



Standards for lightweight
IT service management

FitSM Foundation

Foundation training in IT Service Management according to FitSM

Version 2.11



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



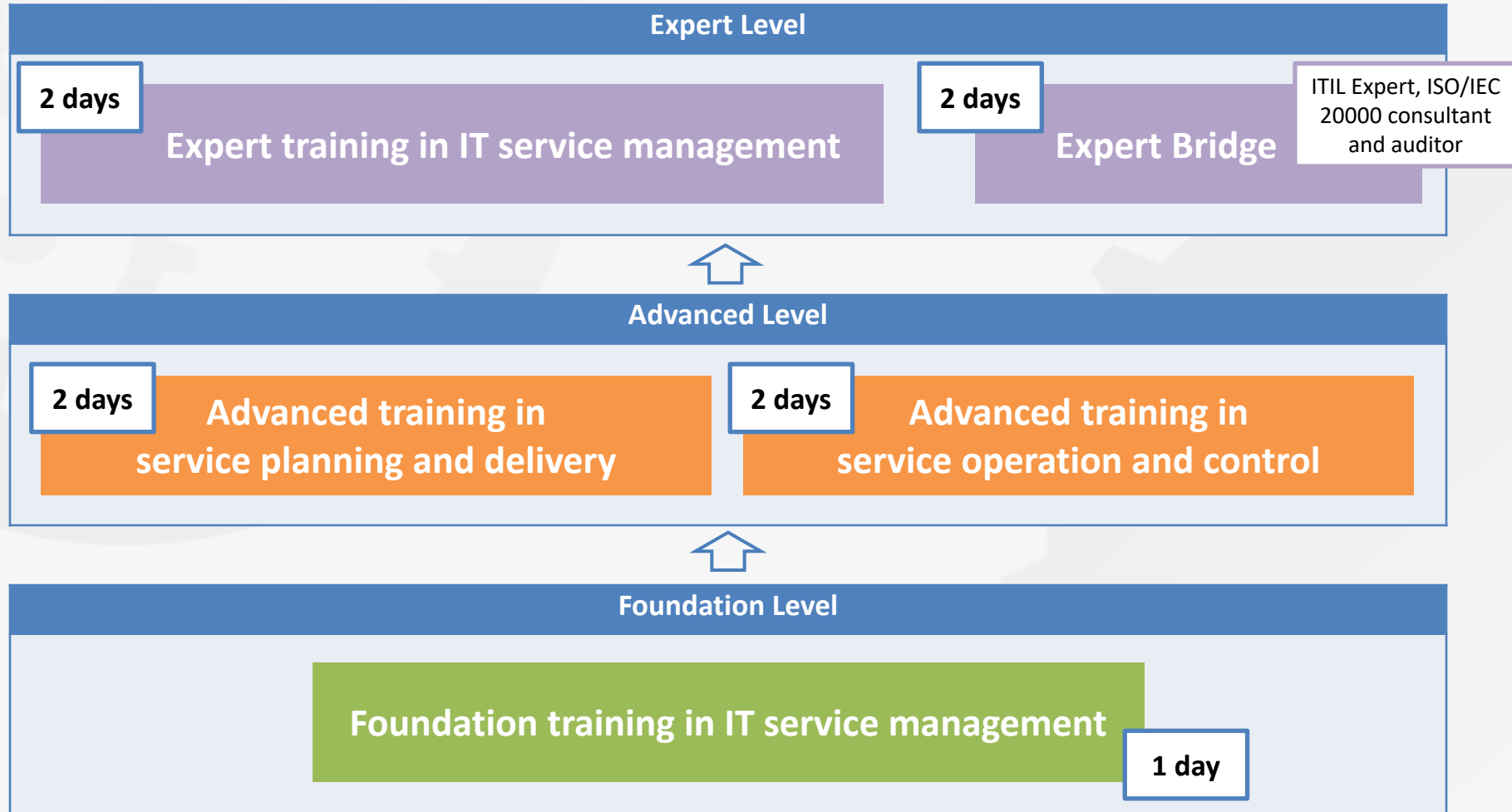
- Become familiar with
 - Basic IT service management concepts and terms
 - Purpose and structure of FitSM standards and their relationship to other standards
 - Process framework underlying FitSM
 - Requirements defined in FitSM-1
- Achieve the
Foundation Certificate in IT Service Management according 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 Standards Family
- IT Service Management – General Aspects
- IT Service Management – Processes
- Benefits, Risks & Challenges of Implementing IT Service Management
- Related Standards & Frameworks



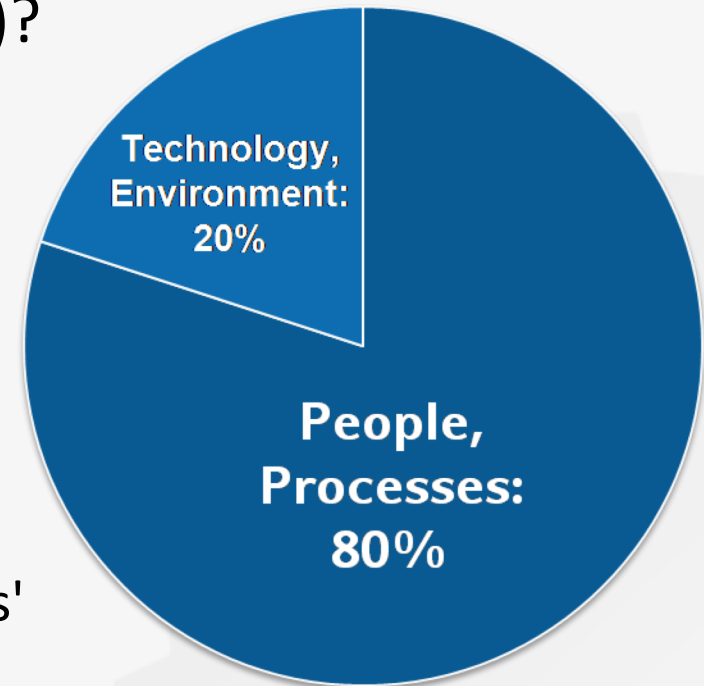
Standards for lightweight
IT service management

IT Service Management: Introduction, Terms & Concepts

Why IT service management is needed



- Why IT service management (ITSM)?
 - About 80% of all 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
[Gartner, 2001]

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 provider:

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

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

- 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.



What does the service do?

How (e.g. regarding reliability, performance etc.) does a service need to be delivered in order to help the customers achieve their goals?

What is a process?

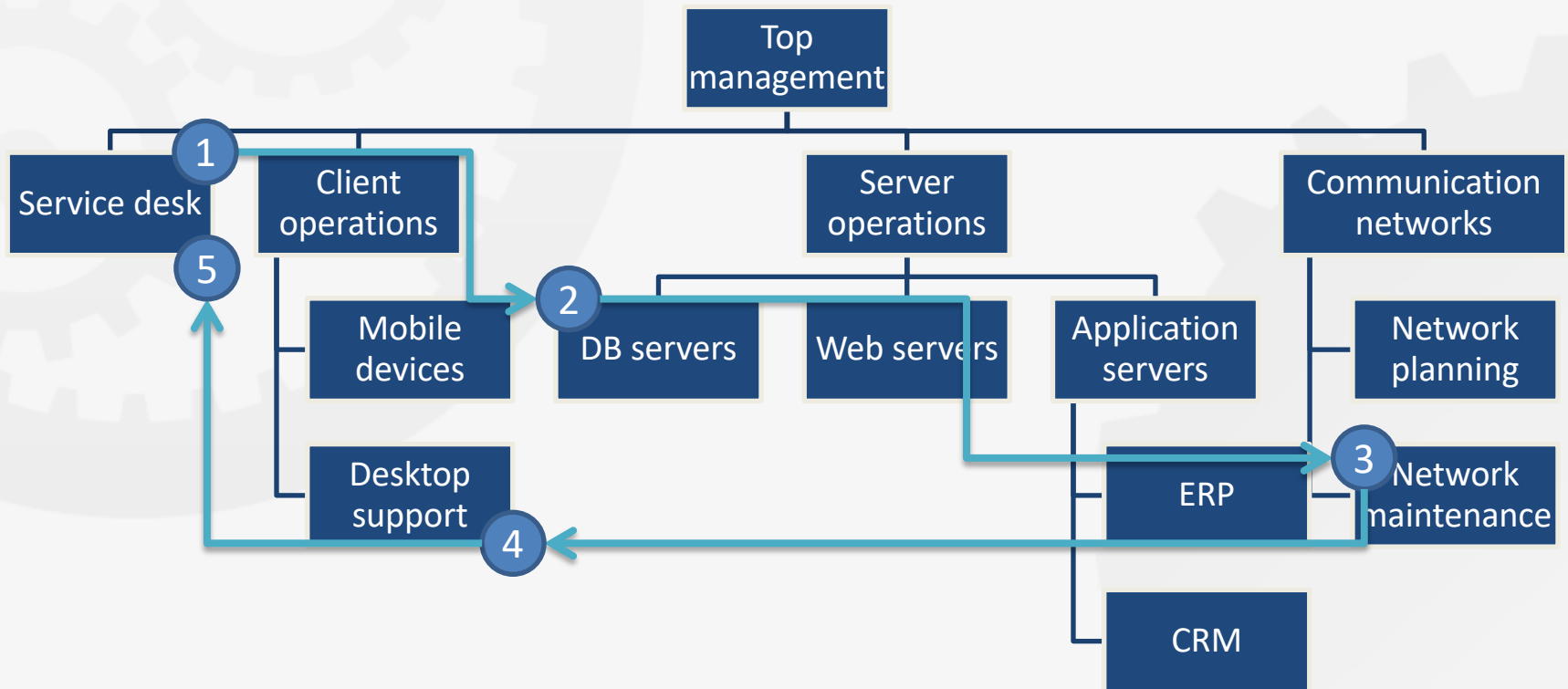
Definition following FitSM-0:

Process:

Set of *activities* that bring about a specific objective or set of results from a set of defined inputs.

- 3 basic facts about IT service management 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.

