Standards for lightweight IT service management

FitSM Expert

Expert training in IT service management according to FitSM

Version 1.5

Purpose of this training

- Become familiar with …
  - ITSM-related frameworks and standards;
  - understanding the organisational context of delivering and managing services;
  - leadership and governance;
  - planning and implementing ITSM;
  - monitoring, reviewing and improving ITSM.
- Achieve the *Expert level certificate in IT service management according to FitSM* issued by a registered Examination Institute

FitSM Expert exam

- At the end of this training
- Closed book, i.e. no aids are allowed
- Duration: 75 minutes
- 40 multiple choice questions:
  - Test knowledge and application of knowledge to typical service management szenarios
  - Four possible answers for each question: A, B, C and D
  - One correct answer per question
- At least 75% correct answers (30 out of 40) required to pass the examination

FitSM qualification program

Expert Level

Expert training in IT service management

2 days

Advanced Level

2 days

Advanced training in service planning and delivery

2 days

Advanced training in service operation and control

Foundation Level

Foundation training in IT service management

1 day

Agenda of this training

- FitSM Foundation & Advanced wrap-up
- ITSM-related frameworks and standards
- Understanding the organisational context of managing and delivering services
- Leadership and governance
- Planning and implementing services and ITSM (PLAN, DO)
- Monitoring, reviewing and improving services and ITSM (CHECK, ACT)

FitSM Foundation & Advanced Wrap-Up

What is a service?

Definition following FitSM-0:
Service: Way to provide *value* to *customers* through bringing about results that they want to achieve

Definition following FitSM-0:
IT service: *Service* that is enabled by the use of information technology (IT)

Function ➕ **Quality** ＝ **Value**

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):
> 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 *management system* that controls and supports management of *services* within an organisation or federation

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

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 activities that people carry out according to defined procedures.

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 consists of a number of activities used to manage services, if the process is part of a service management system (SMS).

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 group to perform one or more *activities* of a *process*

What is a process?
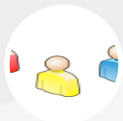
- ## How to define a process:

 Goal(s), objectives

 Clearly defined inputs, triggers and outputs

 Set of interrelated activities

 Roles and responsibilities

Definition following FitSM-0:

Role:
    Set of responsibilities and connected behaviours or actions collected into a logical unit that can be assigned to an individual or group

Agenda of this training

- FitSM Foundation & Advanced wrap-up
- ➢ **ITSM-related frameworks and standards**
- Understanding the organisational context of managing and delivering services
- Leadership and governance
- Planning and implementing services and ITSM (PLAN, DO)
- Monitoring, reviewing and improving services and ITSM (CHECK, ACT)

ITSM-related frameworks and standards

Overview

ISO 9000

ISO/IEC 27000 ←→ ISO/IEC 20000

ITIL → FitSM
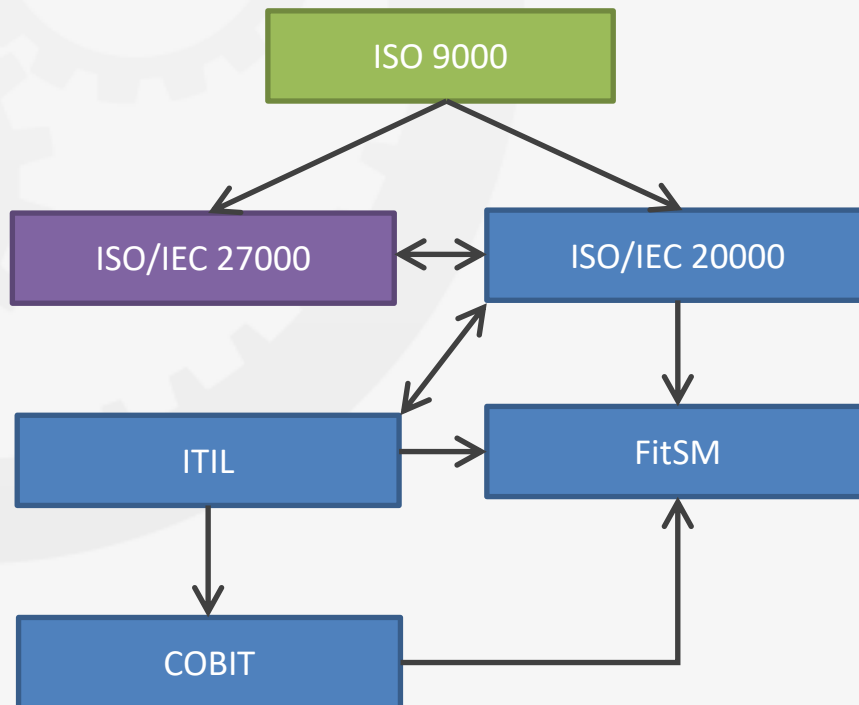
COBIT

Legend

IT (service) management standard / framework

Quality management standard

Information security management standard

adoption of concepts

FitSM, ITIL, COBIT

FitSM • Family of standards for lightweight IT service management • Design principle: Keep it simple! • Provides a glossary of terms, requirements, activities, roles and a capability / maturity assessment tool	• Several parts / core documents, plus ITSM templates and samples • Developed as part of an initiative funded by the European Commission
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	• Popular and wide-spread framework • 5 core books (ITIL V3), one for each phase in a "service lifecycle")
Control Objectives for Information and Related Technologies • IT Governance framework • Specifies control objectives, metrics, maturity models	• Developed by ISACA • Can be combined with ITIL, ISO/IEC 20000 and FitSM

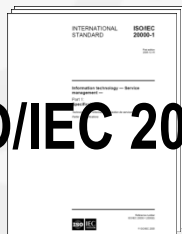# ISO 9000, ISO/IEC 20000, ISO/IEC 27000

FitSM

ISO 9000	**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 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
ISO/IEC 27000	**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 • Based on BS 7799 • Auditable, certifiable • Several documents

FitSM

Standards for lightweight IT service management

Keywords

Family of standards for lightweight ITSM; all parts freely available; main design principle: keep it simple; focus on core ITSM processes; applicable to federated service provisioning scenarios

FitSM: Overview and key facts

- **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

FitSM-0
Overview & vocabulary

FitSM-1
Requirements

FitSM-2
Objectives and activities

FitSM-3
Role model

Implementation aids

FitSM-4
Selected templates and samples

FitSM-5
Selected implementation guides

FitSM-6
Maturity and capability assessment scheme

FitSM: Logic

What do we need to achieve?

