Standards for lightweight IT service management

Service Operation & Control

Advanced training in service operation and control according to FitSM

Version 2.5

Purpose of this training

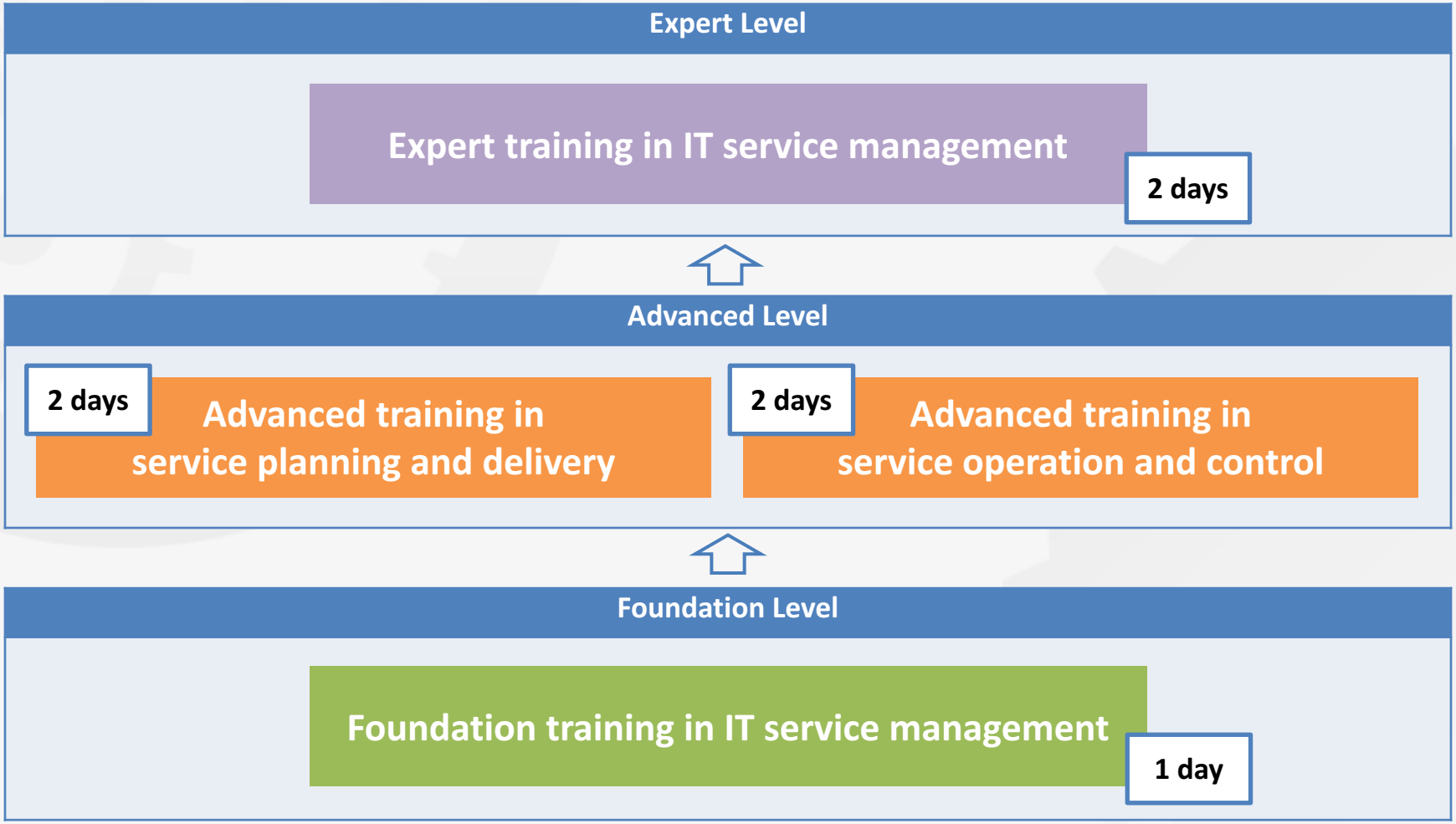
- Repeat the most important foundation knowledge on (lightweight) IT Service Management (ITSM)
- Become familiar with …
  - the general aspects of implementing ITSM;
  - the processes required to operate and control services effectively, according to the FitSM-1 standard;
  - important interfaces in a service management system.
- Achieve the
  Advanced level certificate in service operation and control according to FitSM
  issued by TÜV SÜD Examination Institute

Examination Institute

FitSM Advanced Level exam

- At the end of this training
- Closed book, i.e. no aids are allowed
- Duration: 60 minutes
- 30 multiple choice questions:
  - Four possible answers for each question: A, B, C or D
  - One correct answer per question
- At least 70% correct answers (21 of 30) are required to pass the examination

FitSM qualification program



Agenda of this training

- FitSM Foundation wrap-up & ITSM basics
- Selected general aspects of establishing a service management system (SMS)
- ITSM processes for the operation and control of services
- ITSM process interfaces and dependencies

Standards for lightweight
IT service management

FitSM Foundation Wrap-Up & ITSM Basics

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:

IT service:

A *service* that is enabled by the use of information technology (IT)

What is the **key purpose** of the service?

Which additional factors will impact the customers' service **quality / performance perception**?

IT service management

Definition following FitSM-0:

IT service management (ITSM):

The entirety of *activities* performed by an IT *service provider* to plan, deliver, operate and control *IT services* offered to *customers*

Note: The activities carried out in the ITSM context should be directed by policies and structured and organised by processes and supporting procedures.

Definition following FitSM-0:

Management system:

Entirety of *policies*, *processes*, *procedures* and related resources and capabilities aiming at effectively performing management tasks in a given context and for a given subject

Note: A management system is generally intangible. It is based on the idea of a systematic, structured and process-oriented way of managing.

Service management system (SMS)

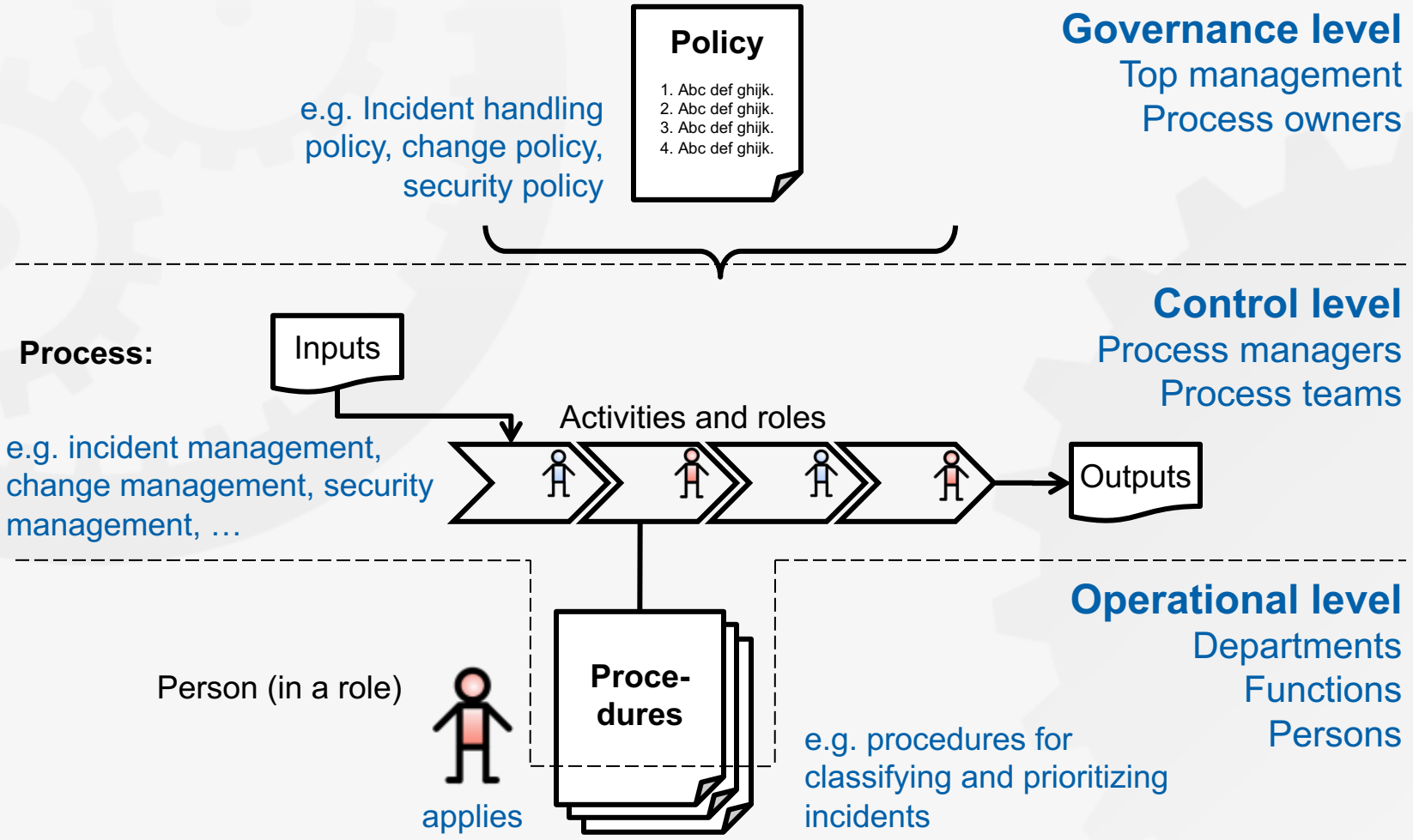
Definition following FitSM-0:

Service management system (SMS):

Overall m*anagement system* that controls and supports *(IT) service management* within an organisation or *federation*

- Key elements in an SMS:
  - Policies
  - Processes
    - Inputs
    - Activities
    - Outputs
  - Roles
  - Procedures

Service management system (SMS)



Policies and processes

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*

Note: Policies are then realised in processes, which are in turn made up of procedures that people carry out.

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

Note: Generally, a process is a logical subdivision of a larger set of activities used to provide or manage services.

Activities and procedures

Definition following FitSM-0:

Activity:

Set of actions carried out within a *process*

Definition following FitSM-0:

Procedure:

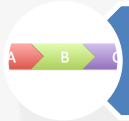
Specified set of steps or instructions to be carried out by an individual or team to perform one or more *activities* of a *process*

What is a process?