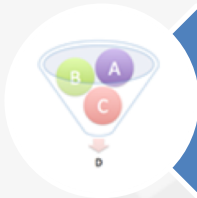
Classic line organization and processes



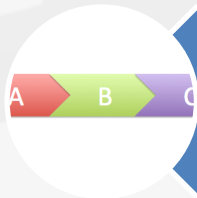
What comprises a process?



Goal(s), objectives



Clearly defined inputs, triggers and outputs



Set of interrelated activities
(across different functions)

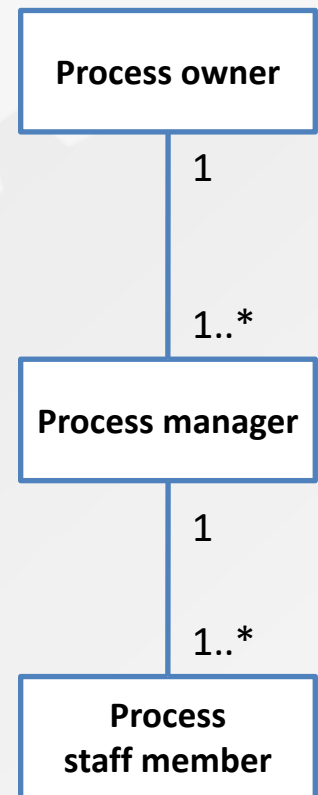


Roles and responsibilities

Process roles



- **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



Additional 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:

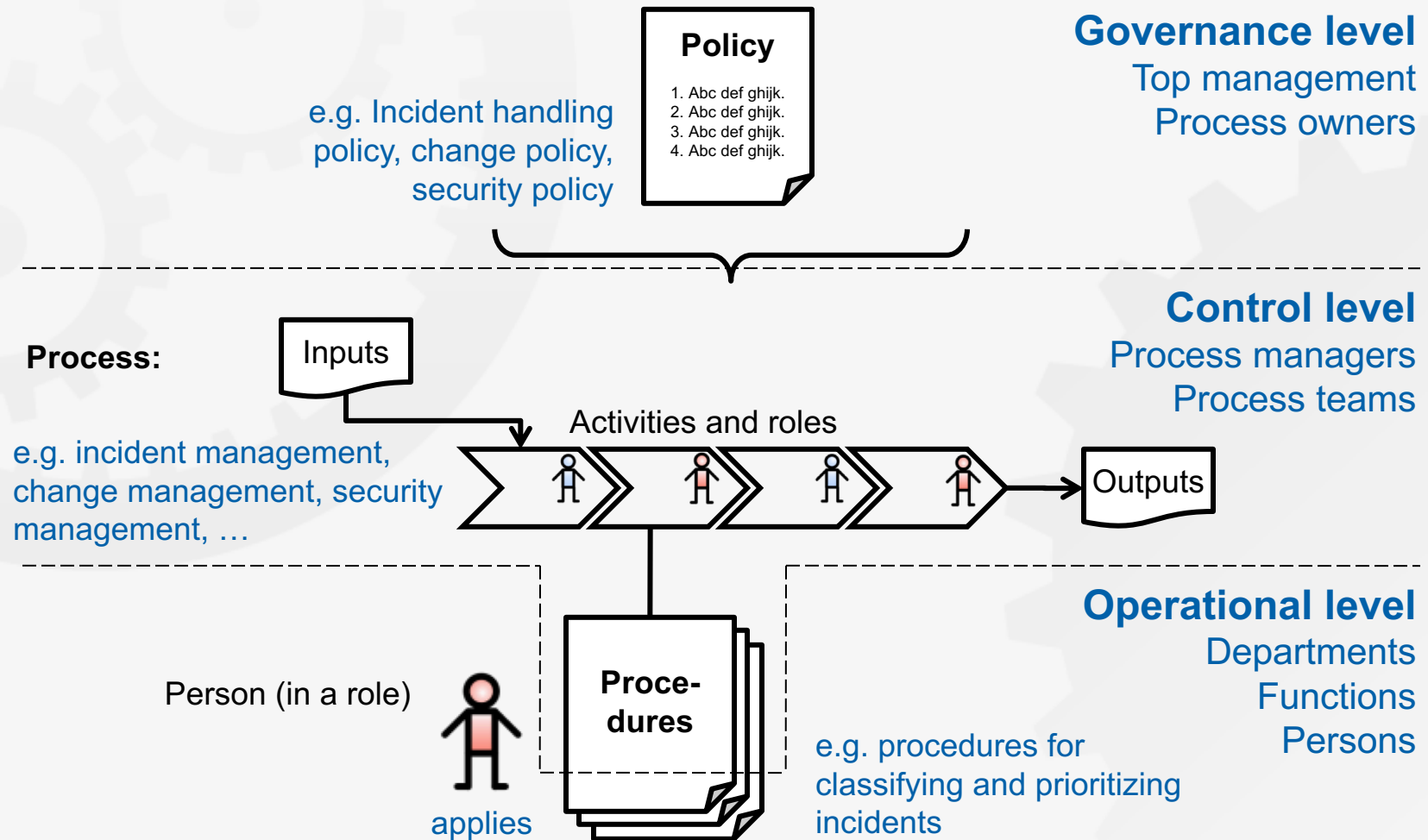
Set of actions carried out within a *process*

Definition following FitSM-0:

Procedure:

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

Service management system (SMS)





Standards for lightweight
IT service management

The FitSM 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

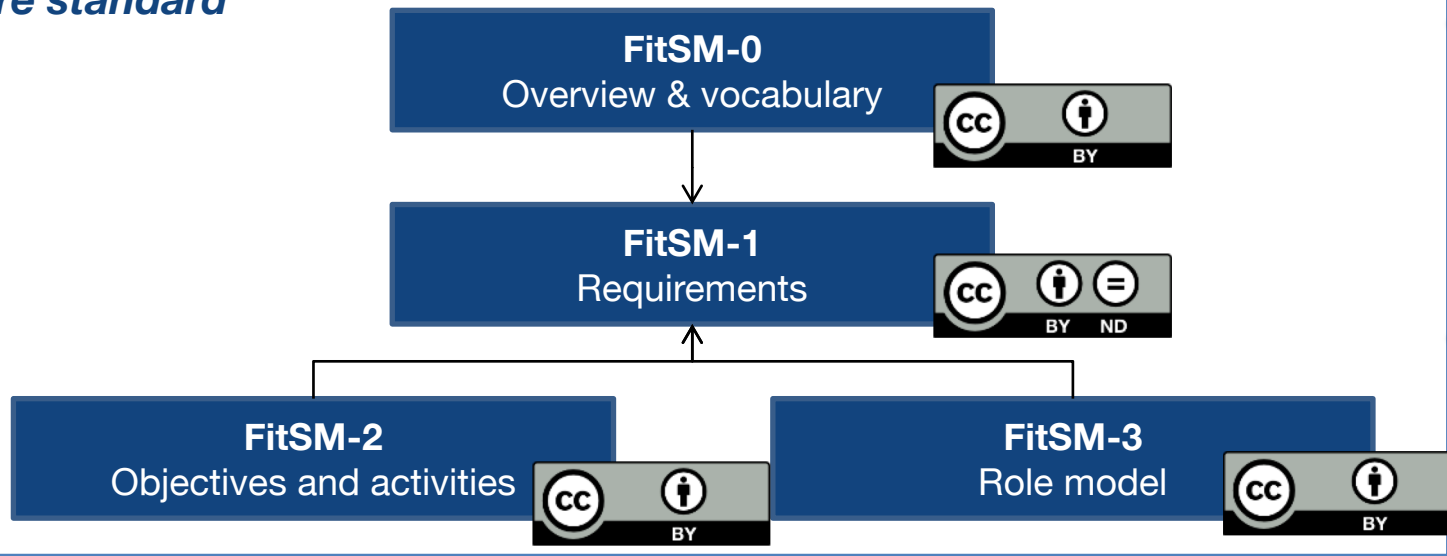


The development of the FitSM standards was supported and funded by the European Commission through the EC-FP7 project "FedSM".

