**
 - **Availability** of information

ISM: Confidentiality, integrity and availability

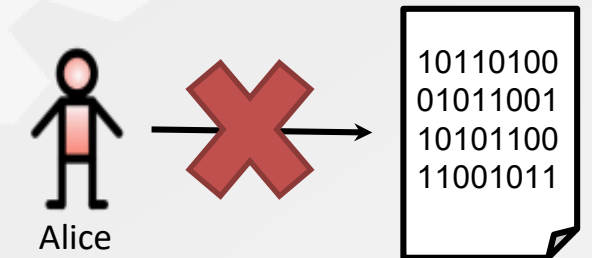
Confidentiality: To protect information from unauthorized disclosure



Integrity: To protect information from unauthorized modification



Availability of information: To protect information from loss



ISM: Requirements according to FitSM-1



PR6 Information Security Management

REQUIREMENTS

- PR6.1 Information security requirements shall be identified and information security policies defined and reviewed at planned intervals.
- PR6.2 Information security risks shall be assessed at planned intervals.
- PR6.3 Physical, technical and organizational information security controls shall be implemented to reduce the probability and impact of identified information security risks and meet identified requirements.
- PR6.4 Information security events and incidents shall be handled in a consistent manner.
- PR6.5 Access control, including provisioning of access rights, shall be carried out in a consistent manner.

- Most important outputs from this process:
 - Information security policies
 - Overall information security policy
 - Specific security policies, including password policy, mobile device policy, access control policy, media disposal policy, ...
 - Information security risk assessment
 - Documented information security controls
- Key objectives and activities:
 - Preserve confidentiality, integrity and accessibility of information assets.
 - Identify and treat information security risks.
 - Produce and enforce information security policies.



Customer Relationship Management (CRM)

Objective

To establish and maintain good relationships with customers receiving services

CRM: Important terms



Definition following FitSM-0:

Customer:

Organisation or part of an organisation that commissions a *service provider* in order to receive one or more *services*

Note: A customer usually represents a number of users.

Definition following FitSM-0:

User:

Individual that primarily benefits from and uses a *service*

CRM: Requirements according to FitSM-1



PR7 Customer Relationship Management

REQUIREMENTS

- PR7.1 Service customers shall be identified.
- PR7.2 For each customer, there shall be a designated contact responsible for managing the relationship with them.
- PR7.3 Channels used to communicate with each customer, including mechanisms for service ordering, escalation and complaint shall be established.
- PR7.4 Service reviews with customers shall be conducted at planned intervals.
- PR7.5 Service complaints from customers shall be handled in a consistent manner.
- PR7.6 Customer satisfaction shall be managed.

CRM: Key concepts

- Maintain information on customers (of IT services).
- Effectively communicate with customers.
- Perform service reviews and handle complaints.
- Understand and manage customer satisfaction.

Supplier Relationship Management (SUPPM)

Objective

To establish and maintain healthy relationships with internal and external suppliers and to monitor their performance

SUPPM: Important terms

Definition following FitSM-0:

Supplier:

Organisation or party that provides a (supporting) *service* or *service component(s)* to the *service provider*, which the *service provider* needs to provide *services* to their *customers / users*

Note: A supplier may be internal or external to the organisation of the service provider.

SUPPM: Requirements according to FitSM-1



PR8 Supplier Relationship Management

REQUIREMENTS

- PR8.1 Internal and external suppliers shall be identified.
- PR8.2 For each supplier, there shall be a designated contact responsible for managing the relationship with them.
- PR8.3 Channels used to communicate with each supplier, including escalation mechanisms, shall be established.
- PR8.4 Suppliers shall be evaluated at planned intervals.

SUPPM: Key concepts

- Maintain information on suppliers.
- Effectively communicate with suppliers.
- Monitor supplier performance.

Incident & Service Request Management (ISRM)

Objective

To restore agreed service operation after the occurrence of an incident and to respond to user service requests

ISRM: Important terms

Definition following FitSM-0:

Incident:

Unplanned disruption of operation in a *service* or *service component*, or degradation of service quality versus the expected or agreed service level or operational level according to *service level agreements (SLAs)*, *operational level agreements (OLAs)* and *underpinning agreements (UAs)* with suppliers

Definition following FitSM-0:

Service request:

User request for information, advice, access to a service or a change

Note: Service requests are often handled by the same process and tools as incidents.