- How to define a process:

Goal(s), objectives

Clearly defined inputs, triggers and outputs



Set of interrelated activities

Roles and responsibilities

Definition following FitSM-0:

Role:

Set of responsibilities collected into a logical unit that can be assigned to an individual

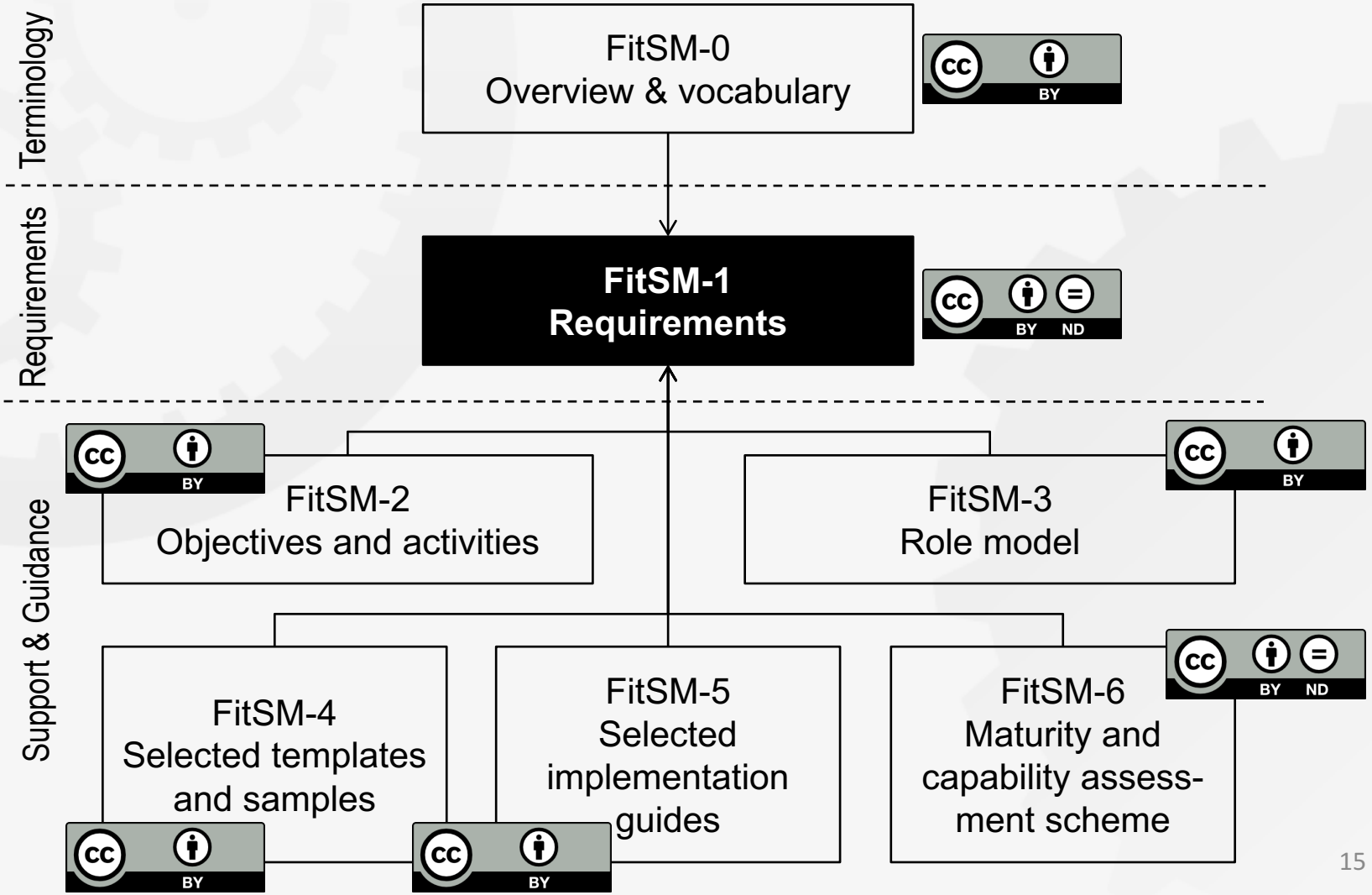
What is FitSM?

- 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 freely available:

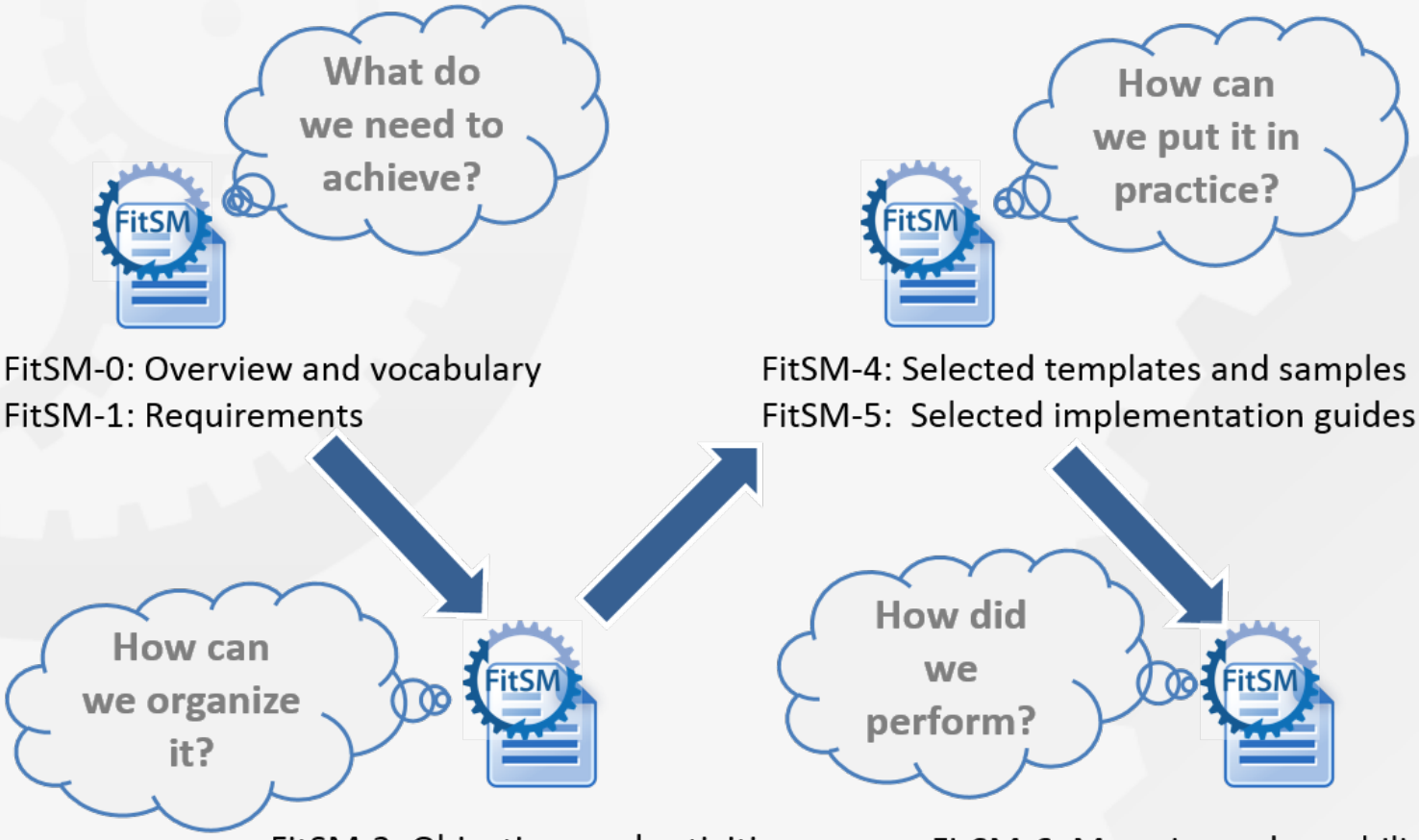
www.fitsm.eu

The development of the FitSM standards is supported and funded by the European Commission through the EC-FP7 project "FedSM" under contract number 312851.

FitSM parts


Terminology
Requirements
Support & Guidance
FitSM-0
Overview & vocabulary
FitSM-1
Requirements
FitSM-2
Objectives and activities
FitSM-3
Role model
FitSM-4
Selected templates and samples
FitSM-5
Selected implementation guides
FitSM-6
Maturity and capability assess-ment scheme

FitSM logic



FitSM-0: Overview and vocabulary
FitSM-1: Requirements

FitSM-4: Selected templates and samples
FitSM-5: Selected implementation guides

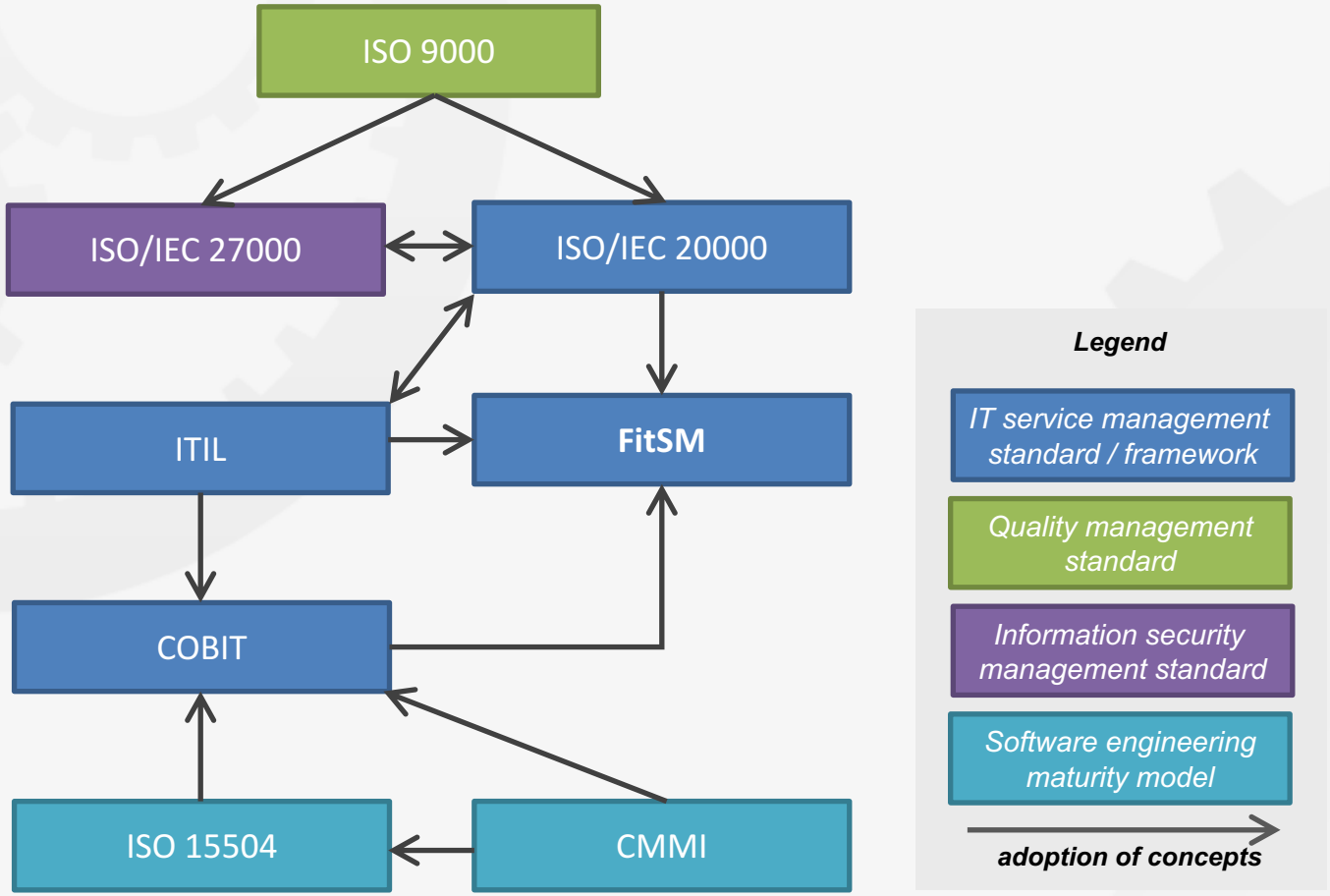
FitSM-2: Objectives and activities
FitSM-3: Role model