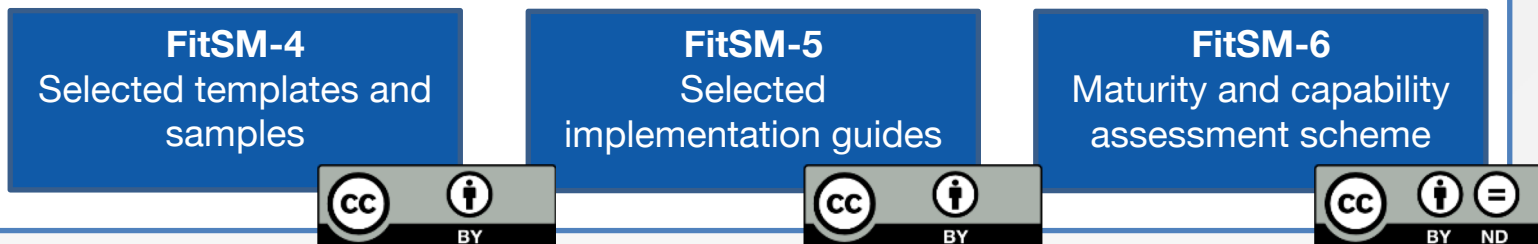
FitSM parts



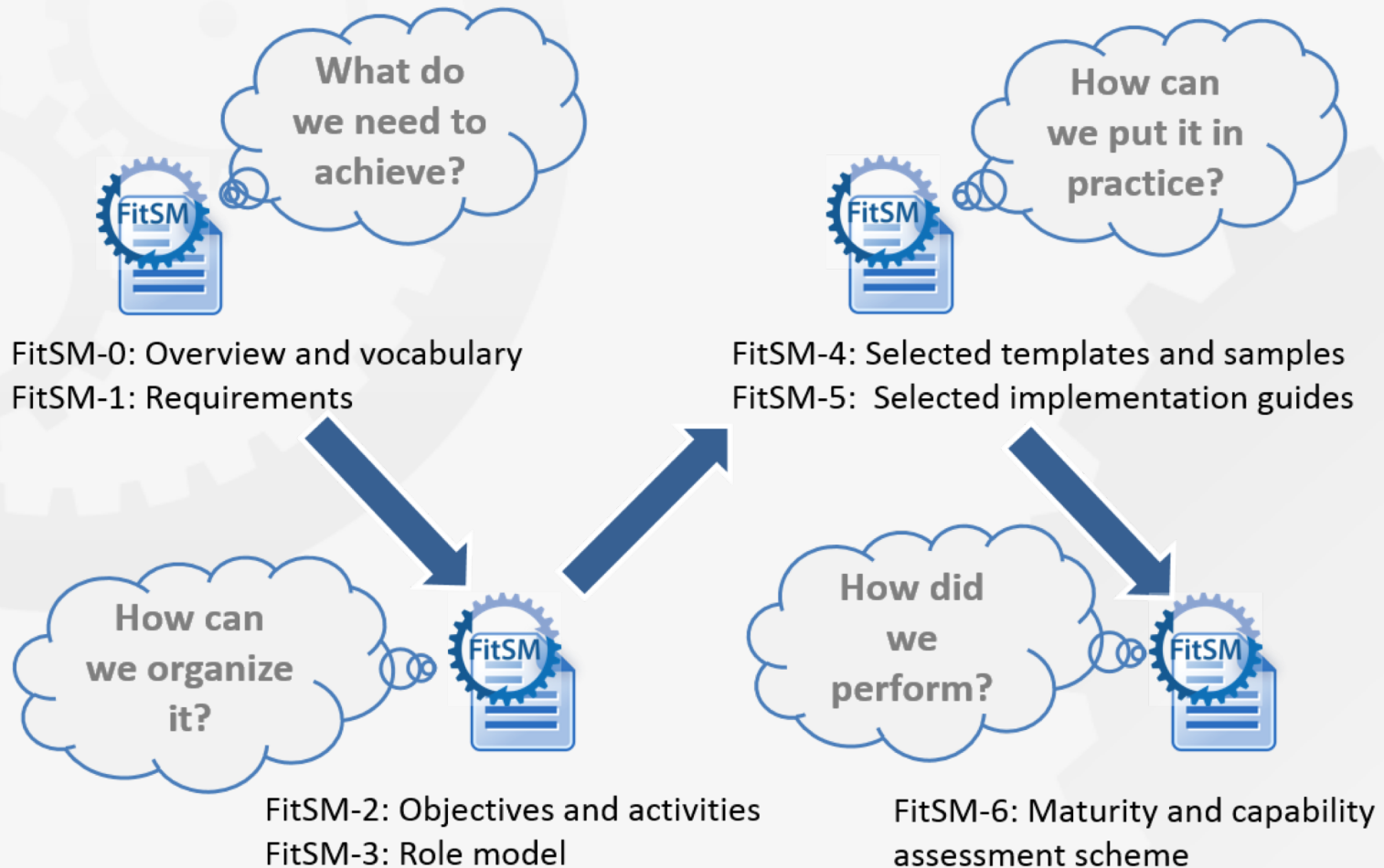
Core standard



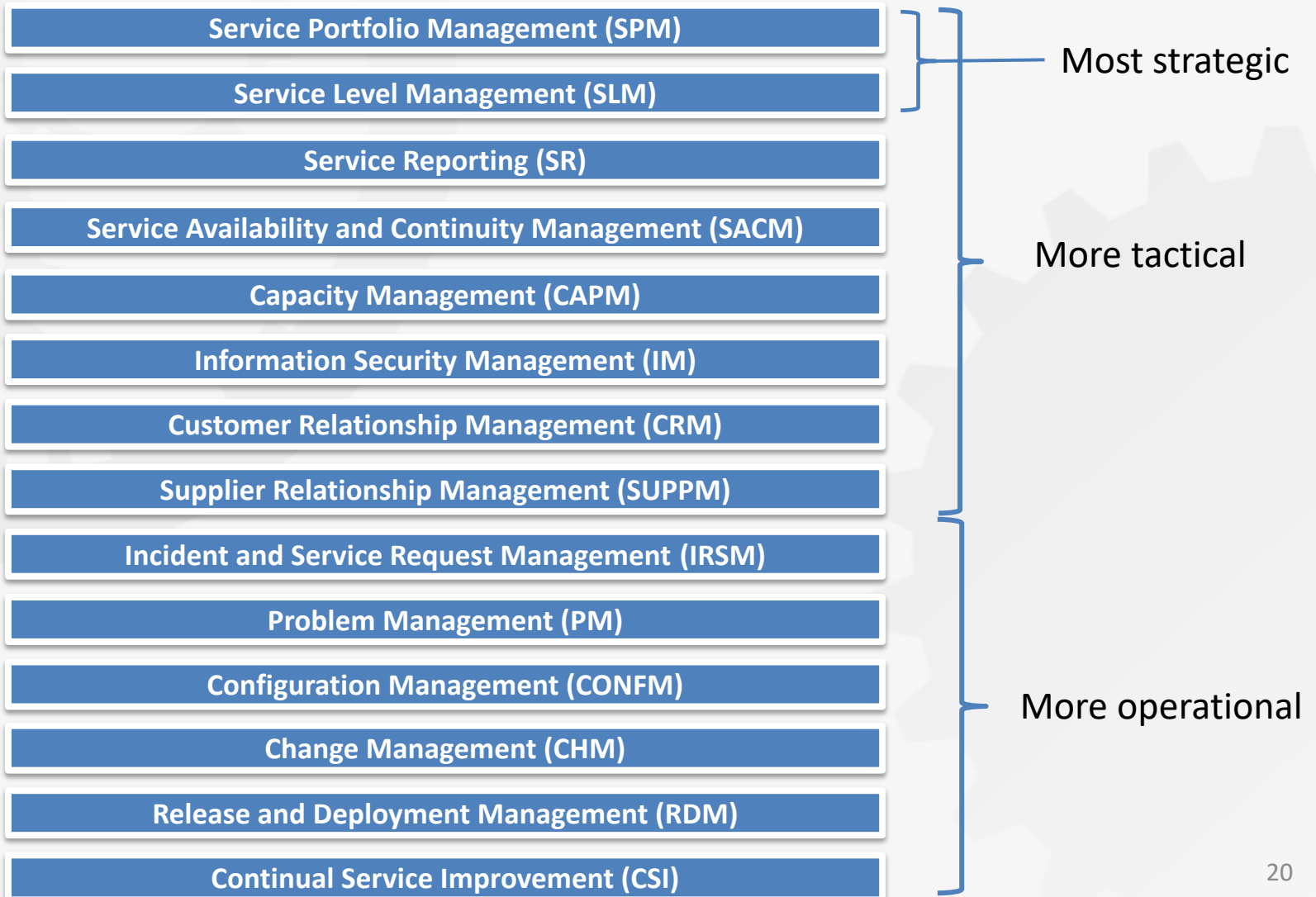
Implementation aids



FitSM logic



FitSM process model



A possible grouping of the FitSM processes



Six main topic areas:

Offer & Agree

- SPM
- SLM
- CRM

Plan & Ensure

- SUPPM
- SACM
- CAPM

Control & Deploy

- CONFM
- CHM
- RDM

Resolve & Prevent

- IM
- PM

Report & Improve

- SRM
- CSI

Protect & Secure

- ISM

FitSM-0: "Overview & vocabulary"



- FitSM-0 defines 70 important terms from the IT service management context
- In alphabetical order:

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

FitSM-1: "Requirements"



- FitSM-1 defines 85 requirements that should be fulfilled by an organisation (or federation) offering IT services to customers.
- Compliance with the 85 requirements can be regarded as a "proof of effectiveness".
- The 85 requirements are structured as follows:
 - 16 general requirements (GR)
 - 69 process-specific requirements (PR)
 - Consideration of the 14 IT service management processes from the FitSM process model
 - Between 3 and 8 requirements per process



Standards for lightweight
IT service management

IT Service Management – General Aspects

Top management responsibility: Requirements according to FitSM-1



GR1 Top Management Commitment & Responsibility

REQUIREMENTS

- GR1.1 Top management of the organisation(s) involved in the delivery of services shall show evidence that they are committed to planning, implementing, operating, monitoring, reviewing, and improving the service management system (SMS) and services. They shall:
 - Assign one individual to be accountable for the overall SMS with sufficient authority to exercise this role
 - Define and communicate goals
 - Define a general service management policy
 - Conduct management reviews at planned intervals
- GR1.2 The service management policy shall include:
 - A commitment to fulfil customer service requirements
 - A commitment to a service-oriented approach
 - A commitment to a process approach
 - A commitment to continual improvement
 - Overall service management goals

Documentation: Requirements according to FitSM-1



GR2 Documentation

REQUIREMENTS

- GR2.1 The overall SMS shall be documented to support effective planning. This documentation shall include:
 - Service management scope statement (see GR3)
 - Service management policy (see GR1)
 - Service management plan and related plans (see GR4)
- GR2.2 Documented definitions of all service management processes (see PR1-PR14) shall be created and maintained. Each of these definitions shall at least cover or reference:
 - Description of the goals of the process
 - Description of the inputs, activities and outputs of the process
 - Description of process-specific roles and responsibilities
 - Description of interfaces to other processes
 - Related process-specific policies as applicable
 - Related process- and activity-specific procedures as required

Documentation: Requirements according to FitSM-1

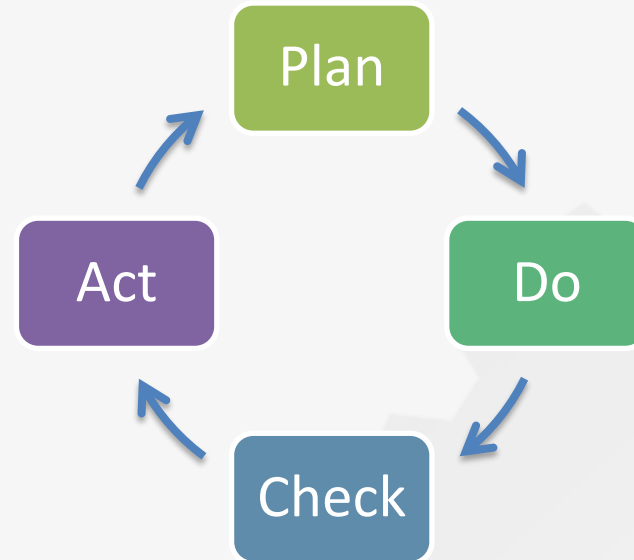
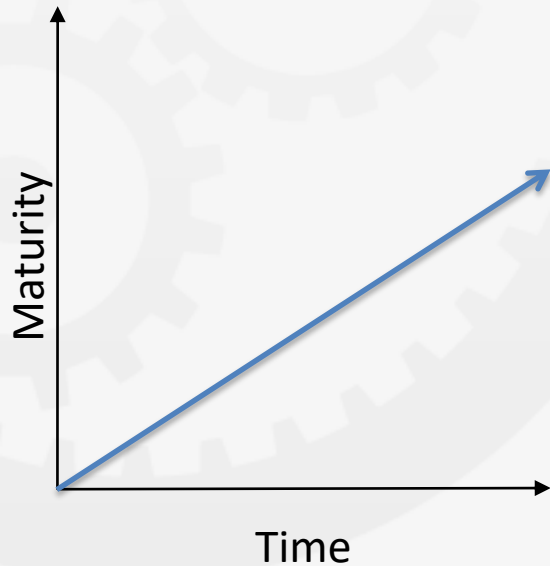