ISRM: Requirements according to FitSM-1

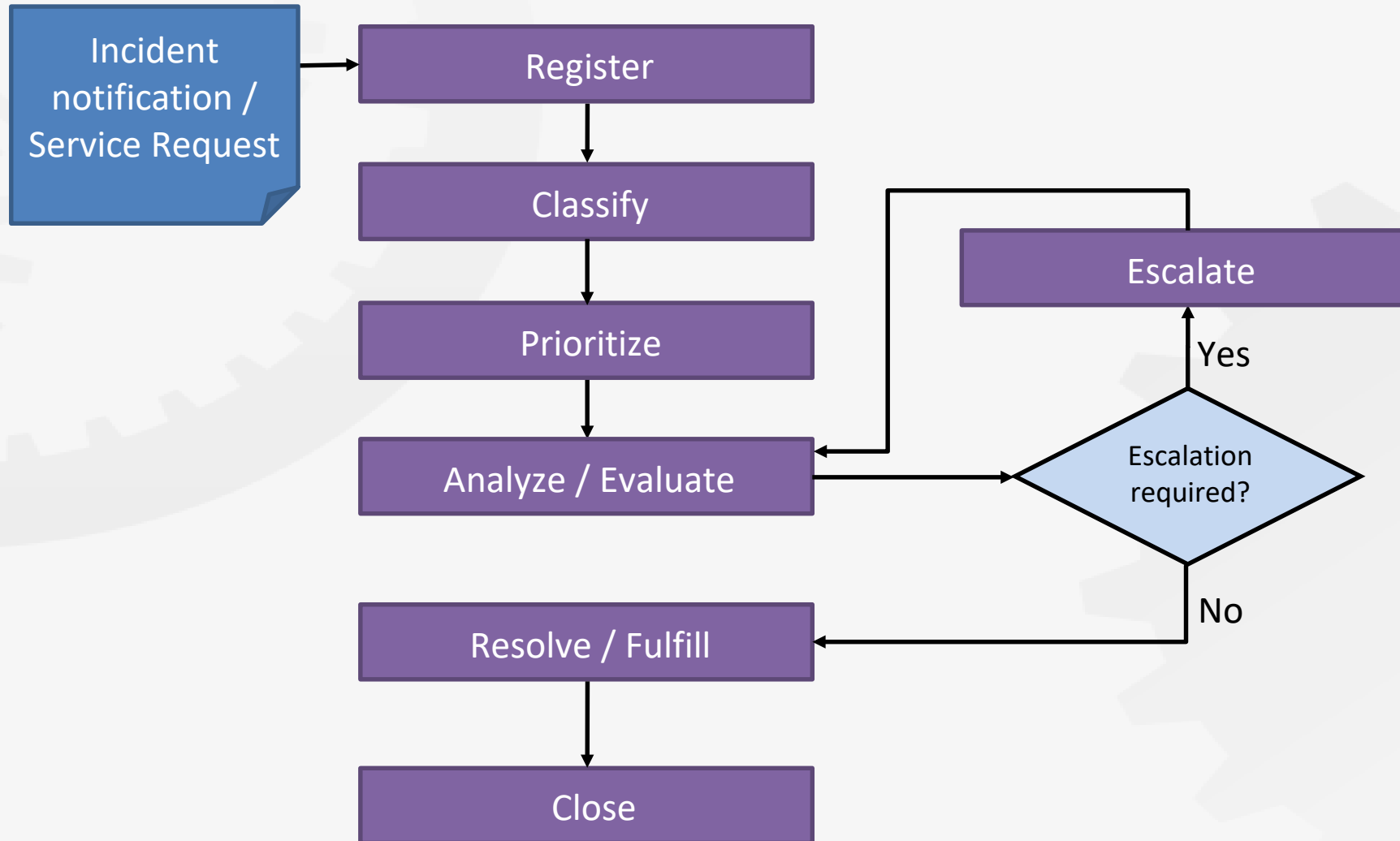


PR9 Incident & Service Request Management

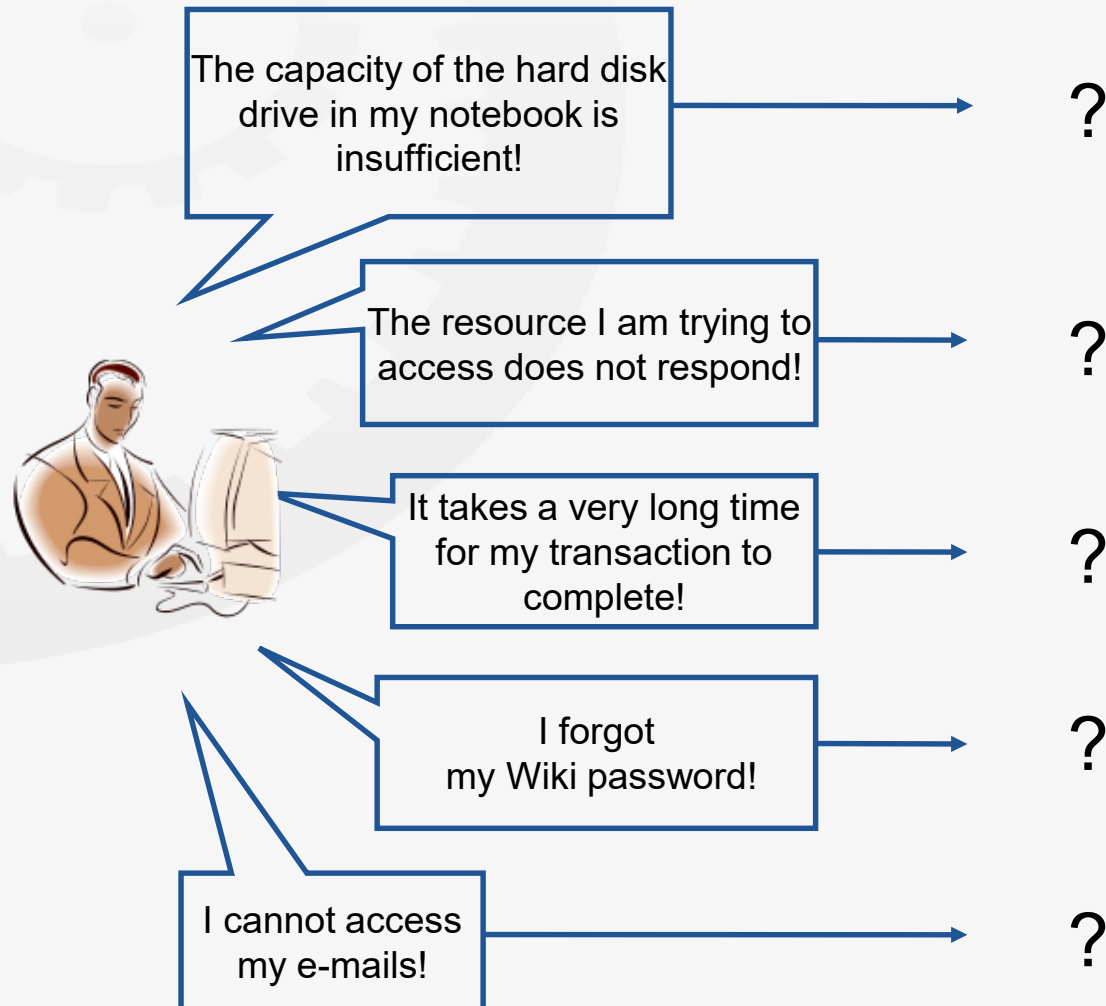
REQUIREMENTS

- PR9.1 All incidents and service requests shall be registered, classified and prioritized in a consistent manner, taking into account service targets from SLAs.
- PR9.2 Incidents shall be resolved and service requests fulfilled, taking into consideration information from SLAs and on known errors, as relevant.
- PR9.3 Functional and hierarchical escalation of incidents and service requests shall be carried out in a consistent manner.
- PR9.4 Customers and users shall be kept informed of the progress of incidents and service requests, as appropriate.
- PR9.5 Closure of incidents and service requests shall be carried out in a consistent manner.
- PR9.6 Major incidents shall be identified based on defined criteria, and handled in a consistent manner.

ISRM: Key concepts – Exemplary workflow



ISRM: Key concepts – Service request or incident?



ISRM: Key concepts – Summary

- Understand the difference between incidents (e.g. degradation of service, failure to meet service targets) and service requests (password reset, request for access or support).
- Follow a well-understood workflow in dealing with incidents and service requests.
- Make sure major incidents get appropriate attention.



Problem Management (PM)

Objective

To identify and investigate problems in order to reduce their impact or prevent them from causing further incidents

PM: Important terms



Definition following FitSM-0:

Problem:

The underlying cause of one or more *incidents* that requires further investigation to prevent *incidents* from recurring or reduce the negative impact on *services*

Definition following FitSM-0:

Known error:

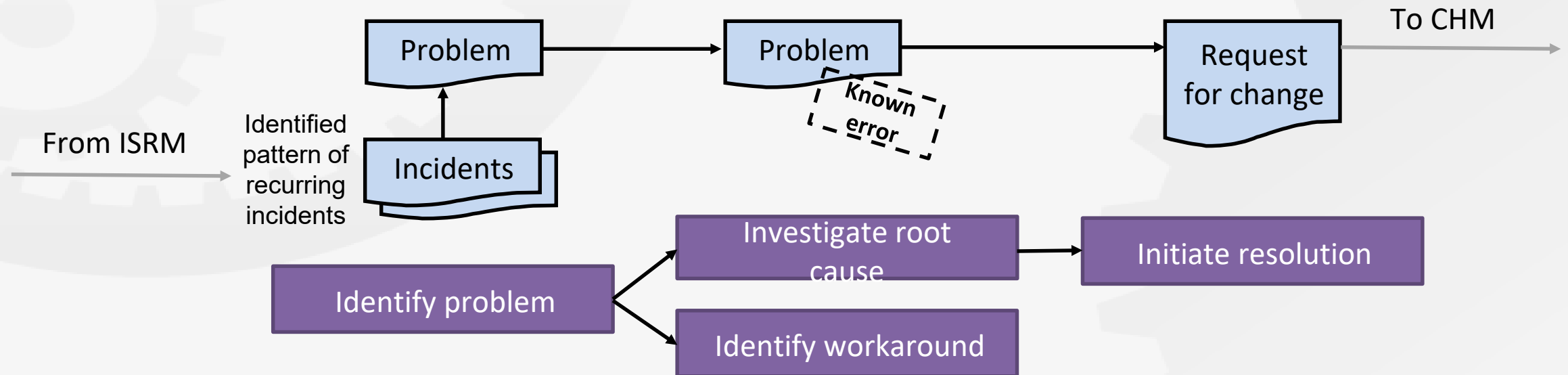
Problem which has not (yet) been resolved, but for which there are documented workarounds or measures to reduce or prevent negative impact on *services*

Definition following FitSM-0:

Workaround:

Means of circumventing or mitigating the symptoms of a *known error* that helps to resolve *incidents* caused by this *known error*, while the underlying root cause is not permanently eliminated

PM: Important terms – visualization



PM: Requirements according to FitSM-1



PR10 Problem Management

REQUIREMENTS

- PR10.1 Problems shall be identified and registered in a consistent manner, based on analysing patterns and trends in the occurrence of incidents.
- PR10.2 Problems shall be investigated to identify actions to resolve them or reduce their impact on services.
- PR10.3 If a problem is not permanently resolved, a known error shall be registered together with actions such as effective workarounds and temporary fixes.
- PR10.4 Up-to-date information on known errors and effective workarounds shall be maintained.

PM: Key concepts – From incidents to problems to resolutions

Incident & Service Request Management

Incidents

It takes a very long time for my transaction to complete!

->Incident re-occurred several times in the past weeks.



Problem Management: Analysis

Problem

- Category: SW/Service
- Impact: High (all users)
- Urgency: Low (no critical SLA violations)

Known error

- Error when writing log files causes job interruption
- Maximum file size of server log file exceeded

Problem Management: Treatment

Workaround

- Back-up log file
- Empty log file
- Reboot system

Resolution

- Patch available
- Request for Change: Install patch T12-02 on pclx3

PM: Key concepts – Summary

- Understand the difference between incidents and problems and how problems are identified based on patterns and trends in the occurrence of incidents.
- Understand the different ways in dealing with problems:
 - Workaround <- Known error
 - Resolution / elimination of the problem -> Change
- Provide information on known errors and workarounds to staff involved in ISRM.



Configuration Management (CONFM)

Objective

To provide and maintain a logical model of configuration items
in support of other service management activities

CONFM: Important terms

Definition following FitSM-0:

Configuration item (CI):

Element that contributes to the delivery of one or more *services* or *service components*, therefore requiring control of its *configuration*

Note: CIs can vary widely, from technical components (e.g. computer hardware, network components, software) to non-technical items such as documents (e.g. service level agreements, manuals, license documentation).

Definition following FitSM-0:

Configuration management database (CMDB):

Store for data about *configuration items (CIs)*

Note: A CMDB is not necessarily a single database covering all configuration items (CIs). It may rather be composed of multiple data stores.

CONFM: Requirements according to FitSM-1



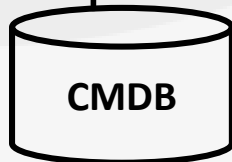
PR11 Configuration Management

REQUIREMENTS

- PR11.1 The scope of configuration management shall be defined together with the types of configuration items (CIs) and relationships to be considered.
- PR11.2 The level of detail of configuration information shall be sufficient to support effective control over CIs.
- PR11.3 Information on CIs and their relationships with other CIs shall be maintained in a configuration management database (CMDB).
- PR11.4 CIs shall be controlled and changes to CIs tracked in the CMDB.
- PR11.5 The information stored in the CMDB shall be verified at planned intervals.