FitSM-6: Maturity and capability assessment scheme

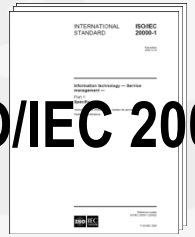
FitSM: ITSM process framework

1. Service portfolio management (SPM)
2. Service level management (SLM)
3. Service reporting management (SRM)
4. Service availability & continuity management (SACM)
5. Capacity management (CAPM)
6. Information security management (ISM)
7. Customer relationship management (CRM)
8. Supplier relationship management (SUPPM)
9. Incident & service request management (ISRM)
10. Problem management (PM)
11. Configuration management (CONFM)
12. Change management (CHM)
13. Release & deployment management (RDM)
14. Continual service improvement management (CSI)

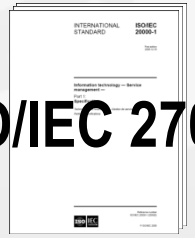
Related standards and frameworks



ITIL, ISO/IEC 20000, COBIT

ITIL	**IT Infrastructure Library** • 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	• Most popular and wide-spread framework • Not a "real" standard, but often related 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 • Defines the minimum requirements on ITSM	• 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** • IT Governance framework • Specifies control objectives, metrics, maturity models	• Developed by ISACA • can be combined with ITIL and ISO/IEC 20000

ISO 9000, ISO/IEC 27000, CMMI



ISO 9000 • International standard for quality management • Quality management principles • Minimum requirements for a quality management system	• Applicable to all organizations and branches • Auditable, certifiable • Several documents
ISO/IEC 27000 • International standard for information security management • Minimum 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
Capability Maturity Model Integration • Maturity and capability model • Organizational maturity assessment	• Developed by SEI (Software Engineering Institute), Carnegie Mellon University

ITSM: Benefits and risks in practice

Typical benefits (excerpt):

- \+ Repeatability of desired outputs
- \+ Higher effectiveness and efficiency
- \+ Customer focus, alignment of IT and their customers
- \+ 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 and personnel do not accept the system
  - − top management lacks a clear commitment and related actions
  - − processes are bypassed

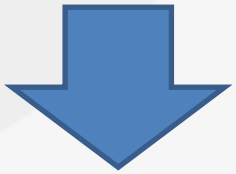
Challenges in federated IT infrastructures

- Traditional IT service management practices …
  - assume single central control over all service management processes by the service provider
  - hardly address collaborative approaches to service delivery
- As a result: Applying IT service management in federated environments may be more difficult, and not all concepts / ideas will work
- Important in a federated environment: Understanding the roles of the federation members as well as the federator's business model

Examples of federator roles ("business models")

Every federation member has to manage their specific services, i.e. ITSM is often **highly decentralized**, and overall integration / coordination is limited to key process interfaces.

ITSM perspective



The integrator needs to manage the services offered by the federation, i.e. ITSM is often more centralized, and a **high level of coordination effort** is required from the integrator.

- Invisible Coordinator
- Advisor
- Matchmaker
- One Stop Shop
- Integrator

Agenda of this training

- FitSM Foundation wrap-up & ITSM basics
- ➢ **Selected general aspects of establishing a service management system (SMS)**
- ITSM processes for the operation and control of services
- ITSM process interfaces and dependencies

Standards for lightweight
IT service management

Selected General Aspects of Establishing a Service Management System

Overview

- Top management responsibility
  - Commitment and leadership
  - Governance and policies
- Documentation
  - Documents and records
  - Document control
- Defining the scope of service management
- The PDCA cycle applied to the SMS
  - Planning service management (PLAN)
  - Implementing service management (DO)
  - Monitoring and reviewing service management (CHECK)
  - Continually improving service management (ACT)

FitSM

Standards for lightweight
IT service management

Top management responsibility

Why?

To ensure that top management of the organisation(s) involved in the delivery of services is clearly committed to a service- and process-oriented approach and that they fulfil their leadership duties

Top management responsibility: Important terms & concepts

Definition following FitSM-0:

Top management:

Senior management within the *service provider* organisation or *federation* who set *policies* and exercise overall control of the organisation or *federation.*

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*

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

FitSM

Standards for lightweight
IT service management

Documentation

Why?

To ensure that policies, processes and procedures and their outputs are sufficiently documented to support and enhance effectiveness and traceability of IT service management

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

Documentation: Important terms & concepts

Definition following FitSM-0:

Document:

Information and its supporting medium

Note: Examples of documents include policies, plans, process descriptions, procedures, SLAs, contract or records.

Definition following FitSM-0:

Record:

Documentation of an event or the results of performing a *process* or *activity*

Documentation: Examples

- Examples of documents that are **not** records:
  - Policy
  - Plan
  - Process description
  - Procedure definition
  - Agreement
  - Contract
- Examples of documents that **are** records:
  - Ticket (e.g. incident / service request / change ticket)
  - Training record
  - Audit report
  - Meeting minutes
  - Visitor list / guestbook

FitSM

Standards for lightweight
IT service management

Defining the scope of service management

Why?

To agree and document the extent and boundaries of the SMS by clearly defining the service(s), organisation(s) and location(s) for which the SMS is valid

Defining the scope of service management: Requirements according to FitSM-1

GR3 Defining The Scope Of Service Management
REQUIREMENTS
• GR3.1 The scope of the SMS shall be defined and a scope statement created.

- The scope of the SMS may be limited to …
  - certain services or service catalogues
  - certain technologies
  - certain (geographical) locations
  - certain organisations or parts of organisations
  - certain parts of a federation (in a federated environment)
  - service provision for specific (groups of) customers / users

Defining the scope of service management: Examples of scope statements

- Generic scope statement:

  The SMS of [name of the service provider or federation] that delivers [technology] [service(s)] from [service provider location(s)] to [customer(s)] at [customer(s') location(s)]

- Example:

  The SMS of the ACME IT service unit that delivers Microsoft Windows-based desktop and communication services from their data center site in Amsterdam to all ACME business units at locations in The Netherlands

FitSM

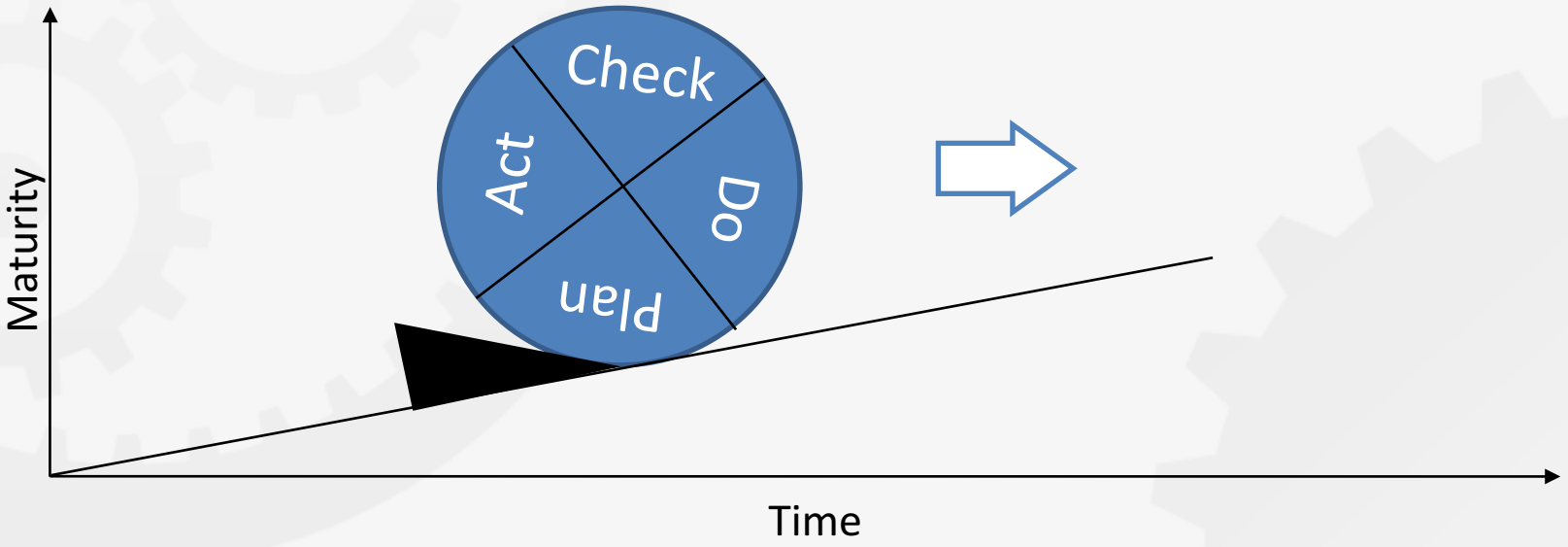
Standards for lightweight
IT service management

The PDCA cycle applied to the SMS

Why?

To ensure that the SMS as a whole is solidly planned, implemented, monitored and continually improved

Plan-Do-Check-Act Cycle (PDCA)



- Quality management approach according to W. E. Deming
- Cyclical optimization of quality leads to continual improvement
- Plan-Do-Check-Act can be applied to the whole service management system

PDCA applied to the SMS: Brief overview

- Plan: GR3, GR4
  - Define the scope of the SMS
  - Set the timeline for implementing service management processes (service management plan)
- Do: GR5
  - Implement processes
  - Provide training to people involved in the 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

Planning ITSM: Requirements according to FitSM-1

GR4 Planning Service Management (PLAN)
REQUIREMENTS

• GR4.1 A service management plan shall be created and maintained.
• GR4.2 The service management plan shall at minimum include or reference:
  ○ Goals and timing of implementing the SMS and the related processes
  ○ Overall roles and responsibilities
  ○ Required training and awareness activities
  ○ Required technology (tools) to support the SMS
• GR4.3 Any plan shall be aligned to other plans and the overall service management plan.