GR2 Documentation

REQUIREMENTS

- GR2.3 The outputs of all service management processes (see PR1-PR14) shall be documented, and the execution of key activities of these processes recorded.
- GR2.4 Documentation shall be controlled, addressing the following activities as applicable:
 - Creation and approval
 - Communication and distribution
 - Review
 - Versioning and change tracking

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

PDCA applied to the SMS

- Plan: GR3, GR4
 - Define the scope of the SMS
 - Set the timeline for implementing service management processes (service management plan)
- Do: GR5
 - Implement processes as planned
 - Support and enforce practical application of defined processes
- Check: GR6
 - Monitor key performance indicators (KPIs) to evaluate effectiveness and efficiency
 - Perform (internal) audits to determine the level of compliance
 - Assess the organisational maturity
- Act: GR7
 - Identify opportunities for improvements
 - Prioritize and initiate improvements



Standards for lightweight
IT service management

IT Service Management – Processes



Standards for lightweight
IT service management

Service Portfolio Management (SPM)

Objective

To define and maintain a service portfolio

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

SPM: Requirements according to FitSM-1

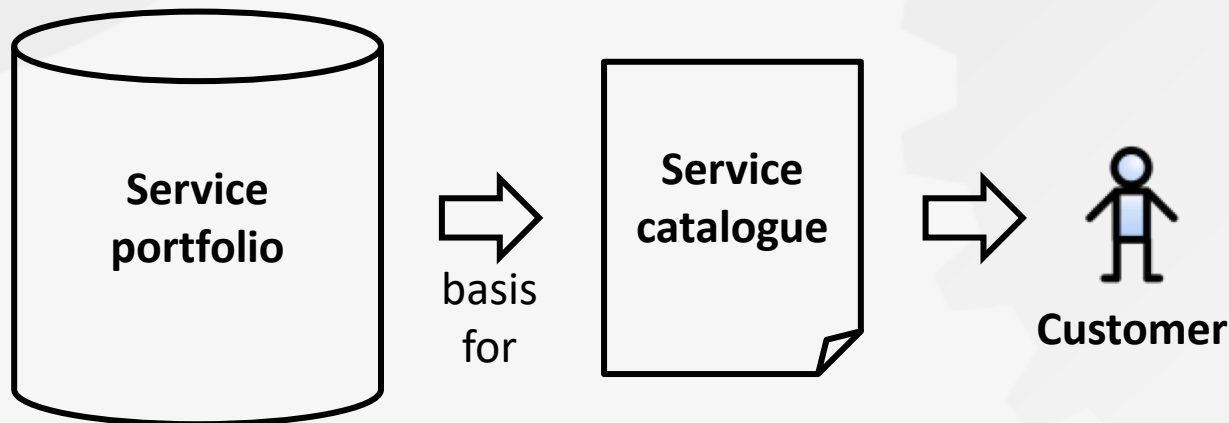


PR1 Service Portfolio Management (SPM)

REQUIREMENTS

- PR1.1 A service portfolio shall be maintained. All services shall be specified as part of the service portfolio.
- PR1.2 Design and transition of new or changed services shall be planned.
- PR1.3 Plans for the design and transition of new or changed services shall consider timescales, responsibilities, new or changed technology, communication and service acceptance criteria.
- PR1.4 The organisational structure supporting the delivery of services shall be identified, including a potential federation structure as well as contact points for all parties involved.

- 3 things to remember:
 - 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.
 - The service portfolio is the basis for the service catalogue.





Standards for lightweight
IT service management

Service Level Management (SLM)

Objective

To maintain a service catalogue, and to define, agree and monitor service levels with customers by establishing meaningful service level agreements (SLAs) and supportive operational level agreements (OLAs) and underpinning agreements (UAs) with suppliers

SLM: Important terms

Definition following FitSM-0:

Service catalogue:

User/customer facing list of all live *services* offered along with relevant information about these services

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)

Agreement between a *service provider* or *federation member* and another part of the service provider's organisation or the *federation* to provide a *service component* or subsidiary *service* needed to allow provision of *services* to *customers*

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

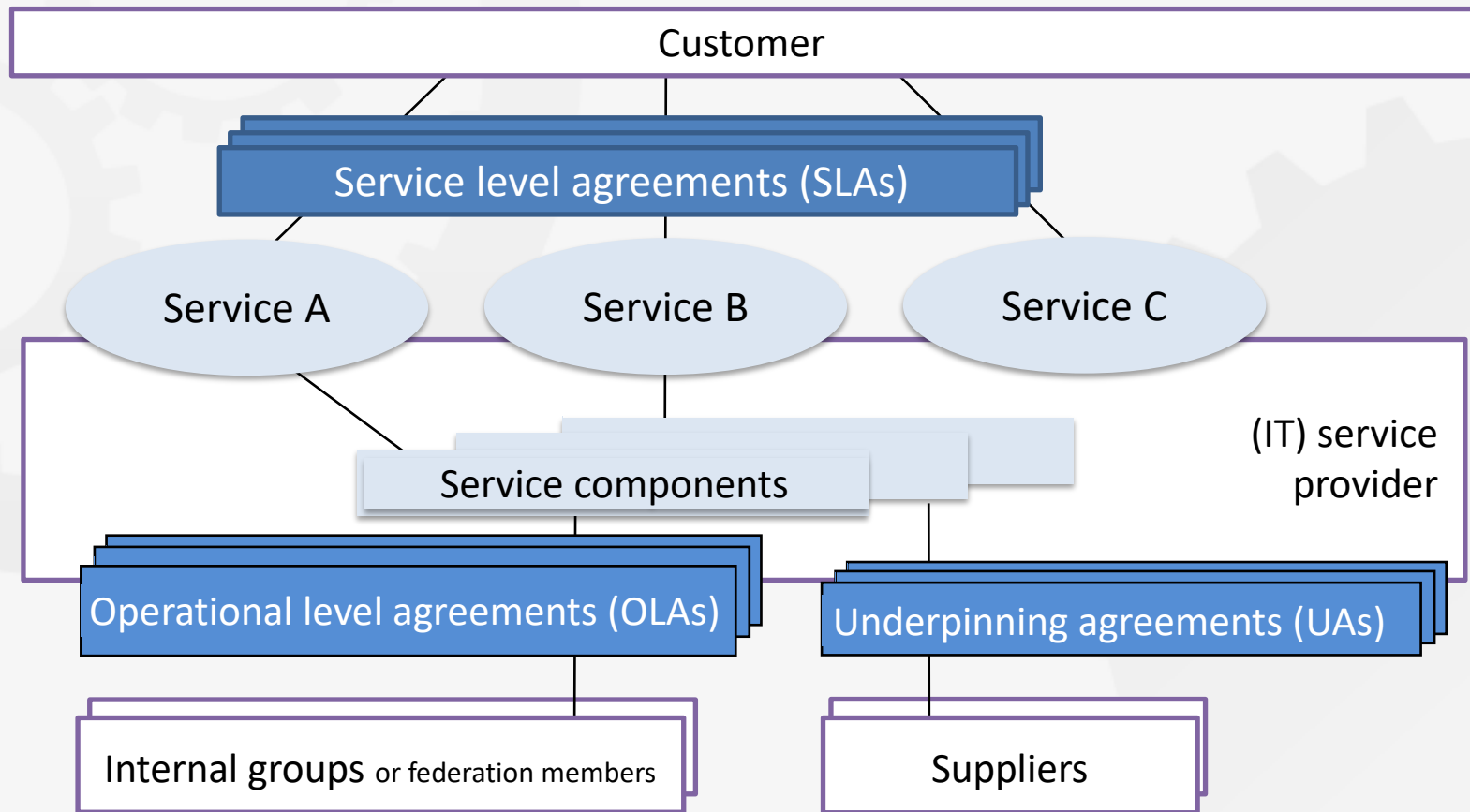
REQUIREMENTS

- PR2.1 A service catalogue shall be maintained.
- PR2.2 For all services delivered to customers, SLAs shall be in place.
- PR2.3 SLAs shall be reviewed at planned intervals.
- PR2.4 Service performance shall be evaluated against service targets defined in SLAs.
- PR2.5 For supporting services or service components provided by federation members or groups belonging to the same organisation as the service provider or external suppliers, OLAs and UAs shall be agreed.
- PR2.6 OLAs and UAs shall be reviewed at planned intervals.
- PR2.7 Performance of service components shall be evaluated against operational targets defined in OLAs and UAs.

SLM: Defining SLAs

- SLAs are agreed between a service provider and its customers
- Typical contents in an SLA (included or referenced):
 - Scope and description of the service
 - Service hours and exceptions
 - Service components & dependencies
 - Support
 - Incident handling
 - Fulfilment of service requests
 - Service level targets
 - Limitations & constraints
 - Communication, reporting & escalation
 - General communication
 - Regular reporting
 - SLA violations
 - Escalation & complaints
 - Information security & data protection
 - Additional responsibilities of the service provider
 - Customer responsibilities
 - Review
 - Glossary of terms

SLM: Types of service agreements and their relationships





- 3 things to remember:
 - 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.