CONFM: Key concepts

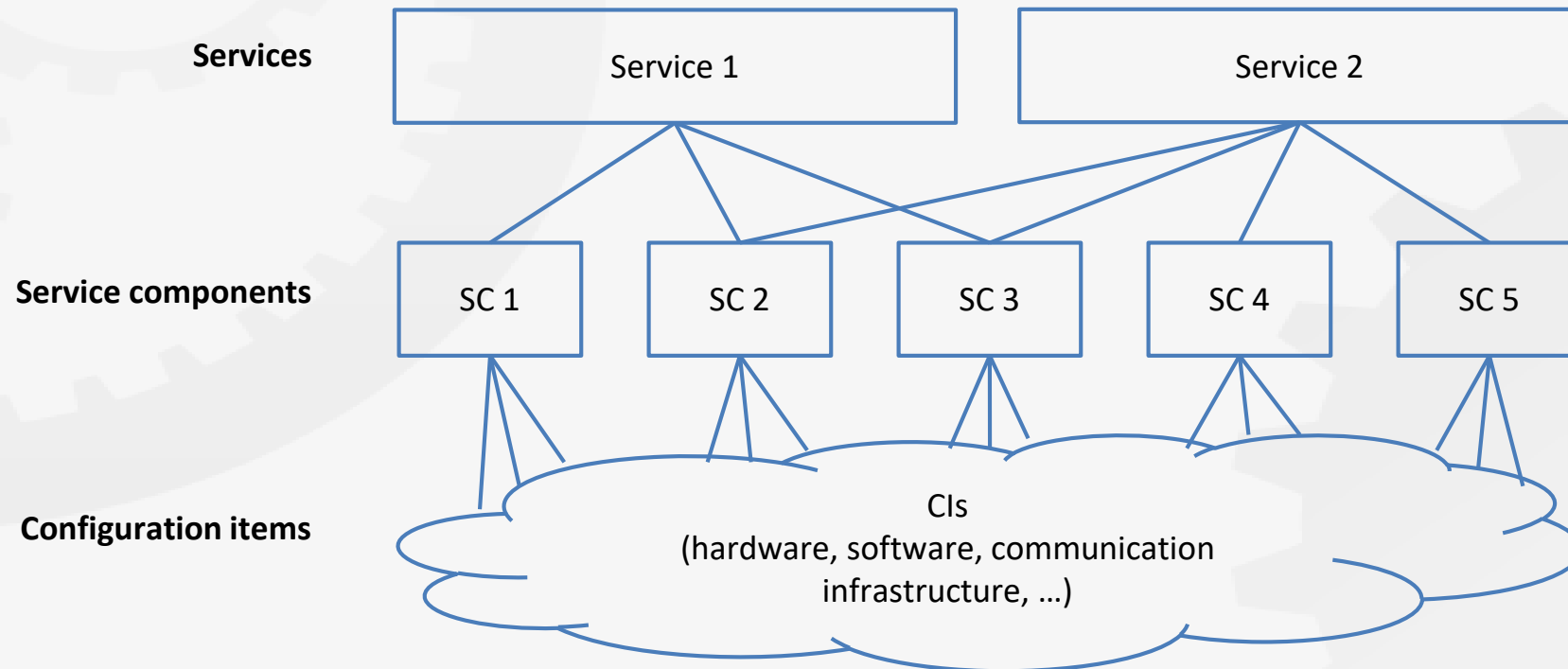
- Configuration Management is not about configuring resources.
- Configuration Management is about understanding (and documenting) CIs, their attributes and relationships.
- Select the adequate level of detail for your CMDB:
 - Too little detail = not enough control
 - Too much detail = excessive bureaucracy
- Most important output from this process:



Logical CMDB:

- Information on CIs, their attributes and relationships
 - Based on information from various sources (physical databases, asset inventories)
-
- The CMDB is a key source of information to staff involved in many other ITSM processes.

CONFM: Key concepts – Services, service components and CIs





Change Management (CHM)

Objective

To plan, approve and review changes in a controlled manner to avoid adverse impact on services

CHM: Important terms

Definition following FitSM-0:

Request for change (RFC):

Documented proposal for a *change*

Definition following FitSM-0:

Change:

Alteration (such as addition, removal, modification, replacement) of a *configuration item (CI)* or another entity that requires change control