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

How can we put it in practice?

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

How can we organize it?

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

How did we perform?

FitSM-6: Maturity and capability assessment scheme

FitSM: Process model

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)

FitSM: A possible process grouping

Six main topic areas:

Offer & Agree	Plan & Ensure	Control & Deploy	Resolve & Prevent	Report & Improve	Protect & Secure
• SPM	• SUPPM	• CONFM	• ISRM	• SRM	• ISM
• SLM	• SACM	• CHM	• PM	• CSI	
• CRM	• CAPM	• RDM			

Standards for lightweight IT service management

ITIL

Keywords

Collection of books; good practices for ITSM; service lifecycle-based approach – 5 phases: service strategy, service design, service transition, service operation, continual service improvement

ITIL: Overview and key facts

- **A number of books with "good practices" for IT service management (ITSM)**
- Slogan: "the key to managing IT services"
- Descriptions of ITSM processes and supporting concepts
- Form of publication: books

ITIL: Structure

- Five lifecycle phases (for each stage: one identically named core publication):
  - Service strategy
  - Service design
  - Service transition
  - Service operation
  - Continual service improvement
- Process model consisting of 26 ITSM processes and 4 'functions'
(ITIL V3 / 2011)

ITIL V3 / 2011: Process model

FitSM

Service Strategy

Strategy management for IT Services

Service portfolio management

Financial management for IT services

Demand management

Business relationship management

Service Design

Design coordination

Service catalogue management

Service-level management

Availability management

Capacity management

IT service continuity management

Security management

Supplier management

Service Transition

Transition planning and support

Change management

Service asset and configuration management

Release and deployment management

Service validation and testing

Change evaluation

Knowledge management

Service Operation

Event Management

Access Management

Request Fulfilment

Problem Management

Incident Management

Service Desk (Function)

Technical Management (Function)

Application Management (Function)

IT Operations Management (Function)

Continual Service Improvement

The 7-Step Improvement Process

Service Reporting

COBIT

Framework for governing and managing enterprise IT

COBIT: Overview and key facts

- **Framework for governing and managing enterprise IT**
- Developed and published by ISACA (Information Systems Audit and Control Association)
- Several documents, including "Enabling Processes" based on a process reference model of 37 governance and management processes in 5 groups (COBIT 5)
- Form of publication: digital documents (PDF), free to members

COBIT 5: Key principles

Meeting Stakeholder Needs

Covering the Enterprise End-to-End

Applying a Single Integrated Framework

Enabling a Holistic Approach

Separating Governance and Management
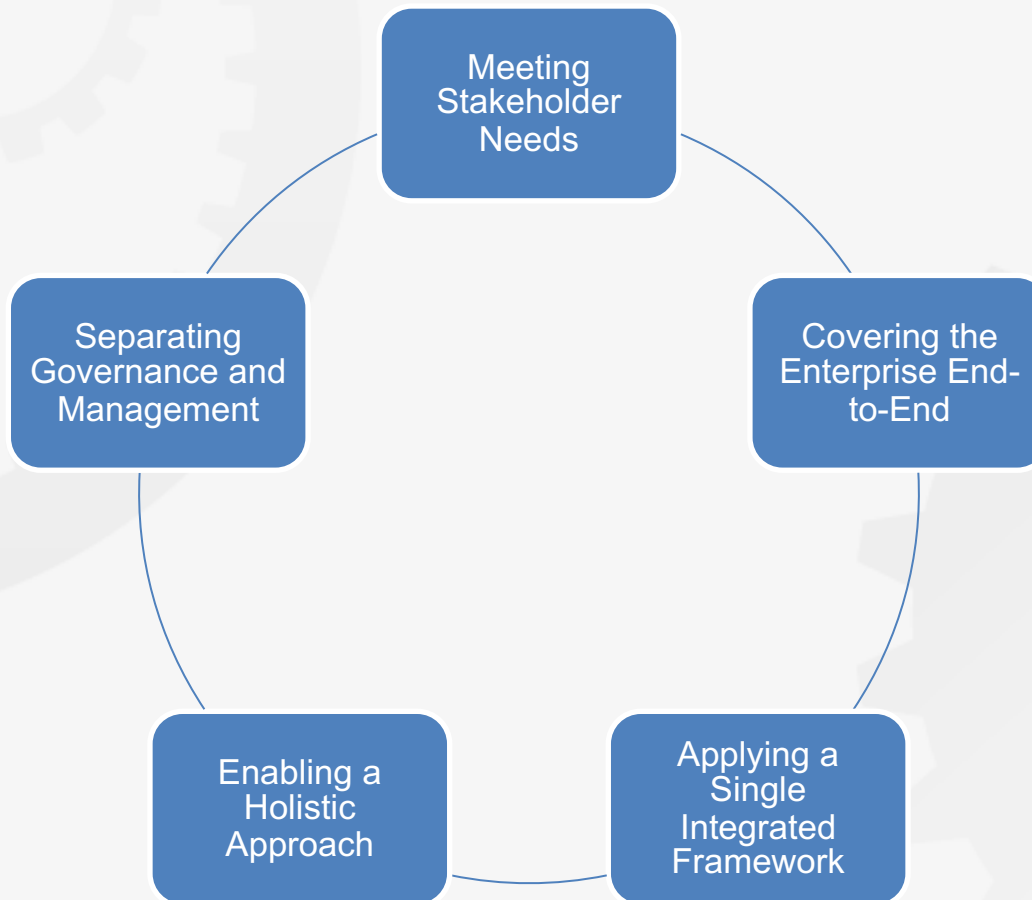
COBIT: Governance vs. management

Definition following COBIT:

Governance:

Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Definition following COBIT:

Management:

Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

Note: This definition refers to "management" as a discipline, not as a function, person or group of persons.

COBIT 5: Goals cascade to meet stakeholder needs

Stakeholder drivers

Stakeholder needs

Enterprise goals

IT-related goals

Enabler goals

COBIT 5: Enabler

Definition following COBIT:

Enabler:
Enablers are factors that influence whether something works or not. Enablers are driven by the goals cascade, which means that IT-related goals define what the different enablers should achieve.