Planning ITSM: Roles and responsibilities

	Description	ITSM example	Non-ITSM example
Generic role	A conceptual class of role which is instantiated in a specific context to create a specific role	Process manager	Flight captain
Specific role	A concrete role which can be assigned to a person or team in order to give this person or team the responsibility for something	Incident manager (process manager for the incident and service request management process) of an IT service provider	Flight captain for flight XX123 from Munich to Brussels

Planning ITSM:
Generic roles according to FitSM-3

- SMS owner
- SMS manager
- Process owner (optional)
- Process manager
- Case owner
- Member of process staff
- Service owner

SMS owner: General tasks

Role	Tasks	Ca. number of persons performing this role
SMS owner	• Senior accountable owner of the entire service management system (SMS) • Overall accountability for all ITSM-related activities • Act as the primary contact point for concerns in the context of governing the entire SMS • Define and approve goals and policies for the entire SMS • Nominate the process owners and/or managers, and ensure they are competent to fulfil their roles • Approve changes to the overall SMS • Decide on the provision of resources dedicated to ITSM • Based on monitoring and reviews, decide on necessary changes in the goals, policies and provided resources for the SMS	1 for the overall SMS *Often, the person taking over the SMS owner role may also take over the process owner role for the entirety or a subset of the ITSM processes.*

SMS manager: General tasks

Role	Tasks	Ca. number of persons performing this role
SMS manager	• Act as the primary contact point for all tactical concerns (including planning and development) in the context of the entire SMS • Maintain the service management plan and ensure it is available to relevant stakeholders • Ensure IT service management processes are implemented according to approved goals and policies • Maintain an adequate level of awareness and competence of the people involved in the SMS, in particular the process managers • Monitor and keep track of the suitability, effectiveness and maturity of the entire SMS • Report and, if necessary, escalate to the SMS owner • Identify opportunities for improving the effectiveness and efficiency of the SMS	1 for the overall SMS

Process owner: General tasks

Role	Tasks	Ca. number of persons performing this role
Process owner *(optional, see comment in right column)*	• Act as the primary contact point for concerns in the context of governing one specific ITSM process • Define and approve goals and policies in the context of the process according to the overall SMS goals and policies • Nominate the process manager, and ensure he / she is competent to fulfil this role • Approve changes / improvements to the operational process, such as (significant) changes to the process definition • Decide on the provision of resources dedicated to the process and its activities • Based on process monitoring and reviews, decide on necessary changes in the process-specific goals, policies and provided resources	1 per process *In many situations in practice, the SMS owner takes over the role of the process owner for all ITSM processes. If this is the case, it is not required to establish the process owner role as a dedicated role at all, since it is merged with the SMS owner role.*

Process manager: General tasks

Role	Tasks	Ca. number of persons performing this role
Process manager	• Act as the primary contact point for operational concerns in the context of the process • Maintain the process definition / description and ensure it is available to relevant persons • Maintain an adequate level of awareness and competence of the people involved in the process • Monitor and keep track of the process execution and results (incl. process reviews) • Report on process performance to the process owner • Escalate to the process owner, if necessary • Identify opportunities for improving the effectiveness and efficiency of the process • ***Additional tasks – depending on the specific process (see: process-specific role models)***	1 per process *One person may take over the process manager role for one or more processes.*

Case owner: General tasks

Role	Tasks	Ca. number of persons performing this role
Case owner	• Overall responsibility for one specific case occurring in a process context (e.g. one specific incident to be resolved or one specific SLA to be maintained) • Act as the primary contact point for all concerns in the context of that specific case • Coordinate all activities required to handle / resolve the specific case • Escalate exceptions to the process manager, where required • ***Additional tasks – depending on the specific process (see: process-specific role models)***	1 per case *There may be different cases per process at a time. One person or group may be assigned the case owner role for one or more (or even all) concurrent cases.*

Note: The role of a case owner is usually required in a process, if occurrences (e.g. incidents, service requests, problems, changes, releases, …) or logical entities / objects (e.g. different types of agreements, reports or plans, …) are managed by the process, and the process manager him- / herself does not take over specific responsibility for all of these occurrences or entities.

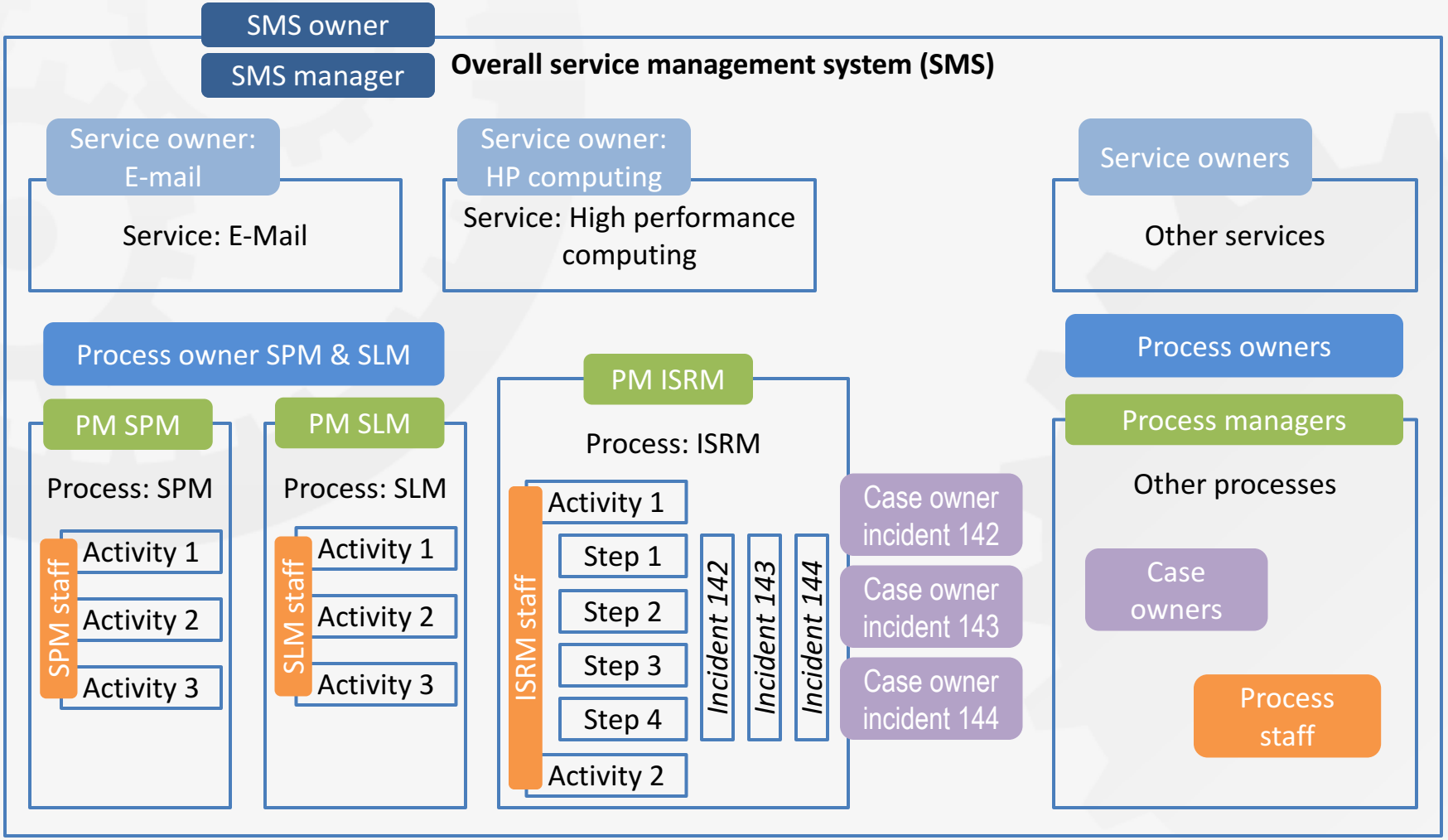
Member of process staff: General tasks

Role	Tasks	Ca. number of persons performing this role
Member of process staff *(sometimes also referred to as process practitioner)*	• Carry out defined activities according to the defined / established process and, as applicable, its procedures (e.g. the activity of prioritizing an incident) • Report to the case owner and / or process manager • ***Additional tasks – depending on the specific process (see: process-specific role models)***	1 or more per process *One person may take over the member of process staff role for one or more processes.*

Service owner: General tasks

Role	Tasks	Ca. number of persons performing this role
Service owner	• Overall responsibility for one specific service which is part of the service portfolio • Act as the primary contact point for all (process-independent) concerns in the context of that specific service • Act as an “expert” for the service in technical and non-technical concerns • Maintain the core service documentation, such as the service specification / description • Be kept informed of every event, situation or change connected to the service • Be involved in tasks significantly related to the service as part of selected ITSM processes, in particular SPM and SLM ***(see: process-specific role models)*** • Report on the service to the SMS owner	1 per service in the service portfolio *One person may take over the service owner role for one or more (or even all) services.*

Planning ITSM: Summary of the role model



Implementing ITSM: Requirements according to FitSM-1

GR5 Implementing Service Management (DO)
REQUIREMENTS
• GR5.1 The service management plan shall be implemented. • GR5.2 Within the scope of the SMS, the defined service management processes shall be followed in practice, and their application, together with the adherence to related policies and procedures, shall be enforced.

Monitoring and reviewing ITSM: Requirements according to FitSM-1

GR6 Monitoring And Reviewing Service Management (CHECK)
REQUIREMENTS
• GR6.1 The effectiveness and performance of the SMS and its service management processes shall be measured and evaluated based on suitable key performance indicators in support of defined or agreed targets. • GR6.2 Assessments and audits of the SMS shall be conducted to evaluate the level of maturity and compliance.

Continually improving ITSM: Requirements according to FitSM-1

GR7 Continually Improving Service Management (ACT)
REQUIREMENTS
• GR7.1 Nonconformities and deviations from targets shall be identified and corrective actions shall be taken to prevent them from recurring. • GR7.2 Improvements shall be planned and implemented according to the Continual Service Improvement Management process (see PR14).

Agenda of this training

- FitSM Foundation wrap-up & ITSM basics
- Selected general aspects of establishing a service management system (SMS)
- **ITSM processes for the operation and control of services**
- ITSM process interfaces and dependencies

Standards for lightweight
IT service management

ITSM Processes for the Operation & Control of Services

Overview

- Incident & service request management (ISRM)
- Problem management (PM)
- Configuration management (CONFM)
- Change management (CHM)
- Release & deployment management (RDM)
- Continual service improvement management (CSI)

Common structure of the presentation of ITSM processes in this training material

- Objective
- Important terms & concepts
- Process-specific requirements according to FitSM-1
- Initial process setup
- Inputs & outputs
- Ongoing process activities
- Roles
- Critical success factors & KPIs
- Simplified application example 

} for selected ITSM processes

Overview

- **Incident & service request management (ISRM)**
- Problem management (PM)
- Configuration management (CONFM)
- Change management (CHM)
- Release & deployment management (RDM)
- Continual service improvement management (CSI)

FitSM

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 & concepts

Definition following FitSM-0:

Incident:

Unplanned disruption of operation in a *service* or degradation of service quality (versus the expected or agreed level of operation according to *service level agreements*)

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: Important terms & concepts

Definition following FitSM-0:

Priority:

Relative importance of a target, object or *activity*

Note: Often incidents, service requests, problems and changes are given a priority. In the case of incidents and problems, priority is usually based on the specific impact and urgency of the situation.

Definition following FitSM-0:

Classification:

The act of breaking down a set of items into a set of categories

ISRM: Service request or incident?

The capacity of the hard disk drive in my notebook is insufficient! → ?

The resource I am trying to access does not respond! → ?

It takes a very long time for my job to complete! → ?

I forgot my Wiki password! → ?

I cannot access my e-mails! → ?