CHM: Requirements according to FitSM-1

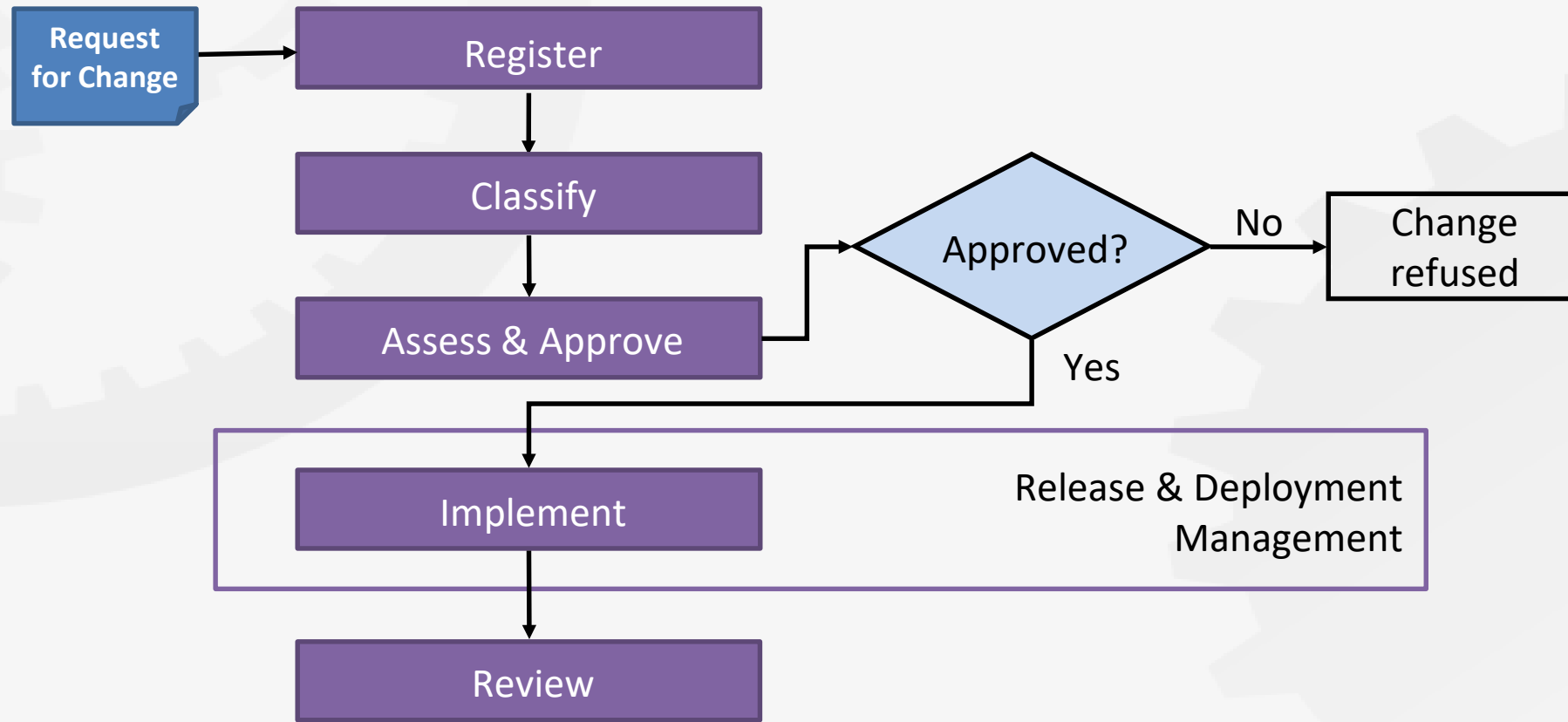


PR12 Change Management

REQUIREMENTS

- PR12.1 All changes shall be registered and classified in a consistent manner. Classification shall be based on defined criteria and consider different types of changes, including emergency changes and major changes.
- PR12.2 For each type of change, steps shall be defined for handling them in a consistent manner.
- PR12.3 Changes shall be assessed in a consistent manner, taking into consideration benefits, risks, potential impact, effort and technical feasibility.
- PR12.4 Changes shall be approved in a consistent manner. The required level of approval shall be determined based on defined criteria.
- PR12.5 Changes shall be subject to a post implementation review as needed, and closed in a consistent manner.
- PR12.6 A schedule of changes shall be maintained. It shall contain details of approved changes and intended deployment dates, which shall be communicated to interested parties.

CHM: Key concepts – Exemplary workflow



- Changes to CIs need to be reflected in the CMDB (interface to CONFM).
- Common types of changes:
 - Minor change (low / medium effort and impact)
 - > Some minor changes may be defined as pre-approved (often referred to as “standard changes”)
 - Major change (significant effort and impact)
 - Emergency change (very high priority / urgency)
- For changes requiring approval, define change authorities and approval mechanisms, such as a change advisory board (CAB).
- Many other ITSM processes will raise RFCs as a process output (and therefore trigger the CHM workflow).