Standards for lightweight
IT service management

Service Reporting Management (SRM)

Objective

To specify all service reports and ensure they are produced according to specifications in a timely manner to support decision-making

SRM: Requirements according to FitSM-1



PR3 Service Reporting

REQUIREMENTS

- PR3.1 Service reports shall be specified and agreed with their recipients.
- PR3.2 The specification of each service report shall include its identity, purpose, audience, frequency, content, format and method of delivery.
- PR3.3 Service reports shall be produced. Service reporting shall include performance against agreed targets, information about significant events and detected nonconformities.



- 3 things to remember:
 - Service reports are important to support decision-making.
 - Service reports can be useful to demonstrate the level of service quality that has been achieved.
 - Agree the reports and their purpose, audience, frequency, content, format and method of delivery with the report stakeholders.



Standards for lightweight
IT service management

Service Availability & Continuity Management (SACM)

Objective

To ensure sufficient service availability to meet agreed requirements and adequate service continuity in case of exceptional situations

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

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

SACM: Requirements according to FitSM-1




PR4 Service Continuity & Availability Management

REQUIREMENTS

- PR4.1 Service availability and continuity requirements shall be identified taking into consideration SLAs.
- PR4.2 Service availability and continuity plans shall be created and maintained.
- PR4.3 Service availability and continuity planning shall consider measures to reduce the probability and impact of identified availability and continuity risks.
- PR4.4 Availability of services and service components shall be monitored.

- Most important output from this process:



Service
availability and
continuity
plan(s)

- 3 things to remember:
 - **Identify** service availability and continuity **requirements** (e.g. from SLAs).
 - **Plan** to reduce the probability and impact of identified availability and continuity risks and produce plans.
 - **Monitor service availability.**



Standards for lightweight
IT service management

Capacity Management (CAPM)

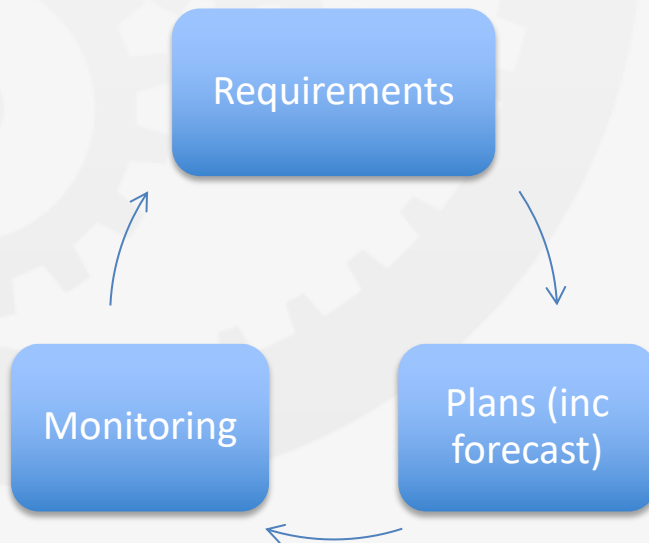
Objective

To ensure sufficient capacities are provided to meet agreed service capacity and performance requirements

CAPM vs SACM

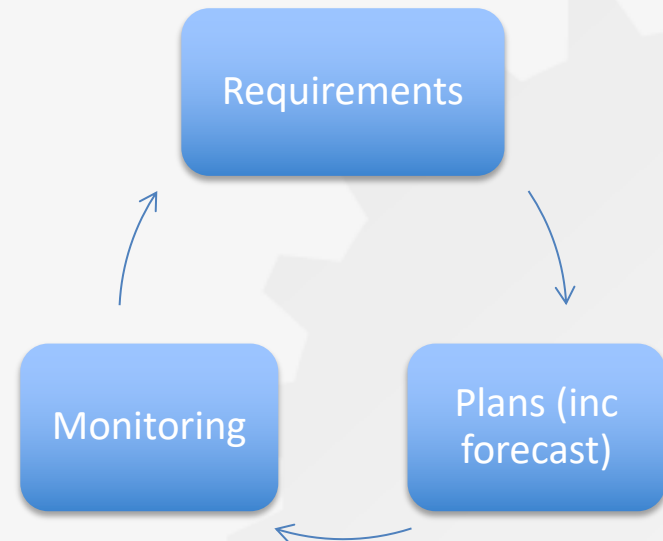


Capacity



Sufficient capacity → Sufficient resources (technical, human, financial...)

Availability and continuity



More availability → more redundancy

CAPM: Requirements according to FitSM-1

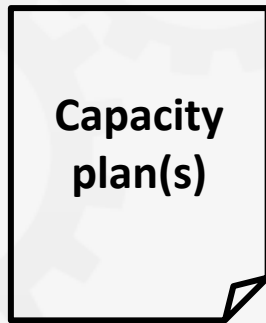


PR5 Capacity Management

REQUIREMENTS

- PR5.1 Service capacity and performance requirements shall be identified taking into consideration SLAs.
- PR5.2 Capacity plans shall be created and maintained.
- PR5.3 Capacity planning shall consider human, technical and financial resources.
- PR5.4 Performance of services and service components shall be monitored based on monitoring the degree of capacity utilisation and identifying operational warnings and exceptions.

- Most important output from this process:



Typical contents:

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

- 3 things to remember:
 - Identify service performance requirements (e.g. from SLAs).
 - Plan the resources required to fulfil the requirements and produce a capacity plan.
 - Monitor service performance.



Standards for lightweight
IT service management

Information Security Management (ISM)

Objective

To manage information security effectively through all activities performed to deliver and manage services, so that the confidentiality, integrity and accessibility of relevant assets are preserved

ISM: What is information security?

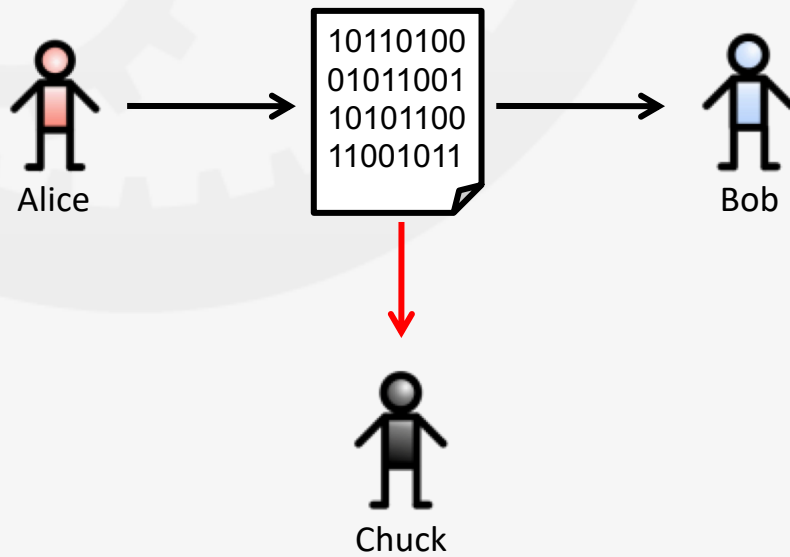
- Information security aspects:

- **Confidentiality**
- **Integrity**
- **Accessibility** of information

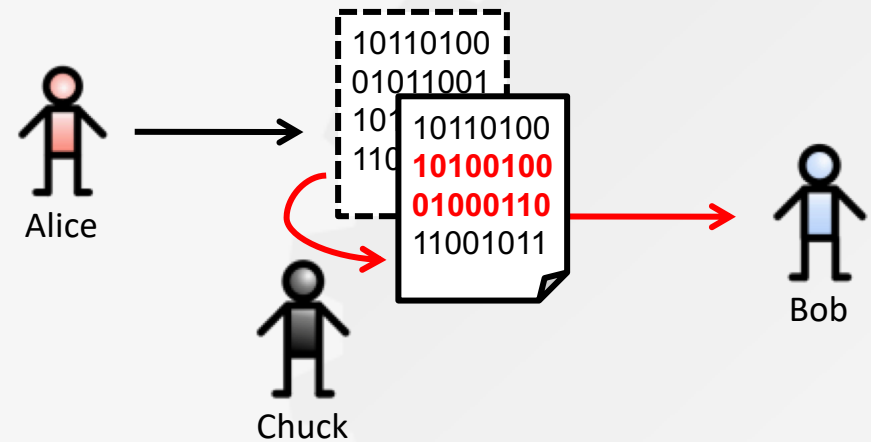
Key aspects

ISM: Confidentiality and integrity

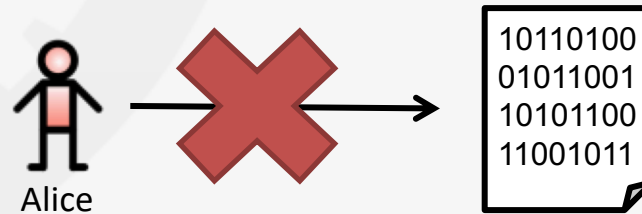
Confidentiality: To protect information from unauthorized disclosure



Integrity: To protect information from modifications, additions, deletions, rearrangement, duplication or re-recording



Accessibility: Information is available and usable when required, and the system that provide it can appropriately resist attacks and recover or prevent failures



ISM: Requirements according to FitSM-1



PR6 Information Security Management

REQUIREMENTS

- PR6.1 Information security policies shall be defined.
- PR6.2 Physical, technical and organizational information security controls shall be implemented to reduce the probability and impact of identified information security risks.
- PR6.3 Information security policies and controls shall be reviewed at planned intervals.
- PR6.4 Information security events and incidents shall be given an appropriate priority and managed accordingly.
- PR6.5 Access control, including provisioning of access rights, for information-processing systems and services 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
 - E-mail policy
 - Mobile device policy
 - Access control policy
 - Media disposal policy
 - ...
 - Information security risk assessment
 - Documented information security controls



- 3 things to remember:
 - Preserve confidentiality, integrity and accessibility of information assets.
 - Identify and treat information security risks.
 - Produce and enforce information security policies.



Standards for lightweight
IT service management

Customer Relationship Management (CRM)

Objective

To establish and maintain a good relationship with customers receiving services

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 customer relationship and customer satisfaction.
- PR7.3 Communication mechanisms with customers shall be established.
- PR7.4 Service reviews with the customers shall be conducted at planned intervals.
- PR7.5 Service complaints from customers shall be managed.
- PR7.6 Customer satisfaction shall be managed.