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: Initial process setup

Initial activities	Typical results
Set up a tool (e.g. ticket / workflow tool) supporting the recording and handling (including classification, prioritization, escalation, closure) of reported incidents and service requests.	Initial (empty) incident and service request recording system
Define a standardized and repeatable way of recording incidents and service requests that specifies the sources and channels through which incidents and service requests may be raised, the required format of an incident report or service request, and the way in which the incident or service request is recorded in the recording system.	Generic template(s) for incident records and service request records; procedure for recording incidents and service requests

ISRM: Initial process setup

Initial activities	Typical results
Define a standardized and repeatable way of classifying incidents and service requests that specifies a suitable classification scheme and describes how it should be applied.	Procedure for classifying incidents and service requests
Define a standardized and repeatable way of prioritizing incidents and service requests that specifies a suitable prioritization scheme and describes how the priority of an incident or service request should be calculated.	Procedure for prioritizing incidents and service requests
Define a standardized and repeatable way of escalating incidents and service requests that specifies functional and hierarchical escalation paths.	Procedure for escalating incidents and service requests

ISRM: Initial process setup

Initial activities	Typical results
Define a standardized and repeatable way of closing incidents and service requests that specifies how incidents and service requests are closed, including required user communication and confirmation.	Procedure for closing incidents and service requests
Define the criteria for identifying a major incident, as well as a standardized and repeatable way of dealing with major incidents from recording to closure, including a major incident review.	Criteria for identifying a major incident; major incident procedure

ISRM: Initial process setup

Initial activities	Typical results
Identify well-known and recurring incidents, and for each of them describe, where required, the concrete steps to be carried out in response to the respective incident in order to manage it effectively from recording to closure.	List of “standard incidents”; templates and / or procedures for handling them
Identify standardized service requests based on service descriptions and SLAs, and for each of them describe, where required, the concrete steps to be carried out in response to the respective service request in order to manage it effectively from recording to closure.	List of “standard service requests”; templates and / or procedures for handling them

ISRM: Inputs & outputs

Inputs

Incidents reported by users or identified by the service provider

Service requests raised by users

Configuration information (CMDB)

Outputs

Incident records

Service request records

Major incident review reports

Requests for changes raised to trigger the change management process, in order to commence the fulfilment of service requests

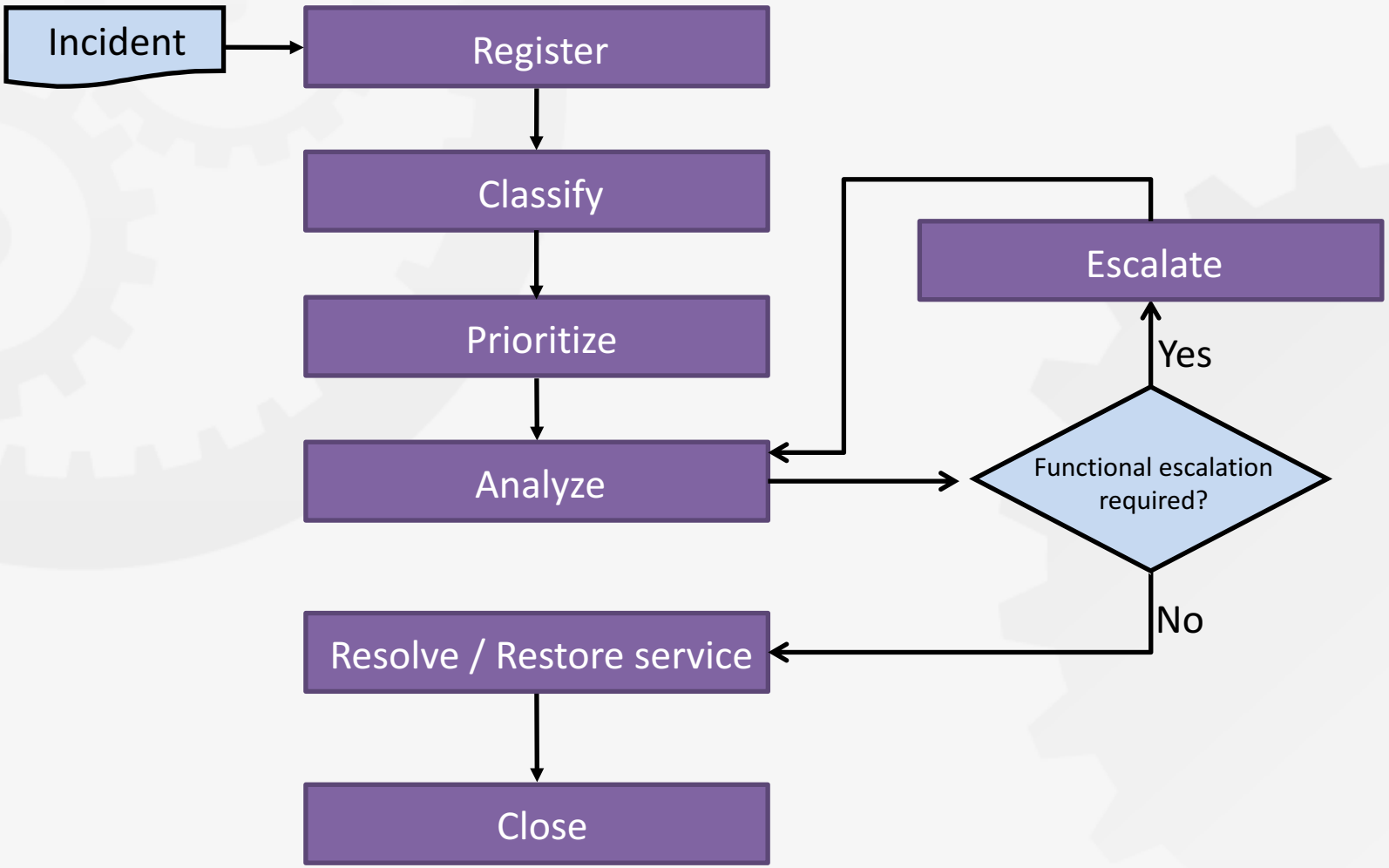
Up-to-date descriptions of step-by-step workflows for standard incidents and service requests

Regular incident reports

ISRM: Ongoing process activities

- Manage incidents (including major incidents) and service requests
  - Record an incident or service request
  - Classify an incident or service request
  - Prioritize an incident or service request
  - Escalate an incident or service request
  - Resolve an incident or service request
  - Close an incident or service request
  - Perform a major incident review
- Maintain the step-by-step workflows for well-known and recurring incidents and standardized service requests

ISRM: Workflow



ISRM: Roles

Role	Tasks	Ca. number of persons performing this role
Process owner ISRM	*Generic tasks of a process owner applied in the context of ISRM*	1 in total
Process manager ISRM	*Generic tasks of a process manager, plus:* • Ensure that all incidents and service requests are recorded, and that records are of sufficient quality to enable traceability and long-term analysis • Monitor the overall progress of incident resolution and service request fulfilment, and identify potential violations of target response and resolution times	1 in total

ISRM: Roles

Role	Tasks	Ca. number of persons performing this role
Incident owner / service request owner	• Coordinate and take over overall responsibility for all activities in the lifecycle of a specific incident or service request • Monitor the progress of incident resolution or request fulfilment taking into account agreed timeframes • Trigger reminders to those involved in incident resolution or request fulfilment and escalate to the process manager as required • In case of a (potential) SLA violation, trigger communication and escalation as defined in the SLM process • Ensure an adequate level of documentation for the specific incident or service request	1 per incident / service request

ISRM: Critical success factors & KPIs

Critical success factors	Key performance indicators (KPIs)
All incidents and service requests are recorded.	• Number of incident and service request records versus number of incidents and service requests actually reported (e.g. based on call / e-mail statistics)
Incidents and service requests are prioritized effectively.	• Distribution of assigned priorities • Relation between assigned priorities and resolution / fulfilment times • Number / percentage of major incidents
Escalation paths are clearly defined and effectively applied.	• Number / percentage of mis-routed incidents and service requests • Total / average delay due to bad / ineffective functional escalation • Total / average delay due to missed hierarchical escalation

ISRM: Critical success factors & KPIs

Critical success factors	Key performance indicators (KPIs)
Incidents are resolved quickly and effectively.	• Percentage of incidents that had to be re-opened after closure • Average incident resolution time (per priority) • Number of violations of maximum resolution times according to SLAs
Service requests are fulfilled in time, according to agreed fulfilment times.	• Average service request fulfilment time (per service request type, priority) • Number of violations of maximum fulfilment times according to SLAs

A simplified example

- A customer is on the phone and complains that the order for 5 large “Pizza Supreme” that he placed online 30 minutes ago hasn’t been delivered yet.

  - Is this an incident?
  - If it is an incident: What should be the pre-defined steps in a standardized procedure for handling this kind of incident?

Overview

- Incident & service request management (ISRM)
- **Problem management (PM)**
- Configuration management (CONFM)
- Change management (CHM)
- Release & deployment management (RDM)
- Continual service improvement management (CSI)

FitSM

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 problem, or to ensure workarounds / temporary fixes are available

PM: Important terms & concepts

Definition following FitSM-0:

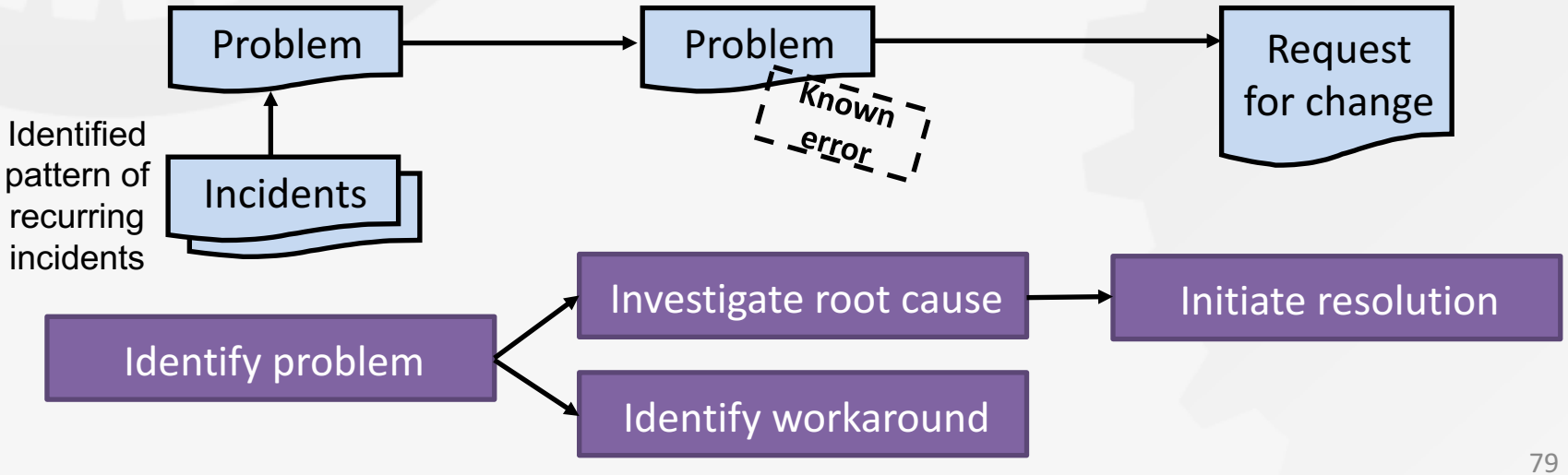
Problem:

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: Initial process setup

Initial activities	Typical results
Define a standardized and repeatable way to record problems, known errors and related workarounds, and set up an initial known error database (KEDB).	Generic template for a problem record; procedure for recording problems
Set up a tool (e.g. ticket / workflow tool) supporting the recording and handling (including classification, prioritization, escalation, closure) of identified problems.	Initial (empty) problem recording system

PM: Inputs & outputs

Inputs

Statistics on incidents and service requests (for trend analysis)

Incident and service request records

Other relevant sources of information to identify (new) problems, including change and release records

Configuration information (CMDB)

Outputs

Up-to-date KEDB with information (records) on problems, known errors and related workarounds

Requests for changes raised to trigger the change management process, in order to resolve the underlying root cause(s) of identified problems / known errors