Release & Deployment Management (RDM)

Objective

To bundle changes into appropriate types of releases and to effectively deploy them

RDM: Important terms

Definition following FitSM-0:

Release:

Set of one or more *changes* that are grouped together and deployed as a logical unit

Definition following FitSM-0:

Release and deployment strategy:

Approach taken to manage releases and their deployment for a given set of *service components* and related *configuration items (CIs)*, including organisational and technical aspects of planning, building, testing, evaluating, accepting and deploying releases

RDM: Requirements according to FitSM-1

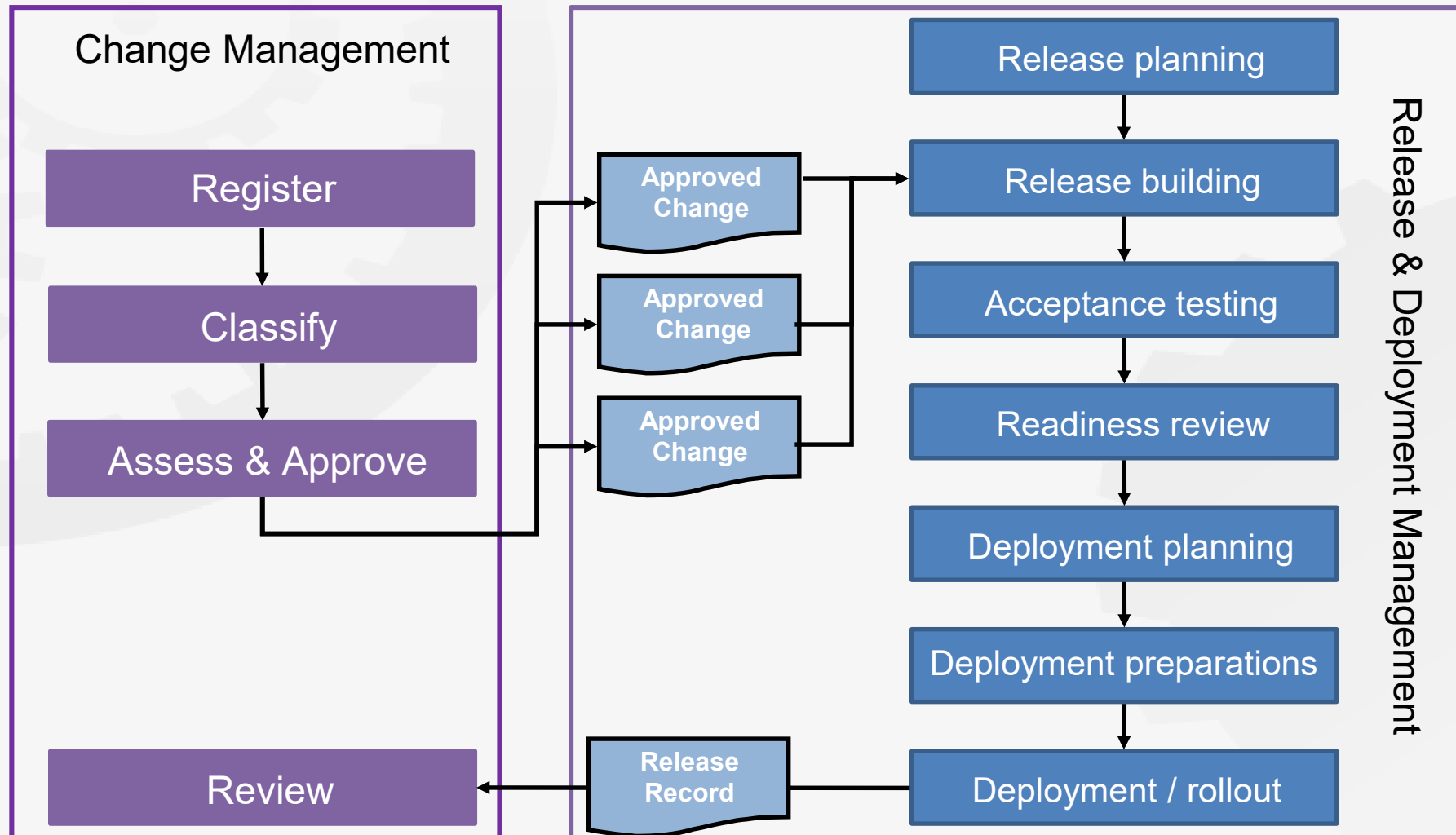


PR13 Release & Deployment Management

REQUIREMENTS

- PR13.1 Release and deployment strategies shall be defined, together with the service components and CIs to which they are applied. Strategies shall be aligned with the frequency and impact of releases as well as the technology supporting deployment.
- PR13.2 Criteria for including approved changes in a release shall be defined, taking into consideration the applicable release and deployment strategy.
- PR13.3 Deployment of releases shall be planned, including acceptance criteria, as needed.
- PR13.4 Releases shall be built, tested and evaluated against acceptance criteria prior to being deployed. The extent of release testing shall be appropriate to the type of release and its potential impact on services.
- PR13.5 Deployment preparation shall consider steps to be taken in case of unsuccessful deployment.
- PR13.6 Deployment activities shall be evaluated for success or failure.