- Typical enabler categories:
  - Principles and policies
  - Processes
  - Organisational structures
  - Culture and behaviour
  - Information
  - Services, infrastructure and applications
  - People, skills and competencies

COBIT 5: Process reference model

Evaluate, direct and monitor

- Ensure governance framework setting and maintenance
- Ensure benefits delivery
- Ensure risk optimisation
- Ensure resource optimisation
- Ensure stakeholder transparency

Align, plan and organise

- Manage the IT management framework
- Manage strategy
- Manage enterprise architecture
- Manage innovation
- Manage portfolio
- Manage budget and costs
- Manage human resources
- Manage relationships
- Manage service agreements
- Manage suppliers
- Manage quality
- Manage risks
- Manage security

Build, acquire and implement

- Manage programme and projects
- Manage requirements definition
- Manage solutions identification and build
- Manage availability and capacity
- Manage organisational change enablement
- Manage changes
- Manage change acceptance and transitioning
- Manage knowledge
- Manage assets
- Manage configuration

Deliver, service and support

- Manage operations
- Manage service requests and incidents
- Manage problems
- Manage continuity
- Manage security services
- Manage business process controls

Monitor, evaluate and assess

- Monitor, evaluate and assess performance and conformance
- Monitor, evaluate and assess the system of internal control
- Monitor, evaluate and assess compliance with external requirements

ISO 9000

Keywords

Requirements for quality management systems, quality management principles

ISO 9000: Overview and key facts

- **International standard for quality management**
- Subject: Development of a quality management system
- Editor: ISO (International Organization for Standardization)
- Application domain / recipients:
  - Manufacturing industry and service providers
  - Every form of industry and organisation
- Form of publication: Print, digital documents (PDF)
- Several parts:
  - ISO 9000: Overview and vocabulary
  - ISO 9001 (normative): Requirements for quality management systems
  - ISO 9004: Managing for the sustained success of an organisation
  - ISO 19011: Guidelines for auditing management systems (covered in later section on auditing)

ISO 9000:
Quality management principles

Process approach

- Consistent and predictable results are achieved more effectively and efficiently when activities are understood and managed as interrelated processes that function as a coherent system

Customer focus

- The primary focus of quality management is to meet customer requirements and to strive to exceed customer expectations.

Leadership

- Leaders at all levels establish unity of purpose and direction and create conditions in which people are engaged in achieving the organization's quality objectives.

Engagement of people

- Competent, empowered and engaged people at all levels throughout the organization are essential to enhance its capability to create and deliver value.

ISO 9000: Quality management principles (2)

Improvement

- Successful organizations have an ongoing focus on improvement.

Evidence-based decision making

- Decisions based on the analysis and evaluation of data and information are more likely to produce desired results.

Relationship management

- For sustained success, an organization manages its relationships with interested parties, such as suppliers.

See https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100080.pdf

ISO 9001: High Level Structure

FitSM

1 Scope

2 Normative references

3 Terms and definitions

4 Context of the organization

5 Leadership

6 Planning

7 Support

8 Operation

9 Performance evaluation

10 Improvement

- Common structure of all ISO and ISO/IEC management system standards published or updated since 2013
- Identical names for clauses, similar names for sub-clauses across all standards
- Use of common terminology and shared definitions of key terms

ISO/IEC 20000

Keywords

Requirements and guidance on the implementation of service management systems

ISO/IEC 20000: Overview and key facts

- **International standard for IT service management**
- Subject: Development of a service management system (SMS)
- Editor: ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission)
- Application domain / recipients: Internal and external IT service providers
- Form of publication: Print, digital documents (PDF)
- Several parts:
  - ISO/IEC 20000-1 (normative): Requirements
  - ISO/IEC 20000-2: Guidance on the application of service management systems
  - ISO/IEC 20000-3: Guidance on scope definition and applicability
  - ISO/IEC 20000-4: Process reference model
  - ISO/IEC 20000-5: Exemplar implementation plan

ISO/IEC 20000-1: Overview

- Normative part of the standard
  - Contains auditable requirements for a service management system (SMS)
  - Follows ISO high level structure
  - Most service management specific requirements in clause 8 (Operation)
- ITSM process requirements in sub-clauses 8.2 to 8.7
  - Service portfolio
  - Relationship and agreement
  - Supply and demand
  - Service design, build and transition
  - Resolution and fulfilment
  - Service assurance
- 20 sub-sub-clauses (to 8.2 through 8.7)
  - E.g. "8.2.2 Service catalogue management" is part of "8.2 Service Portfolio"
  - Fulfillment of each sub-sub-clause's requirements is, in most cases, best achieved by implementing one corresponding service management process.

ISO 20000-1:
ITSM process topics (8.2 to 8.4)

Service portfolio

Plan the services

Service catalogue management

Asset management

Configuration management

Service Delivery

Relationship and agreement

Business relationship management

Service level management

Supplier management

Supply and demand

Budgeting and accounting for services

Demand management

Capacity management

Note:
ISO/IEC 20000-1 does not explicitly speak of processes here.
In most cases, meeting the requirements of the individual sub-subclauses can best be achieved by implementing a corresponding service management process.
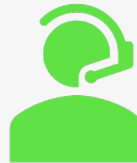However, there is no mandatory process model. It is permissible to establish more or fewer processes or to scope the processes differently, as long as all requirements are fulfilled.

ISO 20000-1:
ITSM process topics (8.5 to 8.7)

Service design, build and transition

Change management
Service design and transition
Release and deployment management

Resolution and fulfilment

Incident management
Service request management
Problem management

Service assurance

Service availability management
Service continuity management
Information security management