Standards for lightweight
IT service management

Supplier Relationship Management (SUPPM)

Objective

To establish and maintain a healthy relationship with suppliers supporting the service provider in delivering services to customers

SUPPM: Requirements according to FitSM-1



PR8 Supplier Relationship Management

REQUIREMENTS

- PR8.1 Suppliers shall be identified.
- PR8.2 For each supplier, there shall be a designated contact responsible for managing the relationship with the supplier.
- PR8.3 Communication mechanisms with suppliers shall be established.
- PR8.4 Supplier performance shall be monitored.



Standards for lightweight
IT service management

Incident & Service Request Management (ISRM)

Objective

To restore normal / agreed service operation within the agreed time 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:

Request for information, advice, access to a *service* or a pre-approved *change*

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

ISRM: Requirements according to FitSM-1

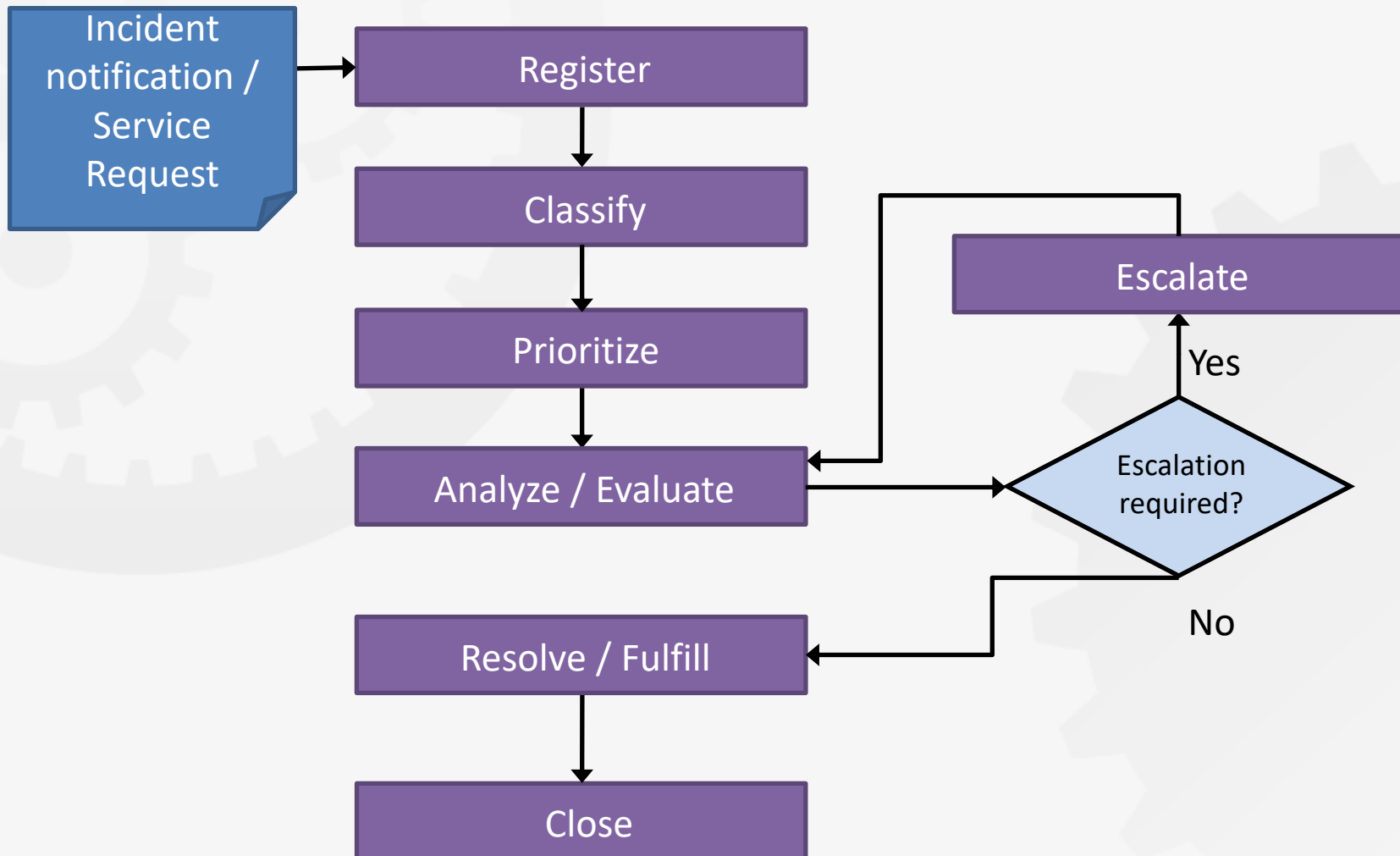


PR9 Incident & Service Request Management

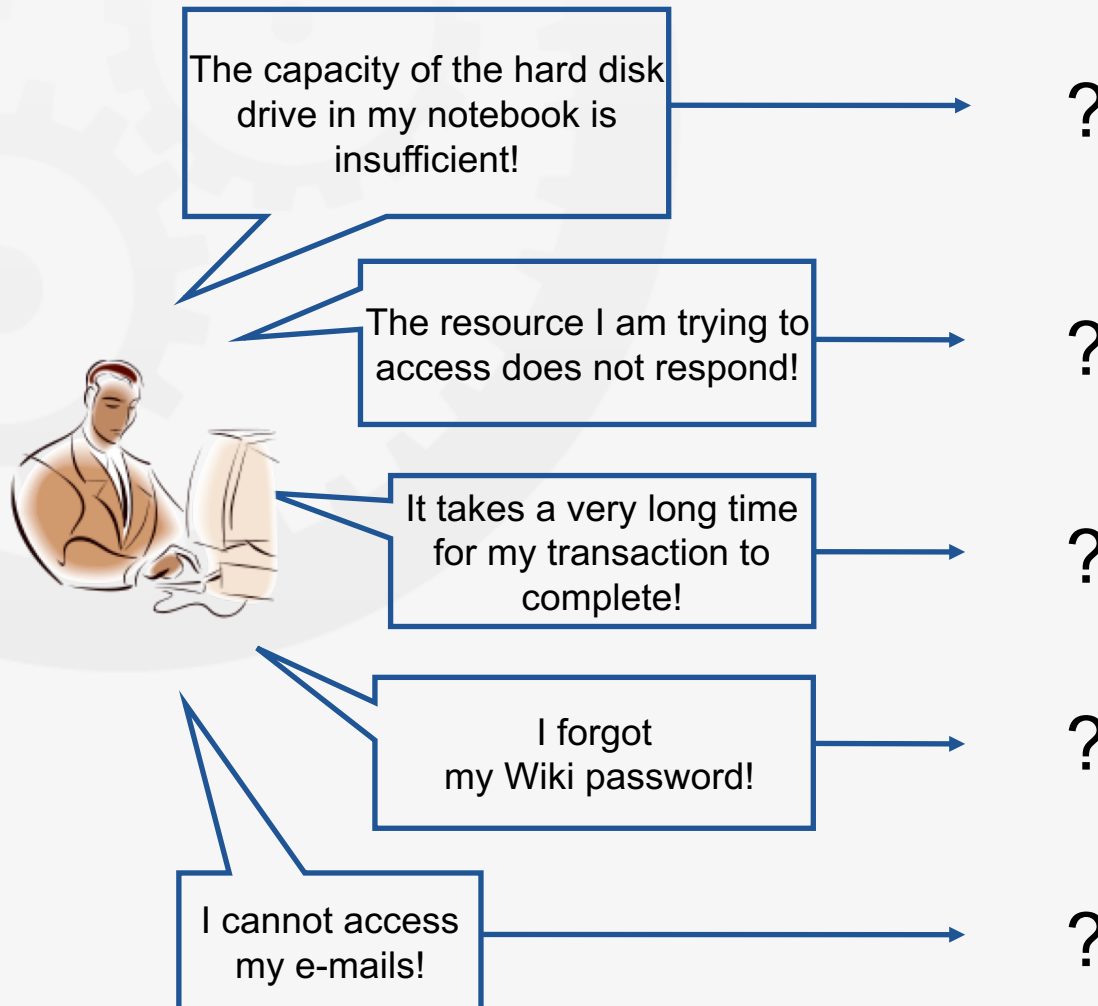
REQUIREMENTS

- PR9.1 All incidents and service requests shall be registered, classified and prioritized in a consistent manner.
- PR9.2 Prioritization of incidents and service requests shall take into account service targets from SLAs.
- PR9.3 Escalation of incidents and service requests shall be carried out in a consistent manner.
- PR9.4 Closure of incidents and service requests shall be carried out in a consistent manner.
- PR9.5 Personnel involved in the incident and service request management process shall have access to relevant information including known errors, workarounds, configuration and release information.
- PR9.6 Users shall be kept informed of the progress of incidents and service requests they have reported.
- PR9.7 There shall be a definition of major incidents and a consistent approach to managing them.

ISRM: Workflow (example)



ISRM: Service request or incident?





Standards for lightweight
IT service management

Problem Management (PM)

Objective

To investigate the root causes of (recurring) incidents in order to avoid future recurrence of incidents by resolving the underlying causes, or to ensure workarounds / temporary fixes are available.