RDM: Key concepts – Exemplary workflow



RDM: Key concepts – Release and deployment strategies



- In practice, service providers may apply different approaches to release and deployment. For example:
 - Traditional fixed release cycles - where minor and major releases are planned according to a long-term schedule, with emergency releases being deployed between release cycles as necessary.
 - Continuous development - a DevOps practice where changes to software source code are regularly merged into a central repository, followed by running automated builds and tests.

Continual Service Improvement Management (CSI)

Objective

To identify, prioritize, plan, implement and review improvements to services and service management

CSI: Important terms

Definition following FitSM-0:

Improvement:

Action or set of actions carried out to increase the level of *conformity*, *effectiveness* or *efficiency* of a *management system*, *process* or *activity*, or to increase the quality or performance of a *service* or *service component*

CSI: Requirements according to FitSM-1



PR14 Continual Service Improvement Management

REQUIREMENTS

- PR14.1 Opportunities for improvement of services and processes shall be identified and registered, based on reports as well as results from measurements, assessments and audits of the SMS.
- PR14.2 Opportunities for improvement shall be evaluated in a consistent manner and actions to address them identified.
- PR14.3 The implementation of actions for improvement shall be controlled in a consistent manner.

- Subject to continual improvement:
 - Services (including underlying service components)
 - The SMS, including all ITSM processes
- Typical sources of improvements: KPI reports, service reviews, internal audits, management reviews, internal suggestions / feedback.
- Ensure that improvements are taken seriously, addressed and tracked.
- In creating a culture of continual improvement, the CSI process is an extension of the general requirements on continually improving IT service management (GR7: ACT).

Benefits, Risks & Challenges of Implementing IT Service Management

ITSM: Benefits and risks in practice

Typical benefits (excerpt):

- + Understand organization (federation) structure
- + Customer focus, alignment of IT and their customers
- + Repeatability of desired outputs
- + Higher effectiveness and efficiency
- + Reduce organization fragmentation / silos
- + Facilitate/capture innovation
- + Improved reputation

Potential risks (excerpt):

- Processes and procedures may become too bureaucratic, more paperwork
- Lower effectiveness and efficiency, if ...
 - Staff are not aware of processes and measures
 - Top management lacks a clear commitment and related actions
 - Personnel do not accept the system
 - Processes are bypassed

Federated IT service provisioning

Definition following FitSM-0:

Federation:

Situation in which multiple parties, the *federation members*, jointly contribute to the delivery of *services to customers* without being organised in a strict hierarchical setup or supply chain

Examples of federated IT service provisioning:

- In a large commercial enterprise / corporation with various business units / divisions: Multiple service providers need to cooperate to deliver a coherent data warehouse service for the whole corporation.
- In public administration: Different government agencies and national bodies jointly operate a public health data service.
- In a network of academic research organisations (e.g. a scientific research collaboration): Multiple IT departments / data centers provide resources for a very large scale computing service used by many researchers.

Federated IT service provisioning: Comparison with non-federated IT service provisioning



	Non-federated (“traditional”) IT service provisioning	Federated IT service provisioning
Service provider model	One organisation acting as the service provider with (sub-) contracted suppliers -> Supply chain	Multiple organisations collaborating and jointly acting as a service provider -> Supply network
Control over <ul style="list-style-type: none"> • Service components • Service management processes / activities • Suppliers 	Single central control by the organisation acting as the service provider	Shared / distributed control among the collaborating organisations
Impact on the SMS	Clear authorities, hierarchical control	Potentially more difficult to control, more ambiguity -> Requires more effort to clarify responsibilities and interfaces



Standards for lightweight
IT service management



Related Standards & Frameworks

ITIL, ISO/IEC 20000 and ISO/IEC 27000

ITIL	ITIL <ul style="list-style-type: none">• Number of “good practices” in IT service management• Descriptions of key principles, concepts and practices in ITSM	<ul style="list-style-type: none">• Popular and wide-spread framework• Published in the form of books• Not auditable
ISO/IEC 20000	ISO/IEC 20000 <ul style="list-style-type: none">• International standard for service management• Requirements for a service management system (SMS)	<ul style="list-style-type: none">• Applicable to organisations providing IT services• Auditable, certifiable
ISO/IEC 27000	ISO/IEC 27000 <ul style="list-style-type: none">• International standard for information security management• Requirements for an information security management system (ISMS)• Defines a number of security controls	<ul style="list-style-type: none">• Applicable to all organisations and branches• Auditable, certifiable