Standards for lightweight IT service management
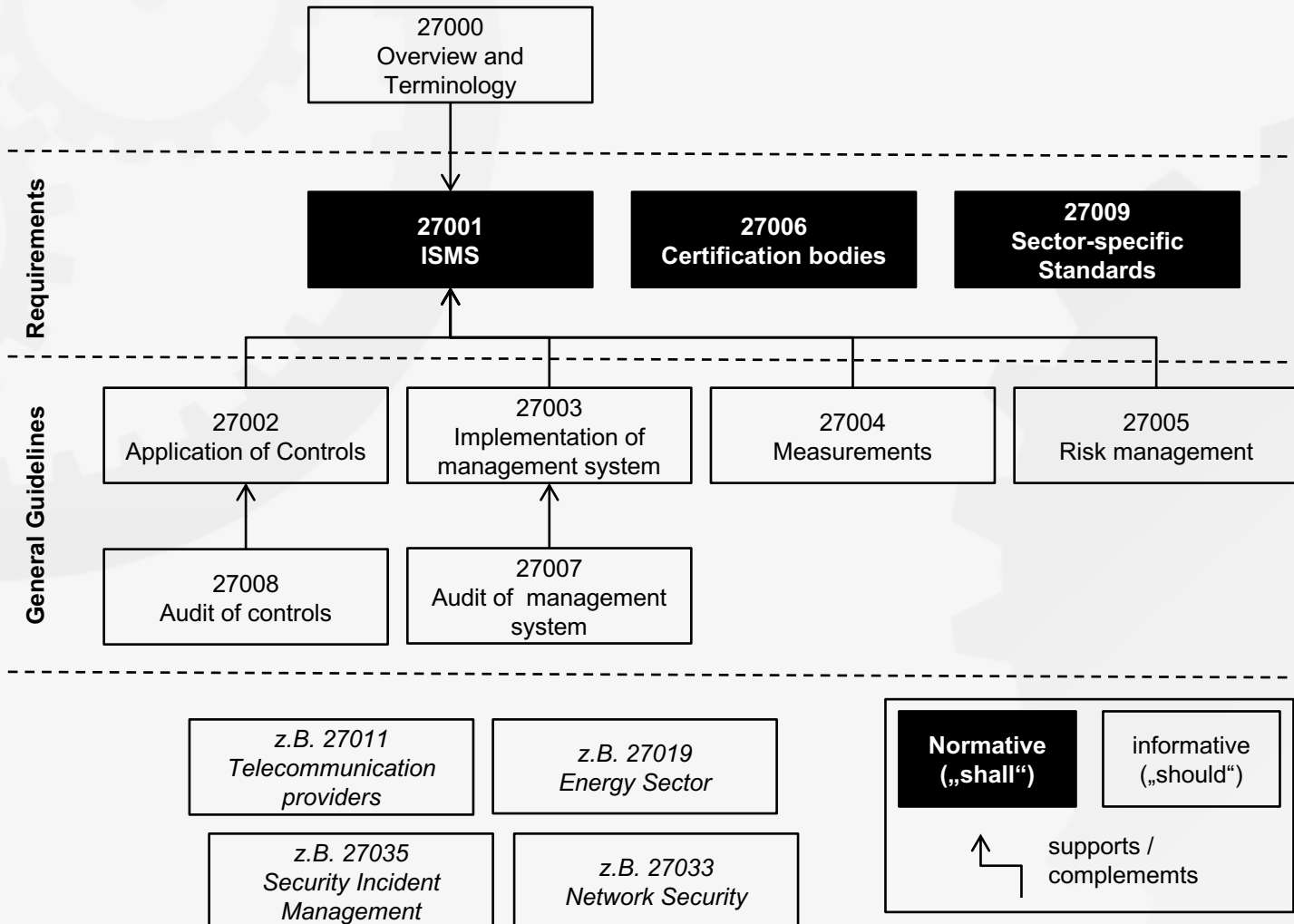
ISO/IEC 27000

Keywords

Requirements and guidance on the implementation of information security management systems

ISO/IEC 27000: Overview and key facts

- **International standard for information security management**
- Subject: Development of an information security management system (ISMS)
- Editor: ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission)
- Application domain / recipients:
  - Manufacturing industry and service providers
  - Every form of industry and organisation
- Form of publication: Print, digital documents (PDF)
- Several parts (see next slide)

ISO/IEC 27000:
The family of ISMS standards

FitSM

Requirements

27000 Overview and Terminology

**27001
ISMS** | **27006
Certification bodies** | **27009
Sector-specific Standards**

General Guidelines

| 27002
Application of Controls | 27003
Implementation of management system | 27004
Measurements | 27005
Risk management |

| 27008
Audit of controls | 27007
Audit of management system |

| *z.B. 27011*
Telecommunication providers | *z.B. 27019*
Energy Sector |
| *z.B. 27035*
Security Incident Management | *z.B. 27033*
Network Security |

Normative („shall") | informative („should")

supports / complememts

48

ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001
- Requirements for an ISMS
- Specification of reference control objectives and controls (Annex A)

ISO/IEC 27002
- Guidance on the application of security controls
- Implementation guidelines on all reference controls

Agenda of this training

- FitSM Foundation & Advanced wrap-up
- ITSM-related frameworks and standards
- ➢ **Understanding the organisational context of managing and delivering services**
- Leadership and governance
- Planning and implementing services and ITSM (PLAN, DO)
- Monitoring, reviewing and improving services and ITSM (CHECK, ACT)

Understanding the organisational context of managing and delivering services

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 work.
- Important in a federated environment:
  - Understanding the needs of different types of federations with respect to (federation-wide) ITSM
  - Understanding the roles of the federation members (including the roles or "business models" of the federators involved)

Examples of types of federation

Invisible Coordination
- An invisible coordinator supports the federation and its members to be capable of providing services to customers.
- Customers, however, only see the different individual federation members, from which they receive their services.

Advisory
- Customers mainly see the individual federation members, from which they receive services.
- One organisation acts as an advisor visible to customers as well, helping them understand the federation and its offerings.

Matchmaking
- A matchmaker helps customers get the services they want and need by bringing customers and federation members together.
- Matchmaking means: connecting customer demand with offerings from one or more federation members.

One stop shop offering
- Customers mainly see the one stop shop where they place their demands in the expectation of getting the "right" services.
- However, customers realise / know that services are actually provided / delivered by a number of different federation members.

Full service integration
- The integrator represents the whole federation and acts as a logical single service provider for customers.
- Customers only see and realise the full service integrator, and are not aware of the individual members of the federation anymore.

Examples of types of federation

In looser federations:
Individual federation members are responsible for delivering services to their customers largely on their own
→ Few, if any, federation-wide ITSM processes

ITSM perspective

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
Advisory	Hotel guide, rating portal
Matchmaking	Travel agent, booking portal
One stop shop offering	Airline with code sharing
Full service integration	Virtual mobile phone operator

Defining the scope of service management

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

Agenda of this training

- FitSM Foundation & Advanced wrap-up
- ITSM-related frameworks and standards
- Understanding the organisational context of managing and delivering services
- ➤ **Leadership and governance**
- Planning and implementing services and ITSM (PLAN, DO)
- Monitoring, reviewing and improving services and ITSM (CHECK, ACT)

Leadership and governance

Leadership and governance: Overview

- Effective policies
- Effective communication
- Governing value-generation through IT services
- Governing risk in ITSM
- Other governance disciplines
  - Governing transparency in ITSM
  - Governing the use of resources for ITSM
  - Governing processes operated by third parties

Effective policies

Why?