PM: Important terms

Definition following FitSM-0:

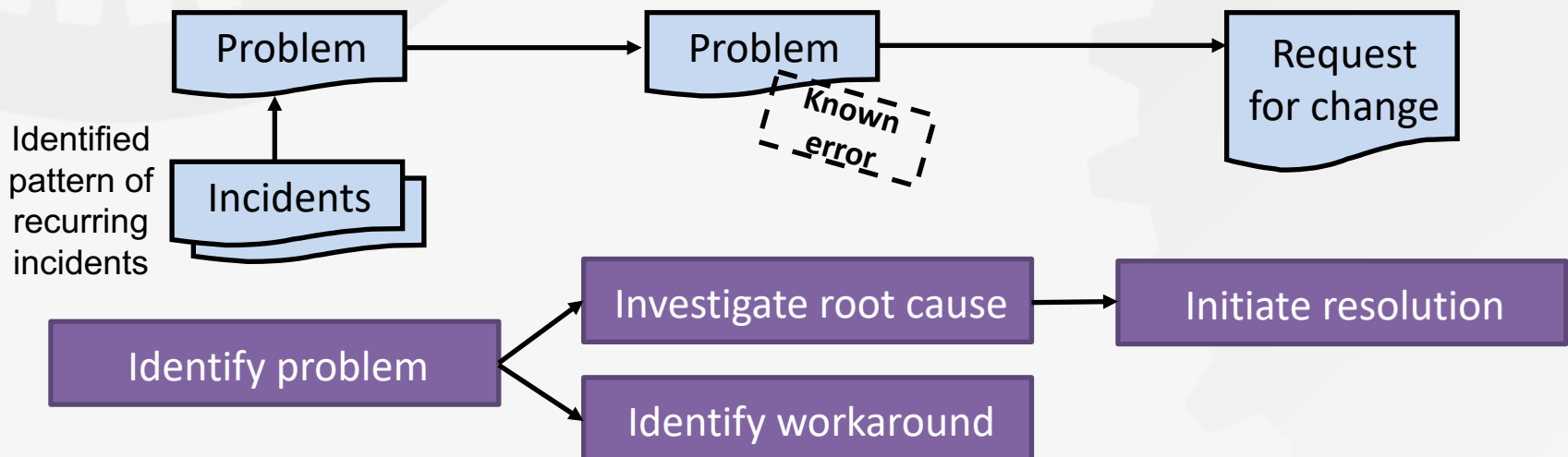
Problem:

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

Definition following FitSM-0:

Known error:

Problem which has not (yet) been corrected, but for which there is a documented workaround or temporary fix to prevent (excessive) negative impact on *services*



PM: Requirements according to FitSM-1



PR10 Problem Management

REQUIREMENTS

- PR10.1 Problems shall be identified and registered based on analysing trends on incidents.
- PR10.2 Problems shall be investigated to identify actions to resolve them or reduce their impact on the 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: Example – From incidents to problems to resolutions



Incident 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 & Workaround

Problem

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

Workaround

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

Problem Management: Resolution

Known error

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

Resolution

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



Standards for lightweight
IT service management

Configuration Management (CONFM)

Objective

To provide and maintain a logical model of all configuration items and their relationships and dependencies



CONFM: Important terms

Definition following FitSM-0:

Configuration item (CI):

Element that contributes to the delivery of one or more *services* or *service components*, and therefore needs to be controlled

Definition following FitSM-0:

Configuration baseline:

The state of a specified set of *configuration items (CIs)* at a given point in time

Definition following FitSM-0:

Configuration management database (CMDB):

Store for data about *configuration items* (therefore configuration data)

Note: The CMDB likely includes attributes of CIs as well as information on relationships between CIs, service components and services.

CONFM: Requirements according to FitSM-1



PR11 Configuration Management

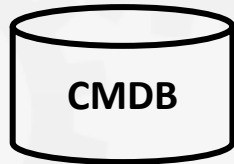
REQUIREMENTS

- PR11.1 Configuration item (CI) types and relationship types shall be defined.
- PR11.2 The level of detail of configuration information recorded shall be sufficient to support effective control over CIs.
- PR11.3 Each CI and its relationships with other CIs shall be recorded 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.
- PR11.6 Before a new release into a live environment, a configuration baseline of the affected CIs shall be taken.

CONFM: Output and summary



- Most important output from this process:



Logical CMDB:

- Information on CIs and their attributes
- Information on the relationships between CIs
- Links to other information systems (physical CMDBs)

- 3 things to remember:
 - Configuration Management is not about configuring resources
 - Configuration Management is about understanding (and documenting) the current configuration
 - Current configuration = All relevant CIs and their attributes and relationships



Standards for lightweight
IT service management

Change Management (CHM)

Objective

To ensure changes to configuration items are planned, approved, implemented and reviewed in a controlled manner to avoid adverse impact of changes to services or the customers receiving services



CHM: Important terms

Definition following FitSM-0:

Request for change (RFC):

Documented proposal for a *change* to be made to one or more *configuration items (CIs)*

Definition following FitSM-0:

Change:

Alteration (such as addition, removal, modification, replacement) of a *configuration item (CI)* that contributes to providing one or more *services*

CHM: Requirements according to FitSM-1

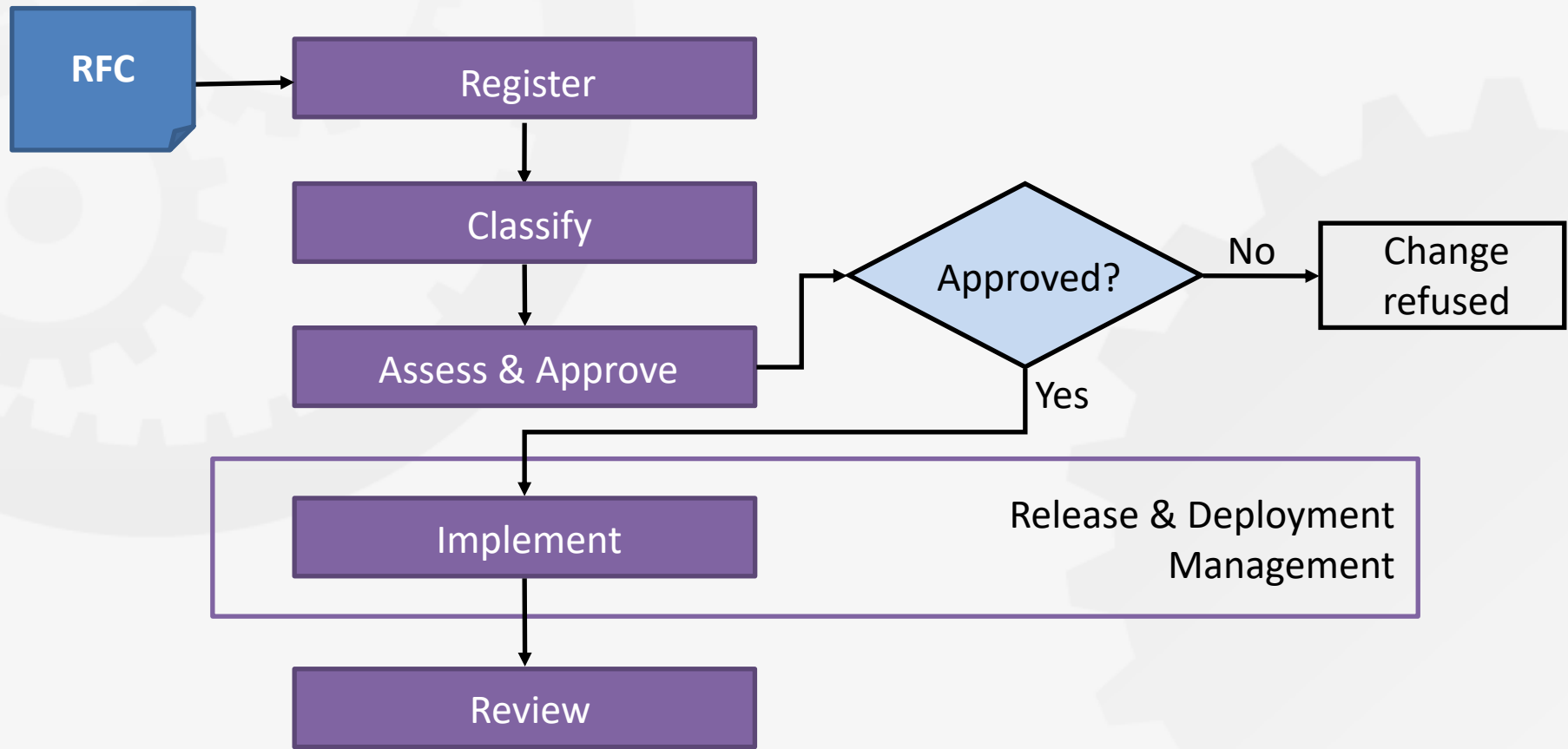


PR12 Change Management

REQUIREMENTS

- PR12.1 All changes shall be registered and classified in a consistent manner.
- PR12.2 All changes shall be assessed and approved in a consistent manner.
- PR12.3 All changes shall be subject to a post implementation review and closed in a consistent manner.
- PR12.4 There shall be a definition of emergency changes and a consistent approach to managing them.
- PR12.5 In making decisions on the acceptance of requests for change, the benefits, risks, potential impact to services and customers and technical feasibility shall be taken into consideration.
- PR12.6 A schedule of changes shall be maintained. It shall contain details of approved changes, and proposed deployment dates, which shall be communicated to interested parties.
- PR12.7 For changes of high impact or high risk, the steps required to reverse an unsuccessful change or remedy any negative effects shall be planned and tested.

CHM: Workflow (example)





- 3 things to remember:
 - All changes to CIs should be controlled by the change management process.
 - Typical categories of changes:
 - Standard change (pre- or self-approved)
 - Non-standard change
 - Emergency change
 - A change advisory board (CAB) may be established. During CAB meetings, requests for non-standard changes are evaluated and discussed.