PM: Ongoing process activities

- Perform regular incident trend analysis to identify (new) problems
- Manage problems
  - Identify and record a problem
  - Classify a problem
  - Prioritize a problem
  - Escalate a problem
  - Resolve a problem
  - Close a problem
- Maintain the KEDB
  - Add a known error (and workaround) to the KEDB
  - Update a known error (and workaround) in the KEDB
  - Remove a known error (and workaround) from the KEDB
  - Perform a KEDB review

PM: Roles

Role	Tasks	Ca. number of persons performing this role
Process owner PM	*Generic tasks of a process owner applied in the context of PM*	1 in total
Process manager PM	*Generic tasks of a process manager, plus:* • Ensure that incident trends are regularly analysed to identify problems • Ensure that identified problems are recorded, and that records are of sufficient quality • Ensure that problems are analysed, information on known errors recorded, and problems brought to closure	1 in total

PM: Roles

Role	Tasks	Ca. number of persons performing this role
Problem owner	• Coordinate and take over overall responsibility for all activities in the lifecycle of a specific problem, including problem analysis and identification of options to handle the problem • Monitor the progress of problem resolution and ensure that the problem is escalated effectively, if required • Ensure the information in the KEDB on this problem / known error are up-to-date, including appropriate descriptions of potential workarounds • Communicate the problem / known error and potential workarounds to relevant stakeholders (e.g. ISRM staff and service users) • Depending on the selected option for dealing with the problem / known error, raise requests for changes or trigger the continual service improvement process as required	1 per problem

PM: Critical success factors & KPIs

Critical success factors	Key performance indicators (KPIs)
Problems are recorded.	• Number of newly created problem records per month • Percentage of incidents linked to problem records
A known error database (KEDB) is set up and kept up-to-date.	• Number of known error records • Percentage of known error records updated in the last three months
Effective workarounds are described in the KEDB and made available to staff involved in the incident management process.	• Percentage of incidents linked to known error records
If possible, problems are resolved.	• Percentage of resolved problems
Problems are brought to closure.	• Age of oldest problem record • Age of oldest known error record • Number of problem records not updated in the last three months

A simplified example

- In the past month, 15 incidents have been recorded, where customers complained about cold pizzas.

  - Record the problem! (What information / fields should be mandatory for the problem record?)
  - Perform a preliminary analysis of possible root causes! (Do you know a problem analysis / brainstorming technique you could use?)

Overview

- Incident & service request management (ISRM)
- Problem management (PM)
- **Configuration management (CONFM)**
- Change management (CHM)
- Release & deployment management (RDM)
- Continual service improvement management (CSI)

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 & concepts

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

Note: CIs vary widely and can be anything from technical components (computer hardware, network components, cables, software) to documents (SLAs, manuals, contracts, license documentation).

Definition following FitSM-0:

Configuration management database (CMDB):

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

Note: The CMDB likely includes attributes of CIs as well as information on relationships between them.

CONFM: Important terms & concepts

Definition following FitSM-0:

Configuration baseline:

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

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: Initial process setup

Initial activities	Typical results
Define the scope of the configuration management process and the integrated configuration management database (CMDB).	CMDB scope statement
Identify and define CI types (including their attributes) and relationship types.	CMDB model document, CI type specifications
Based on the defined scope, identify all existing sources of configuration information in the environment of the service provider.	List of definitive sources of configuration information (and a mapping to CI types, relationships and their attributes)
Create a configuration management plan to describe the concept for integrating available sources of configuration information and add missing configuration information to the integrated CMDB, including the selection of appropriate supporting technology / tools.	Configuration management plan

CONFM: Inputs & outputs

Inputs

Relevant information / data on configuration items (CIs) and their relationships

Information on changes to CIs

Outputs

Up-to-date logical model of all relevant CIs and their attributes and relationships, reflected by the information / records stored in the configuration management database (CMDB)

Configuration baselines

Configuration verification reports

CONFM: Ongoing process activities

- Continual maintenance of documentation of the current configuration
  - Create a configuration record
  - Update a configuration record
- Verify information in CMDB
  - Plan automated and non-automated configuration verifications
  - Perform a configuration verification
  - Inform stakeholders about inconsistencies and identify follow-up actions

CONFM: Roles

Role	Tasks	Ca. number of persons performing this role
Process owner CONFM	*Generic tasks of a process owner applied in the context of CONFM*	1 in total
Process manager CONFM	*Generic tasks of a process manager, plus:* • Maintain the definitions of all CI and relationship types • Plan regular verifications of the configuration information held in the CMDB • Ensure that configuration verifications are conducted and identified nonconformities addressed • Take a configuration baseline when needed	1 in total
CI owner	• Ensure that the information on a specific CI in the CMDB is accurate and up-to-date • Collaborate with the process manager and other CI owners to ensure that all information on the relationships from / to a specific CI are accurate and up-to-date	1 per CI

CONFM: Critical success factors & KPIs

Critical success factors	Key performance indicators (KPIs)
Balanced approach to CMDB scope and model	• Number of defined CI and relationship types • Number of CI and relationship attributes • Number of actual CIs and attributes • Percentage of incident, service request, problem and change records linked to CIs • Average and maximum number of CIs linked to of incident, service request, problem and change records • Average workload for creating and updating CIs
Effective control over configuration information	• Percentage of nonconformities per configuration item reviewed

A simplified example

- For a pizza delivery company, what would the scope and model for a CMDB look like?

  - Define at least 3 CI types (including attributes) and 1 relationship type
  - What would be the pros and cons of defining a “pizza box” CI type?

Overview

- Incident & service request management (ISRM)
- Problem management (PM)
- Configuration management (CONFM)
- **Change management (CHM)**
- Release & deployment management (RDM)
- Continual service improvement management (CSI)

Standards for lightweight
IT service management

Change Management (CHM)

Objective

To ensure changes to CIs 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 & concepts

Definition following FitSM-0:

Request for change:

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.

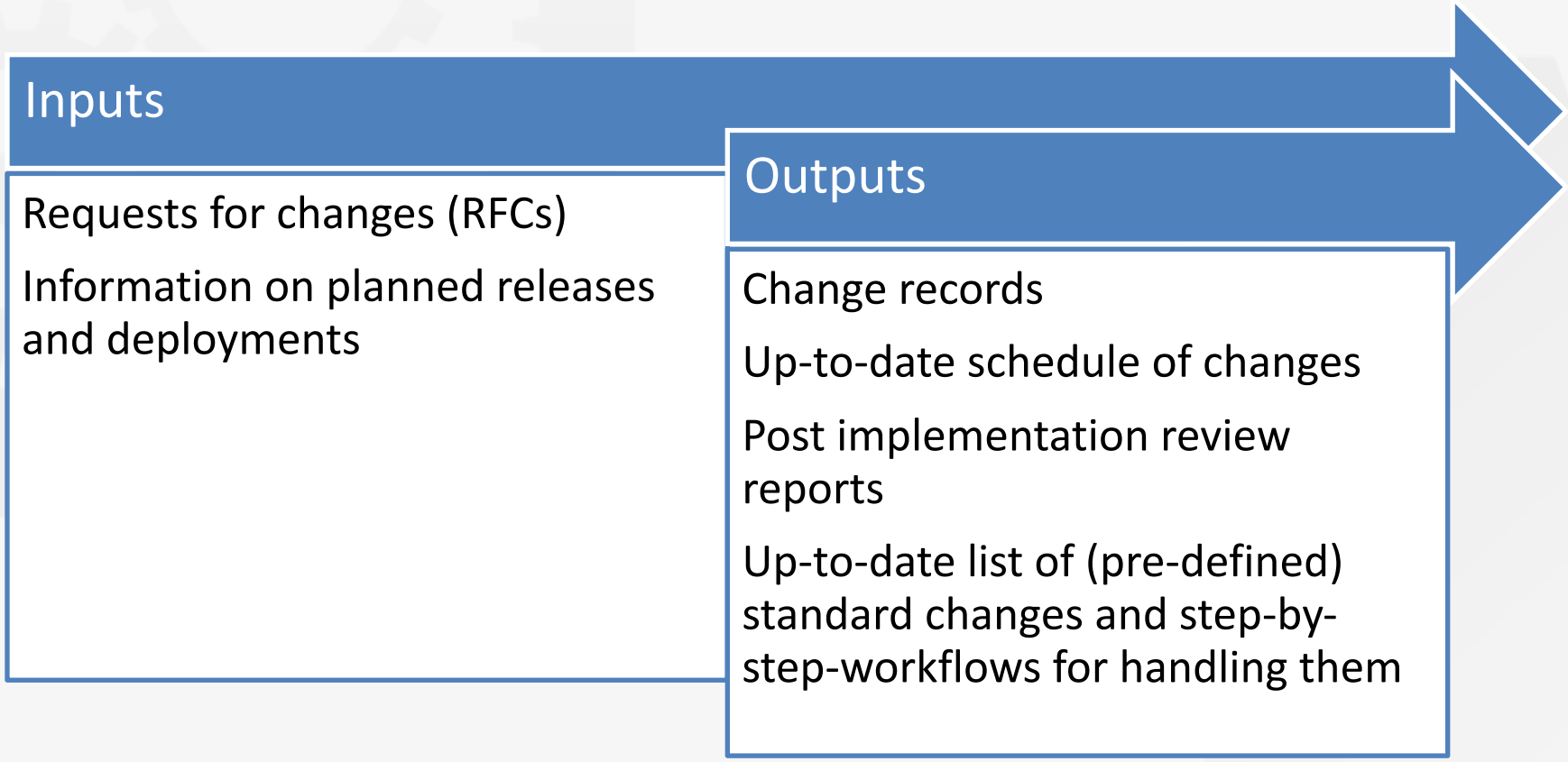
CHM: Initial process setup

Initial activities	Typical results
Set up a tool (e.g. ticket / workflow tool) supporting the recording and handling (including classification, evaluation, approval, implementation, post implementation review) of requested and approved changes.	Initial (empty) RFC / change recording system
Define a standardized and repeatable way of recording requests for changes (RFCs) and resulting approved changes that specifies the sources and channels through which RFCs may be raised, the required format of an RFC, and the way in which the RFC is recorded in the recording system.	Generic template(s) for change records; procedure for recording requests for changes

CHM: Initial process setup

Initial activities	Typical results
Define the criteria for identifying emergency changes, as well as a standardized and repeatable way of dealing with emergency changes from recording to closure, including an emergency change review.	Criteria for identifying a emergency changes, emergency change procedure
Identify well-known and recurring changes (standard changes), and for each of them describe, where required, the concrete steps to be carried out in order to manage the respective change effectively from recording to closure (including the steps for implementing the change and ensuring adequate traceability and documentation).	List of standard changes; templates and / or procedures for handling them