Ensure that policies are effective in providing direction and enforced

The role of policies in an SMS

Policy

1. Abc def ghijk.
2. Abc def ghijk.
3. Abc def ghijk.
4. Abc def ghijk.

Governance level
Top management
Process owners

Process:

Inputs

Activities and roles

Outputs
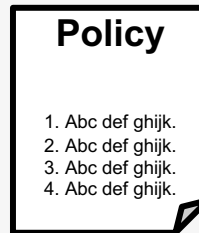
Control level
Process managers
Process teams
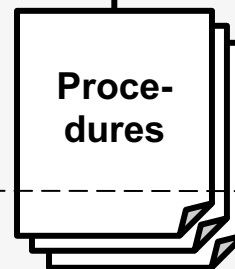
Person (in a role)

applies

Proce-dures
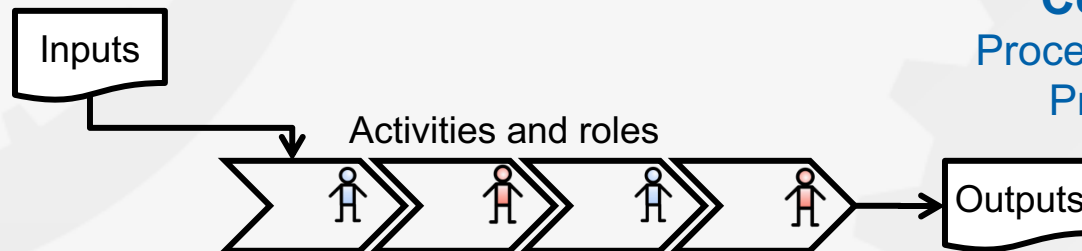
Operational level
Departments
Functions
Persons

61

Policies for ITSM

- **General policies, e.g.:**
  - Overall service management policy
  - Policy on continual improvement
  - …
- **Process-specific policies, e.g.:**
  - Configuration management policy
  - Change management policy
  - Release policy
  - Information security policies
  - …

Policies for ITSM

- Policies are one of the most important mechanisms for exerting governance (in an organisation / federation and over a management system).
- **The 5 Cs towards effective policies:**
    - Clear: Avoid too generic or ambiguous formulations!
    - Concise: Keep policies as brief as possible!
    - Consistent: Different policies must not contradict each other!
    - Communicated: Policies should be communicated effectively and to relevant target groups!
    - Committed: Those who approve and release policies (e.g. SMS owner, process owners) must be committed to their contents themselves, and enforce adherence to the policies!

Policy enforcement

- Create awareness
- Enable the organisation / federation and its people to act on the policy
  - Transfer of knowledge
  - Provision of resources
  - Motivation
- Monitor conformity
- Detect and follow-up on nonconformity
  - Reasons for nonconformity?
  - Decide on disciplinary measures

Policy enforcement: Exemplary disciplinary measures

	Unintentional, first time	Unintentional, repeated	Deliberately, first time	Deliberately, repeated
Minor nonconformity (low impact on effectiveness of ITSM)	Message / conversation	Message / conversation; consider topic-related training	Message / conversation; consider motivational measures	Written warning; consider: • motivational measures • re-assignment of responsibilities
Significant nonconformity (significant impact on effectiveness of ITSM)	Message / conversation, consider topic-related training	Message / conversation; consider: • topic-related training • written warning • re-assignment of responsibilities	Written warning; consider: • motivational measures • re-assignment of responsibilities	Written warning; consider: • motivational measures • re-assignment of responsibilities • Further action

Effective communication

Why?

Ensure that communication is well-planned and carried out, adequate means of communication are chosen and meetings are used effectively

Effective communication

- Create a communication plan for communicating one or more changes regarding the SMS
- Typical aspects to be considered in communication planning:
    1. Who informs?
    2. Who is informed?
    3. About what? (What is the message / content?)
    4. When and how often? (Timing, frequency)
    5. By which means? (Communication medium)
    6. How is the success of the communication measured?

Choosing adequate means of communication

- Examples of categories of communication media:
  - Mailing, memo
  - Meeting
  - Social event
- Examples of communication channels:
  - Broadcast communication (all)
  - Group communication (some)
  - Individual communication (exactly one)
- Examples of variations of acknowledgment:
  - No acknowledgment required
  - Acknowledged / approved, if no veto
  - Explicit acknowledgment / approval