Standards for lightweight
IT service management

Release & Deployment Management (RDM)

Objective

To bundle changes of one or more configuration items to releases, so that these changes can be tested and deployed to the live environment together



RDM: Important terms

Definition following FitSM-0:

Release:

Set of one or more *changes to configuration items (CIs)* that are grouped together and deployed as a logical unit

RDM: Requirements according to FitSM-1

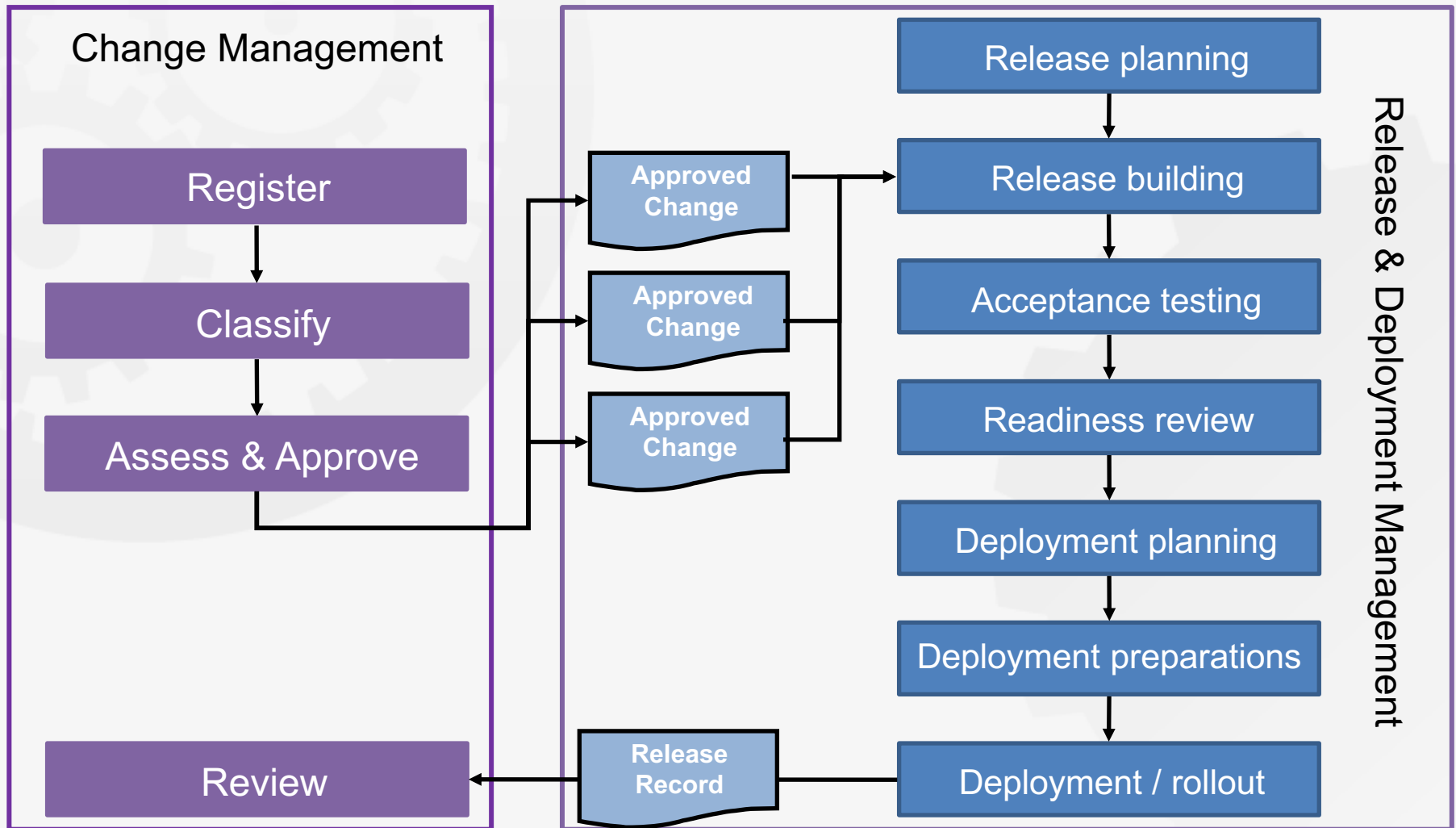


PR13 Release & Deployment Management

REQUIREMENTS

- PR13.1 A release policy shall be defined.
- PR13.2 The deployment of new or changed services and service components to the live environment shall be planned with all relevant parties including affected customers.
- PR13.3 Releases shall be built and tested prior to being deployed.
- PR13.4 Acceptance criteria for each release shall be agreed with the customers and any other relevant parties. Before deployment the release shall be verified against the agreed acceptance criteria and approved.
- PR13.5 Deployment preparation shall consider steps to be taken in case of unsuccessful deployment to reduce the impact on services and customers.
- PR13.6 Releases shall be evaluated for success or failure.

RDM: Workflow





Standards for lightweight
IT service management

Continual Service Improvement Management (CSI)

Objective

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

CSI: Requirements according to FitSM-1



PR14 Continual Service Improvement Management

REQUIREMENTS

- PR14.1 Opportunities for improvement shall be identified and registered.
- PR14.2 Opportunities for improvement shall be evaluated and approved in a consistent manner.



Standards for lightweight
IT service management

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

Challenges in federated IT service provisioning



- Traditional IT service management (ITSM) practices ...
 - assume single central control over all service management processes by one organisation acting as the service provider;
 - hardly address collaborative approaches to service delivery.
- As a result: Applying ITSM in federated environments may be more difficult, and not all concepts / ideas will apply.
- Important in a federated environment: Understanding the needs of different types of federations with respect to (federation-wide) ITSM

Examples of types of federation

ITSM perspective

In looser federations:

Individual federation members are responsible for delivering services to their customers largely on their own. Integration and coordination falls upon individual federation members or customers themselves.

→ Few, if any, federation-wide ITSM processes



In more tightly integrated federations:

Service delivery to customers requires joint effort from multiple federation members

→ Many, if not all, ITSM processes are federation-wide

Invisible
coordination

Hotel industry
association

...

Hotel guide,
rating portal

Matchmaking

Travel agent,
booking portal

...

Airline with
code sharing

Full service
integration

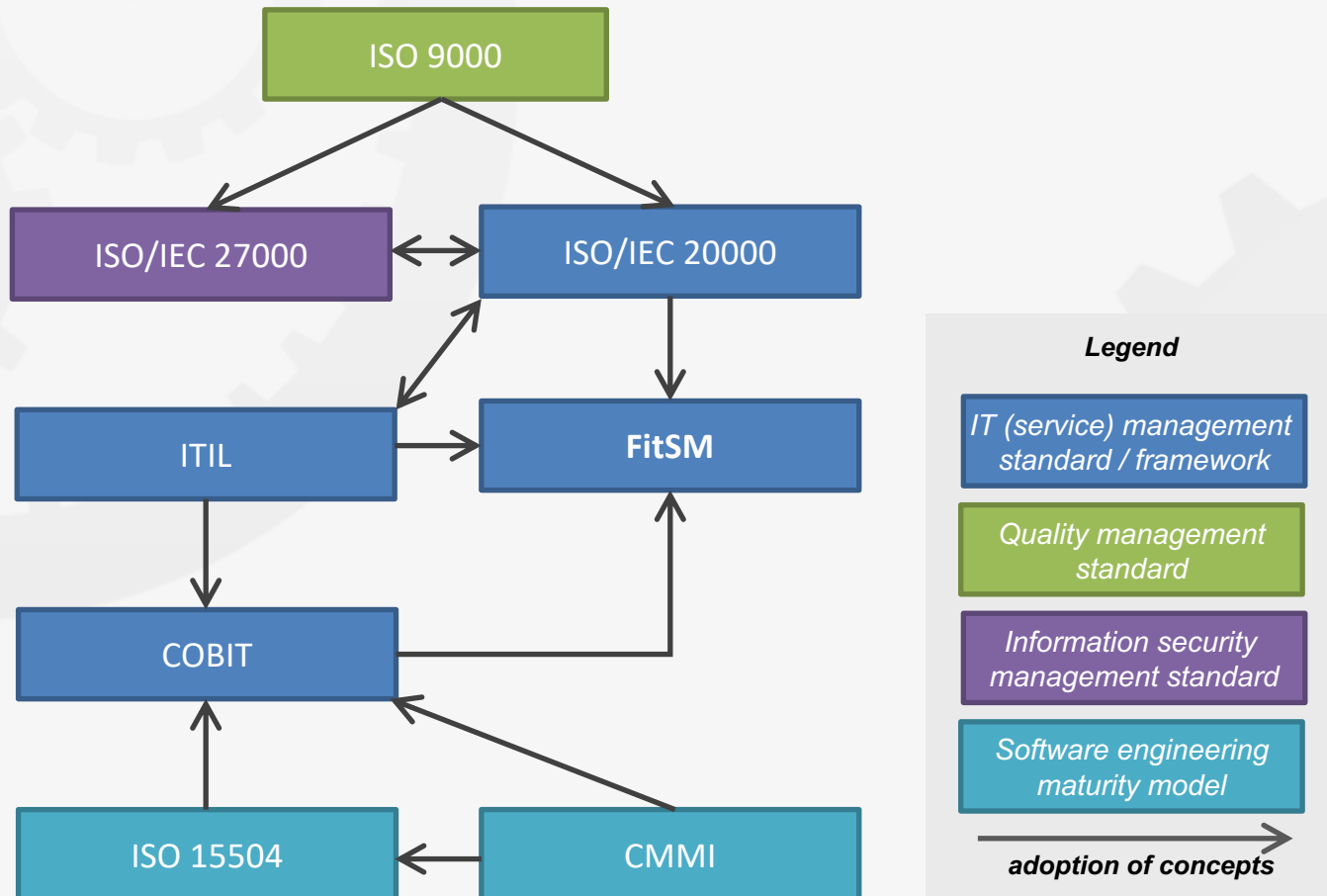
Virtual mobile
phone operator



Standards for lightweight
IT service management

Related Standards & Frameworks

Related standards and frameworks



ITIL, ISO/IEC 20000, COBIT



ITIL

IT Infrastructure Library (ITIL®)

- Number of books with "good practice" in IT Service Management
- Slogan: "the key to managing IT services"
- Descriptions of key principles, concepts and processes in ITSM

- Popular and wide-spread framework
- Not a "real" standard, but often regarded to as "de-facto standard"
- 5 books released by the British Cabinet Office

ISO/IEC 20000

ISO/IEC 20000

- International standard for managing and delivering IT services
- Requirements for a service management system (SMS)

- Developed by a joint committee (JTC) of ISO and IEC
- Based on ITIL, BS 15000
- Auditable, certifiable

COBIT

Control Objectives for Information and Related Technologies (COBIT)

- Framework for governance and management of enterprise IT

- Developed by ISACA
- can be combined with ITIL and ISO/IEC 20000

ISO 9000, ISO/IEC 27000, CMMI



ISO 9000

ISO 9000

- International standard for quality management
- Quality management principles
- Requirements for a quality management system

- Applicable to all organizations and branches
- Auditable, certifiable
- Several documents

ISO/IEC 27000

ISO/IEC 27000

- International standard for information security management
- Requirements for an information security management system (ISMS)
- More than 100 security controls

- Applicable to all organizations and branches
- Auditable, certifiable
- Based on BS 7799
- Auditable, certifiable
- Several documents

CMMI

Capability Maturity Model Integration

- Maturity and capability model
- Organizational maturity assessment

- Developed by SEI (Software Engineering Institute), Carnegie Mellon University