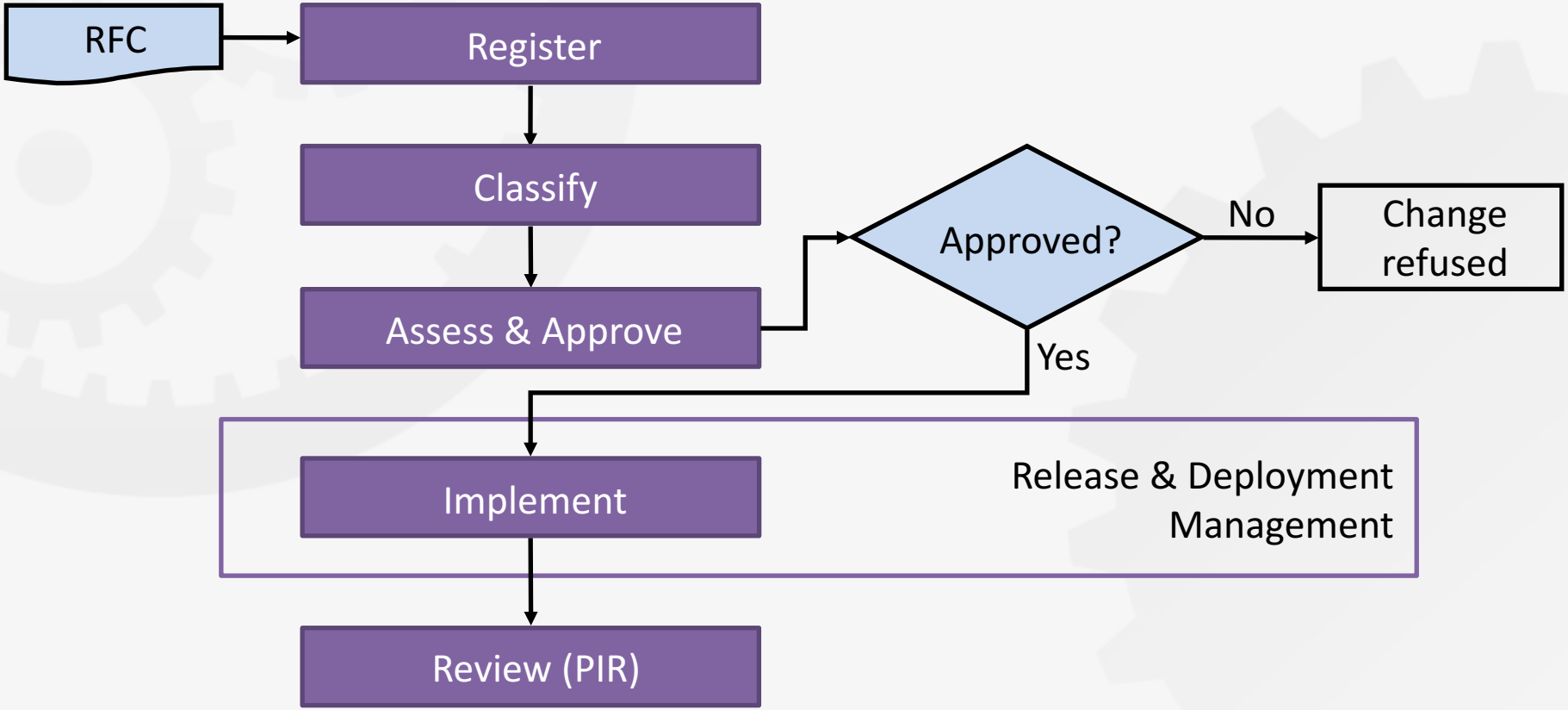
CHM: Inputs & outputs



CHM: Ongoing process activities

- Manage changes (including emergency changes)
  - Record an RFC
  - Classify an RFC
  - Evaluate an RFC
  - Approve a change
  - Implement a change
  - Perform a post implementation review
- Maintain the list, descriptions and step-by-step workflows for well-known and recurring changes (standard changes)
- Maintain the schedule of changes

CHM: Workflow



CHM: Roles

Role	Tasks	Ca. number of persons performing this role
Process owner CHM	*Generic tasks of a process owner applied in the context of CHM*	1 in total
Process manager CHM	*Generic tasks of a process manager, plus:* • Plan, schedule, prepare and moderate change advisory board (CAB) meetings • Maintain the list and descriptions of standard changes, together with relevant technical experts • Ensure that all requests for changes are processed effectively, and in a timely manner • Monitor the overall progress of change evaluation, approval and implementation • Review the change records in regular intervals, to identify trends or nonconformities or poor documentation / traceability	1 in total

CHM: Roles

Role	Tasks	Ca. number of persons performing this role
Change requester	• Raise a request for change • If necessary, provide additional information to the change manager and represent the change during a CAB meeting	1 per request for change
Change owner	• Control and coordinate all activities in the lifecycle of a specific change • Monitor the progress of change evaluation and implementation for this change • Ensure that the change record is complete and up-to-date at any time from recording the request for change to completion of the post implementation review • As applicable, communicate with the release owner of the release containing this change	1 per change

CHM: Roles

Role	Tasks	Ca. number of persons performing this role

Change advisory board (CAB)	• Evaluate non-standard changes, taking into account at least:
	  • Benefits
	  • Risks
	  • Potential impact
	  • Technical feasibility
	  • Effort / cost
	• Decide on the approval of non-standard changes, based on the evaluation results
	
	Important notes:
	• *The CAB should be composed of (all) relevant stakeholders of the changes that are currently subject to evaluation and approval.*
	• *CAB meetings should take place in regular intervals, although the specific composition of the CAB may / will vary.*
		1 board for a certain number of changes

CHM: Critical success factors & KPIs

Critical success factors	Key performance indicators (KPIs)
All changes to CIs are under the control of the change management process	• Number / percentage of (identified) changes that bypassed the change management process
The majority of low-risk, low-complexity, and high-frequency changes is handled as (pre-defined) standard changes, which are clearly defined.	• Number / percentage of standard changes versus the overall number of changes

A simplified example

- For a pizza delivery company, what are typical examples of changes that need to be managed?

  - Standard changes?
  - Non-standard (“normal”) changes?
  - Emergency changes?

Overview

- Incident & service request management (ISRM)
- Problem management (PM)
- Configuration management (CONFM)
- Change management (CHM)
- **Release & deployment management (RDM)**
- Continual service improvement management (CSI)

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 & concepts

Definition following FitSM-0:

Release:

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

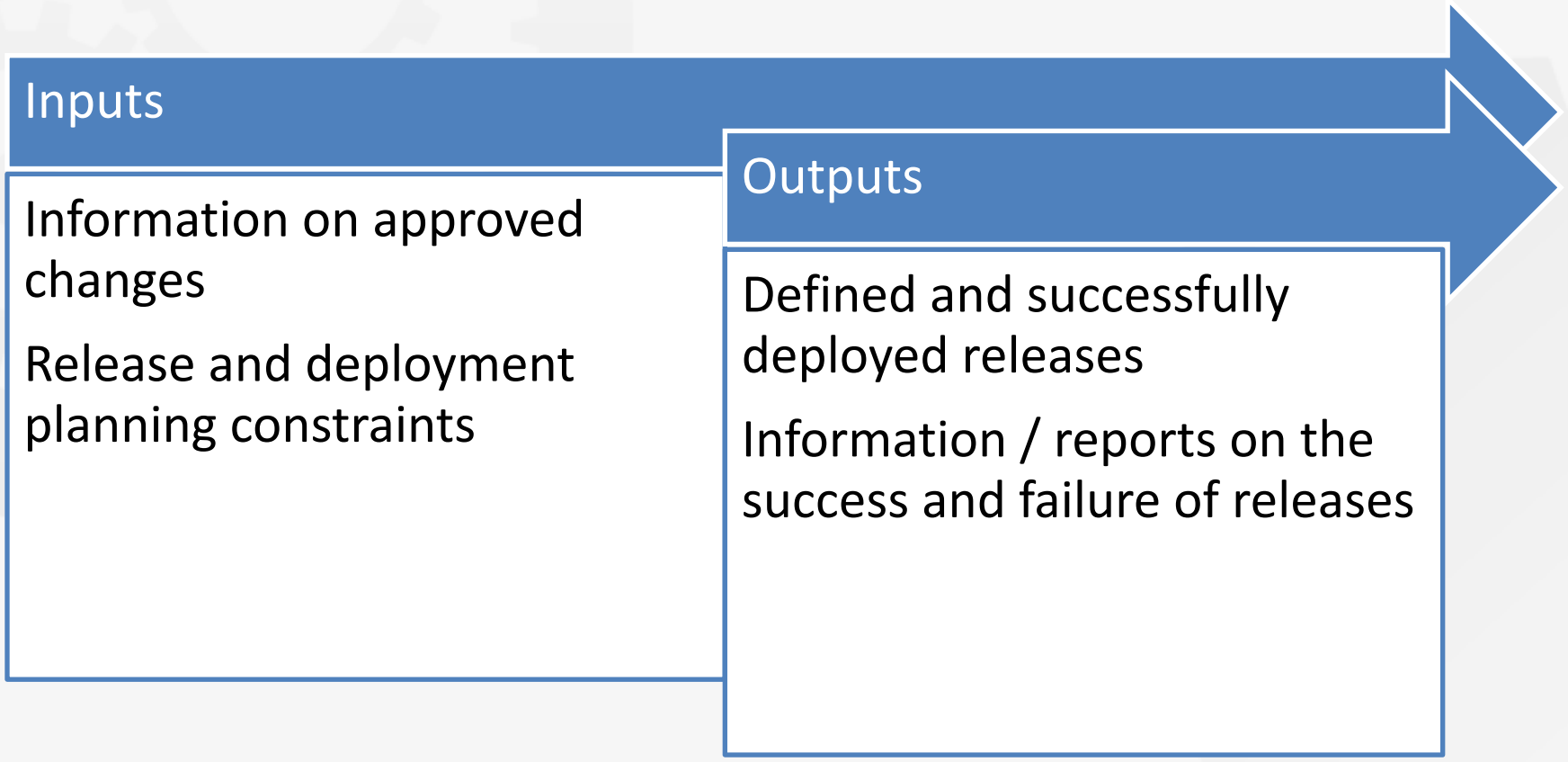
RDM: Requirements according to FitSM-1

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: Initial process setup

Initial activities	Typical results
Define a standardized way to define and plan releases, based on approved changes and the schedule of changes.	Template for a release plan
Define criteria for identifying different types of releases, such as major releases, minor releases or emergency releases.	List of criteria to classify releases
Define a release policy.	Release policy
Define a way to record the results of release and deployment testing and evaluation of acceptance criteria.	Template for a release readiness review report