Effective use of meetings

Good meetings …
- … are planned in advance
- … have a defined purpose and agenda
- … start on time
- … have all participants follow common ground rules (e.g. "cell-phones are turned off")
- … are moderated with respect for every participant, but also respect for the agenda and timing
- … end with the discussion follow-up actions ("Who will do what by when?")
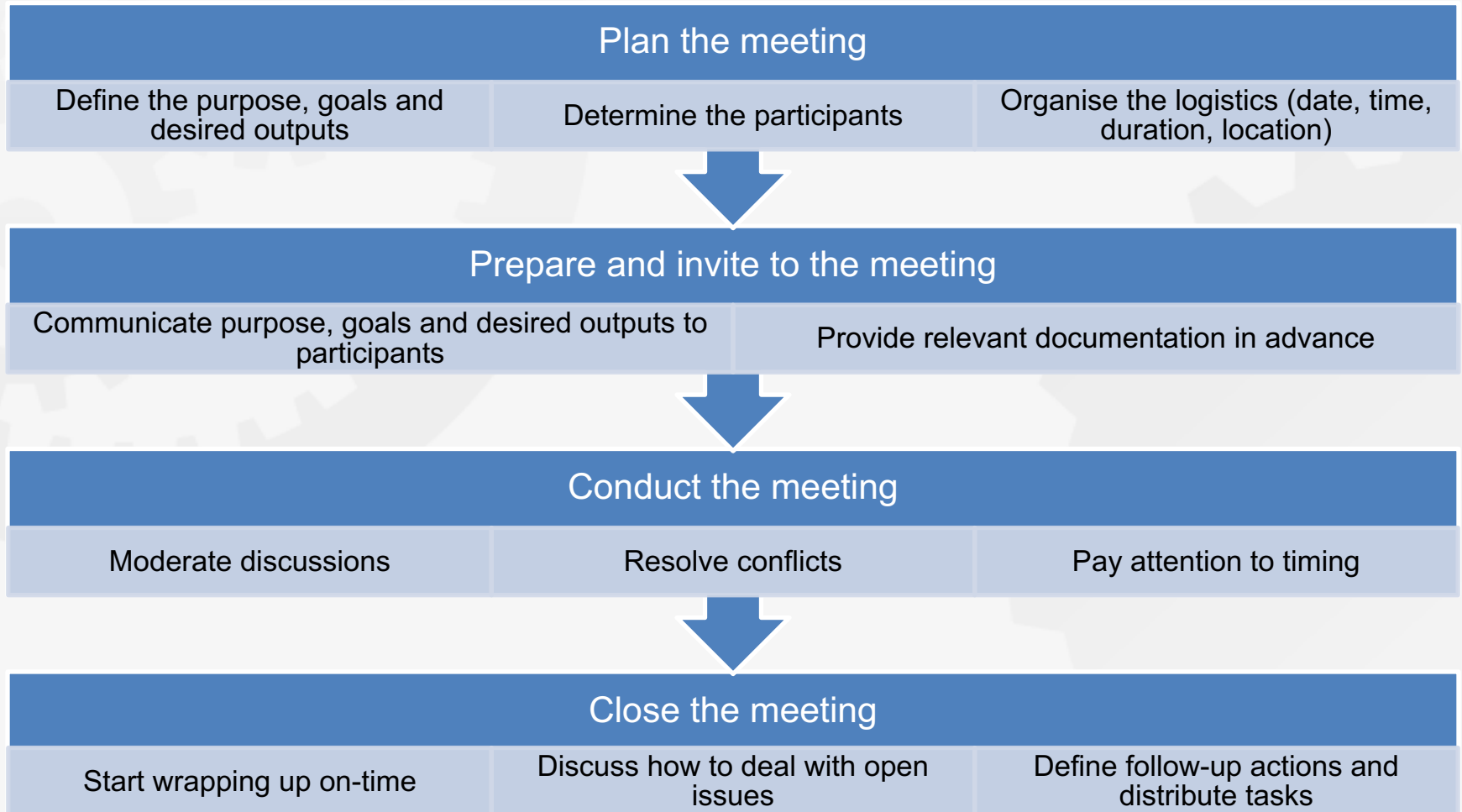- … end on time

Are you lonely?
Work on your own?
Hate to make decisions?
Rather talk about it than do it?

Then why not
HOLD A MEETING!

You can get to see
other people,
offload decisions,
feel important and
impress your colleagues.

MEETINGS
– the practical
alternative to work!

Effective use of meetings

Plan the meeting

| Define the purpose, goals and desired outputs | Determine the participants | Organise the logistics (date, time, duration, location) |

Prepare and invite to the meeting

| Communicate purpose, goals and desired outputs to participants | Provide relevant documentation in advance |

Conduct the meeting

| Moderate discussions | Resolve conflicts | Pay attention to timing |

Close the meeting

| Start wrapping up on-time | Discuss how to deal with open issues | Define follow-up actions and distribute tasks |

Governing value-generation through IT services

Why?

Ensure that IT services provided to customers are aligned to customers' needs and effectively support the customers' business

Service and value

FitSM

Definition following FitSM-0:

Service:

Way to provide *value* to *customers* through bringing about results that they want to achieve

Note: In the context of the FitSM standard series, when referring to services, usually IT services are meant.

Function **+** **Quality** **=** **Value**

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

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

Creating a business case for a service

FitSM

- A business case is a conceptual tool to support decision making, often used to justify a significant item of expenditure.
- General recommendations:
  - Create a business case for every service
    - Existing services (already in your portfolio)
    - New services (to be included in your portfolio)
    - Services undergoing major change
  - Keep it simple
  - When defining assumptions, identifying risks and calculating costs consider different scenarios / situations (including: best case, worst case)
- The business case for a service should help understand the value proposition of this service

Creating a business case for a service: Exemplary structure and contents

Part 1: The customer perspective	
Status quo / current situation (baseline)	*Describe the situation without the new or changed service, including potential pain points the service is intended to resolve or unexploited opportunities for the customer(s).*
Expected customer and user benefits / value proposition	*Describe how the new or changed service alleviates specific user pains and/or supports its intended customer(s) to exploit new opportunities.*

Part 2: The service provider perspective			
	Best case	Expected case	Worst case
Demand assessment			
Assumptions and constraints			
Expected organisational impact on the service provider			
Expected financial impact — Expenses			
Expected financial impact — Revenue			
Risks			

Creating a business case for a service: Financial impact

- Expenses: Consider the total cost of ownership, i.e.:
  - Direct and indirect costs for the service
  - Variable and fixed costs
  - Cost types and accounts
  - Apportioning of shared costs to the service
  - Costs through all service lifecycle phases (including design, development, operation and removal from operation)
- Returns: Consider any income, e.g. from …
  - Charging
  - Funding

Creating a business case for a service: Constraints (limiting factors)

- Legal requirements / constraints, including regulation
- Contractual requirements / constraints
- Policies
- Any other forms of compliance / conformity issues
- Monetary requirements / constraints
- People / staffing / competence requirements / constraints
- Any other resource constraints

Standards for lightweight
IT service management

Governing and managing risk in ITSM

Why?
Ensure that risks connected to planning, delivering, operating and controlling IT services are effectively identified, assessed and treated

Risk

Definition following FitSM-0:

Risk:

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

Hazard / Threat **+** Exposure / Vulner-ability **=** Risk

The level of a risk is usually assessed based on the probability and impact of the negative occurrence.
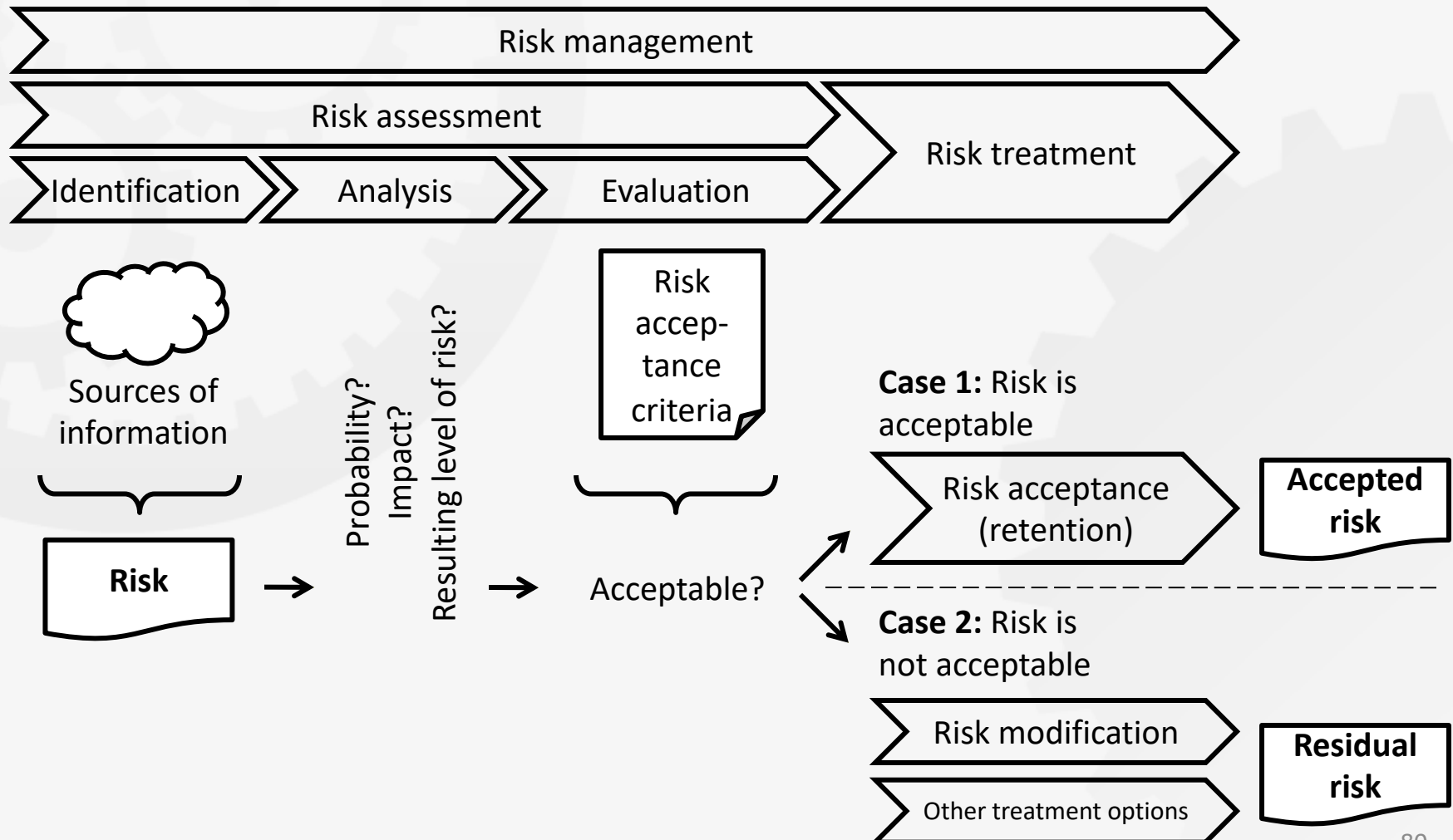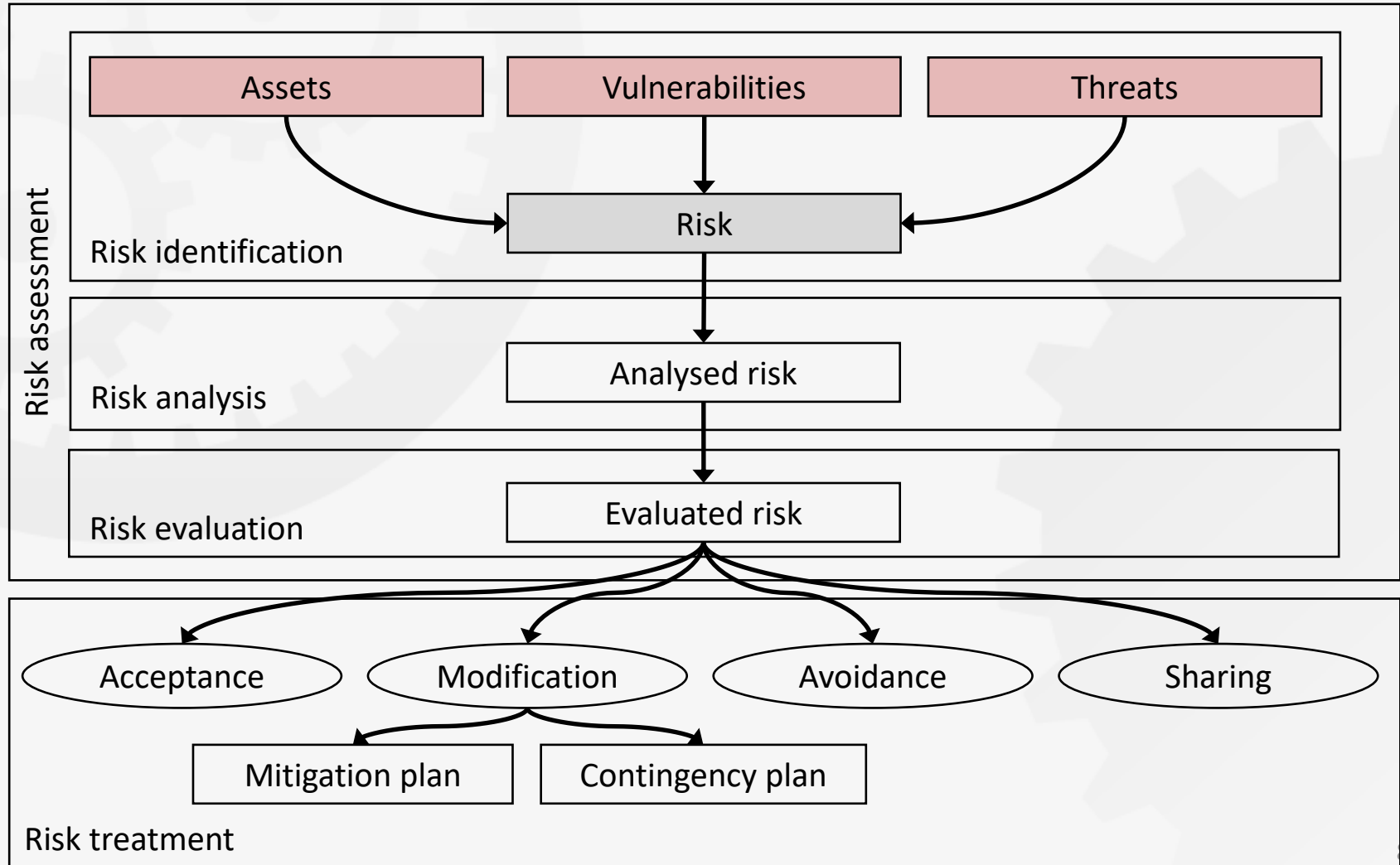
Governing risk in ITSM: Overview