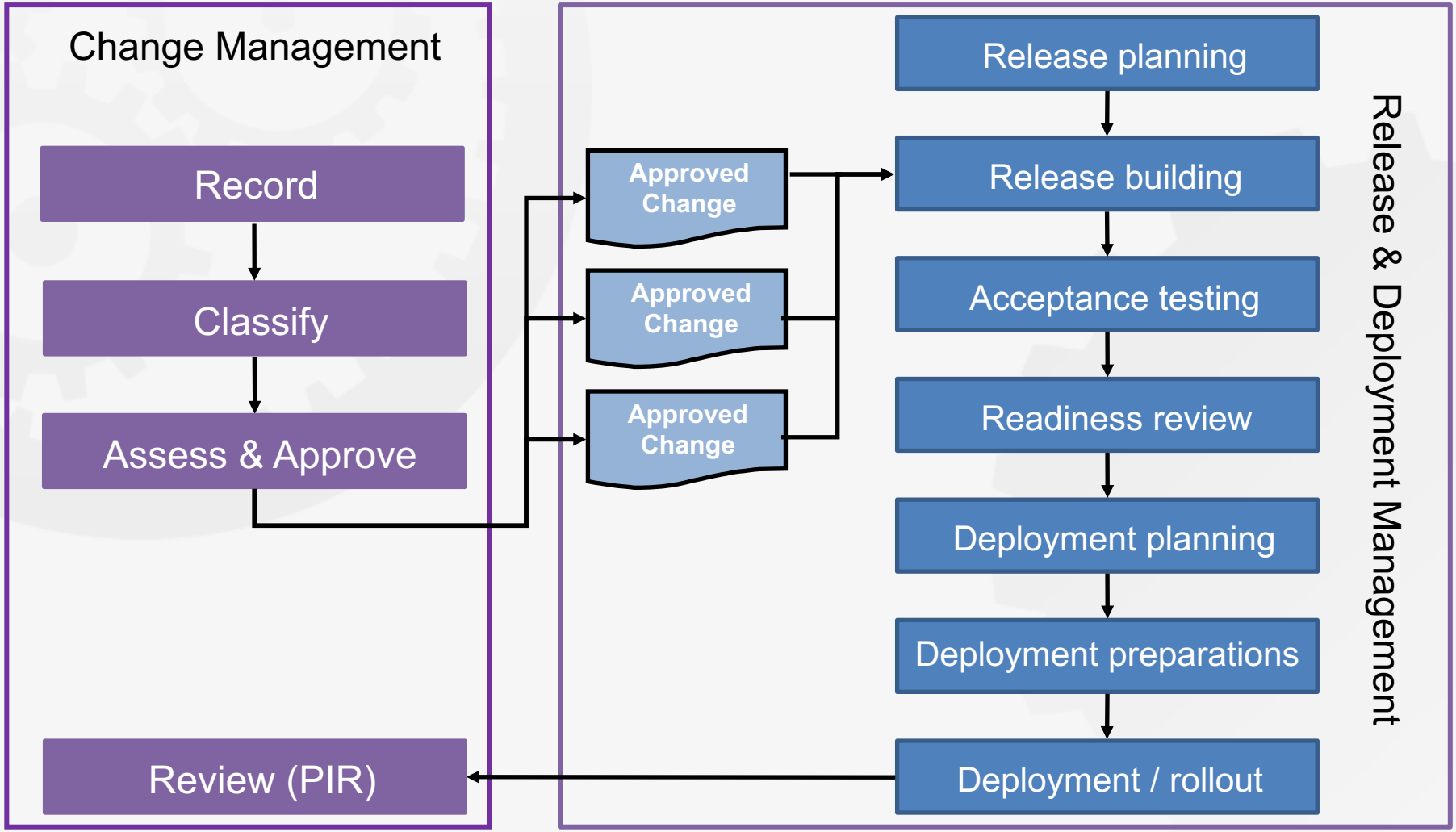
RDM: Inputs & outputs



RDM: Ongoing process activities

- Manage releases
  - Plan a release
  - Build a release
  - Test a release
  - Inform, educate and train users on deployment
  - Inform, educate and train support staff on deployment
  - Prepare the live environment for deployment
  - Deploy a release
  - Review a release for success

RDM: Workflow



RDM: Roles

Role	Tasks	Ca. number of persons performing this role
Process owner RDM	*Generic tasks of a process owner applied in the context of RDM*	1 in total
Process manager RDM	*Generic tasks of a process manager, plus:* • Maintain the overall release planning, including release cycles • Review deployed releases fur success	1 in total
Release owner	• Control and coordinate the activities in the lifecycle of a specific release, including planning, building, testing and deploying • Ensure that the required documentation of the release (including release plans) is complete and of adequate quality • Act as a single point of contact for the release for all stakeholders of this release, including the change manager, affected change owners, developers, problem manager and customer representatives.	1 per release

RDM: Critical success factors & KPIs

Critical success factors	Key performance indicators (KPIs)
Errors identified during release tests are either eliminated / resolved or recorded in the known error database (KEDB).	• (Average) number of errors identified and recorded in the KEDB per release • (Average) number / impact of incidents that occurred due to the deployment of a new release • (Average) number of identified problems connected to a deployed release that have not been identified during release tests
Appropriate transfer of knowledge prior to the deployment of a release	• Number of incidents and service requests raised due to poor user communication and education in the context of releases

Overview

- Incident & service request management (ISRM)
- Problem management (PM)
- Configuration management (CONFM)
- Change management (CHM)
- Release & deployment management (RDM)
- **Continual service improvement management (CSI)**

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: Important terms & concepts

- Types and typical sources of improvements:
  - Internal suggestions for improvement made by process managers, process staff members, service owners etc.
  - Audit findings / conclusions
  - Maturity / capability assessments
  - Customer feedback and complaints
  - Results from a customer satisfaction survey
  - Service review results
  - Service performance / SLA compliance reports

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.

CSI: Initial process setup

Initial activities	Typical results
Identify all relevant sources of potential suggestions for improvement.	List of sources of improvements / suggestions for improvements
Define a standardized and repeatable way of recording suggestions for improvements from the identified sources.	Template for recording an improvement / suggestion for improvement
Set up a tool (e.g. ticket / workflow tool) supporting the recording and handling (including prioritization, evaluation approval) of suggestions for improvement.	Initial (empty) recording system for improvements

CSI: Inputs & outputs

Inputs

Identified nonconformities as well as deficiencies in effectiveness and efficiency of ITSM processes, and resulting opportunities for improvement

Identified deficiencies in the performance of services or supporting service components, and resulting opportunities for improvement

Outputs

Requests for changes raised to trigger the change management process, in order to implement improvements

Reports on the status and progress of improvements

CSI: Ongoing process activities

- Manage improvements
  - Identify and record an opportunity / suggestion for improvement
  - Prioritize an opportunity / suggestion for improvement
  - Evaluate and approve an opportunity / suggestion for improvement
- Review the status and progress of improvements

CSI: Roles

Role	Tasks	Ca. number of persons performing this role
Process owner CSI	*Generic tasks of a process owner applied in the context of CSI*	1 in total
Process manager CSI	*Generic tasks of a process manager, plus:* • Review the status and progress of ongoing improvements in regular intervals	1 in total
Improvement owner	• Maintain the improvement under his/her ownership • Coordinate the activities to implement the improvement	1 per improvement

CSI: Critical success factors & KPIs

Critical success factors	Key performance indicators (KPIs)
All suggestions for improvements are recorded.	• Number of registered improvements (vs. numbers from past periods)
Every suggestion for improvement is taken serious, evaluated, and feedback is provided to the originator.	• Percentage of improvements with a positive / negative evaluation result • Percentage of improvements for which a reasonable feedback was provided to the originator • Percentage of successfully implemented improvements

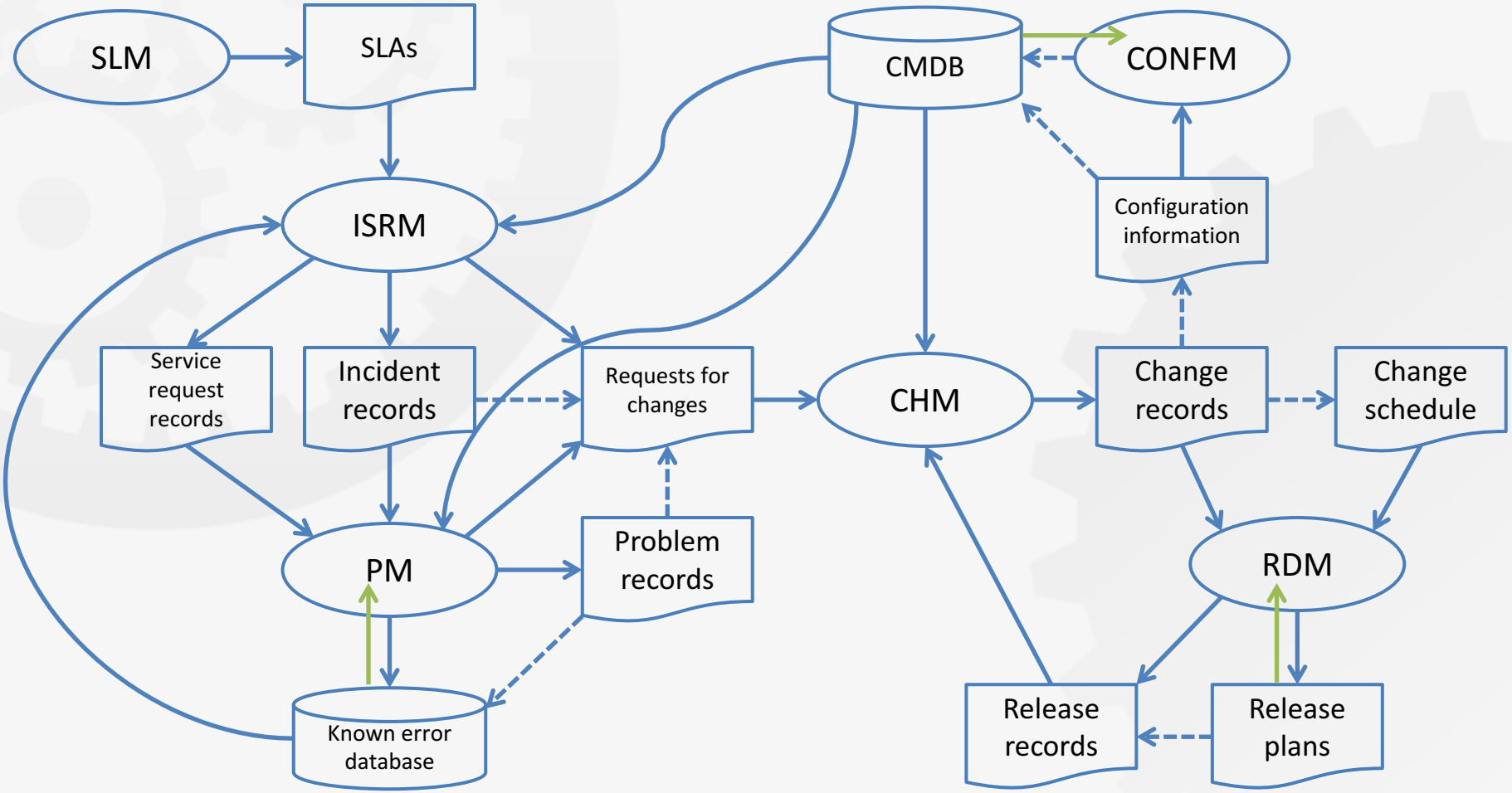
Agenda of this training

- FitSM Foundation wrap-up & ITSM basics
- Selected general aspects of establishing a service management system (SMS)
- ITSM processes for the operation and control of services
- **ITSM process interfaces and dependencies**

Standards for lightweight
IT service management

ITSM Process Interfaces & Dependencies

Service Operation & Control: Overview of key process interfaces

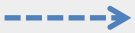


Explanations

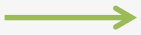
ITSM process, i.e. one of the service planning & delivery processes introduced earlier

Process artefact, i.e. input to or output to / from an ITSM process

[artefact] is input to [ITSM process] / [artefact] is output from [ITSM process]



[artefact] is a basis for / used for / aligned with / referenced from [artefact]



[output] is at the same time input to [ITSM process] (relevant for “closed-loop” processes) – i.e. the output is maintained by its “producing” ITSM process and requires regular reviews / updates

Info

slide in this deck (v2.5)	what has changed compard to v2.4?	comments
23 (federation models)	slight update with examples and minor text adjustments	copied over from latest interim Foundation slides (v2.10b)
45 (SMS manager role)	new slide	
72, 73 (ISRM roles)	process owner added, case owner more explicit (+ 1 slide)	
84, 85 (PM roles)	process owner added, case owner more explicit (+ 1 slide)	
Other slides about roles	process owner added	