- Main risk categories to be addressed by an SMS:
  - Risks connected to the availability and continuity of IT services
  - Risks connected to information security
- Risk governance vs. risk management:
  - Governing risk:
    - Defining criteria for risk analysis, evaluation and acceptance
    - Assigning risk owners
    - Sign-off of accepted (residual) risks
  - Managing risk:
    - Maintaining information on risk factors
    - Identifying, analysing and evaluating risks
    - Planning and implementing measures for risk treatment
    - Reviewing and monitoring risks and measures

Risk management: Main activities and outputs

Risk management: Steps and outputs

Risk assessment

Risk identification

Assets → Risk ← Threats
Vulnerabilities → Risk

Risk analysis

Risk → Analysed risk

Risk evaluation

Analysed risk → Evaluated risk

Risk treatment

Evaluated risk → Acceptance, Modification, Avoidance, Sharing

Modification → Mitigation plan, Contingency plan

Other governance disciplines

Why?

Ensure that IT service management is transparent, systematic and reproducible, the use of resources is optimized, and processes operated by other parties are under control

Governing transparency in ITSM

- Service management system with clear policies, processes and procedures
- Documentation and recording
- Effective reporting of all key activities, according to defined lines of reporting
- Identification of nonconformities through (internal) audits

Governing the optimal use of resources for ITSM

- Key resources in ITSM:
    - Human resources
    - Technology to support ITSM
    - External resources, such as required consultancy and auditing

Governing processes operated by third parties

- Third parties in this context:
  - External suppliers / partners
  - Customers
- Approach:
  - Identify the processes or parts of processes that are performed by third parties
  - Govern the third party in performing the process by …
    - demonstrating accountability for the process and authority to require adherence to it;
    - controlling the process definition and interfaces;
    - controlling improvements to the process;
   - monitoring process performance and compliance.

Agenda of this training

- FitSM Foundation & Advanced wrap-up
- ITSM-related frameworks and standards
- Understanding the organisational context of managing and delivering services
- Leadership and governance
- ➤ **Planning and implementing services and ITSM (PLAN, DO)**
- Monitoring, reviewing and improving services and ITSM (CHECK, ACT)

Planning and implementing ITSM
(PLAN, DO)
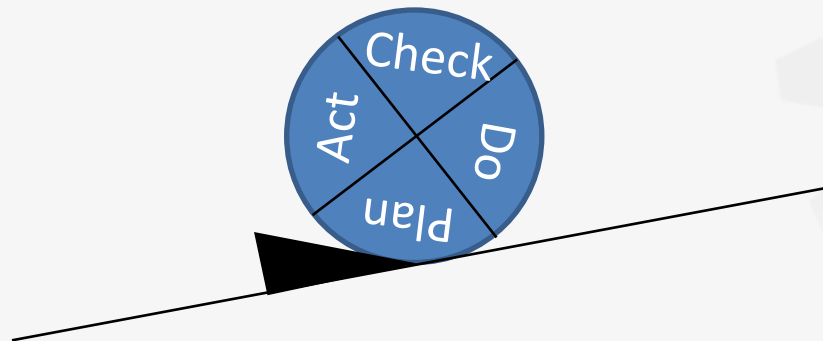
Planning and implementing ITSM: Overview

- Requirements according to FitSM-1
- Creating and maintaining a service management plan
- Defining and assigning roles and responsibilities
- ITSM training and awareness
- Managing organisational change
- Planning and implementing new or changed services

Planning and implementing 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.

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.

Creating and maintaining a service management plan

Keywords

Service management plan, goals

Service management plan

Definition following FitSM-0:
Service management plan: Overall plan for implementing and operating a *service management system (SMS)*

- **Possible general structure of a service management plan:**
  1. Status quo of the SMS (e.g. based on self-assessment, reviews, audits)
  2. Overall goals for the period covered by the plan, including:
     - Identification of focus areas / high-priority topics
     - Definition of milestones and timing for achieving goals
  3. Overview of current and future ITSM-related core roles and responsibilities
  4. Overview of planned ITSM-related training and awareness activities
  5. Overview of the current and future tool support for ITSM
  6. Overview of work packages and tasks
  7. References to other relevant plans (including task-specific plans)

Service management plan: Exemplary goals

- Extend the scope of the configuration management process all CIs supporting service components
- Apply the change management process to all CIs (including those new in the scope of configuration management)
- Conduct annual service reviews with all customers through the customer relationship management process
- Reduce the number of SLA violations by 30 per cent
- Harmonise the service specifications in the service portfolio (by applying a consistent specification template)
- Increase the number of internal SMS audits from 2 to 4
- Improve the documentation quality of known errors and workarounds in the known error database (KEDB) by establishing a four-eyes principle for new entries and monthly reviews of all entries
- …

![FitSM - Standards for lightweight IT service management]

Defining and assigning roles and responsibilities

Keywords

Generic and specific roles, allocation of responsibilities, RACI

Roles and responsibilities: Generic and specific roles

|	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 group in order to give this person or group the responsibility for something	Process manager for the incident and service request management process of an IT service provider	Flight captain for flight XX123 from Munich to Brussels

Generic roles
according to FitSM-3

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

Visualization of the role model
according to FitSM-3
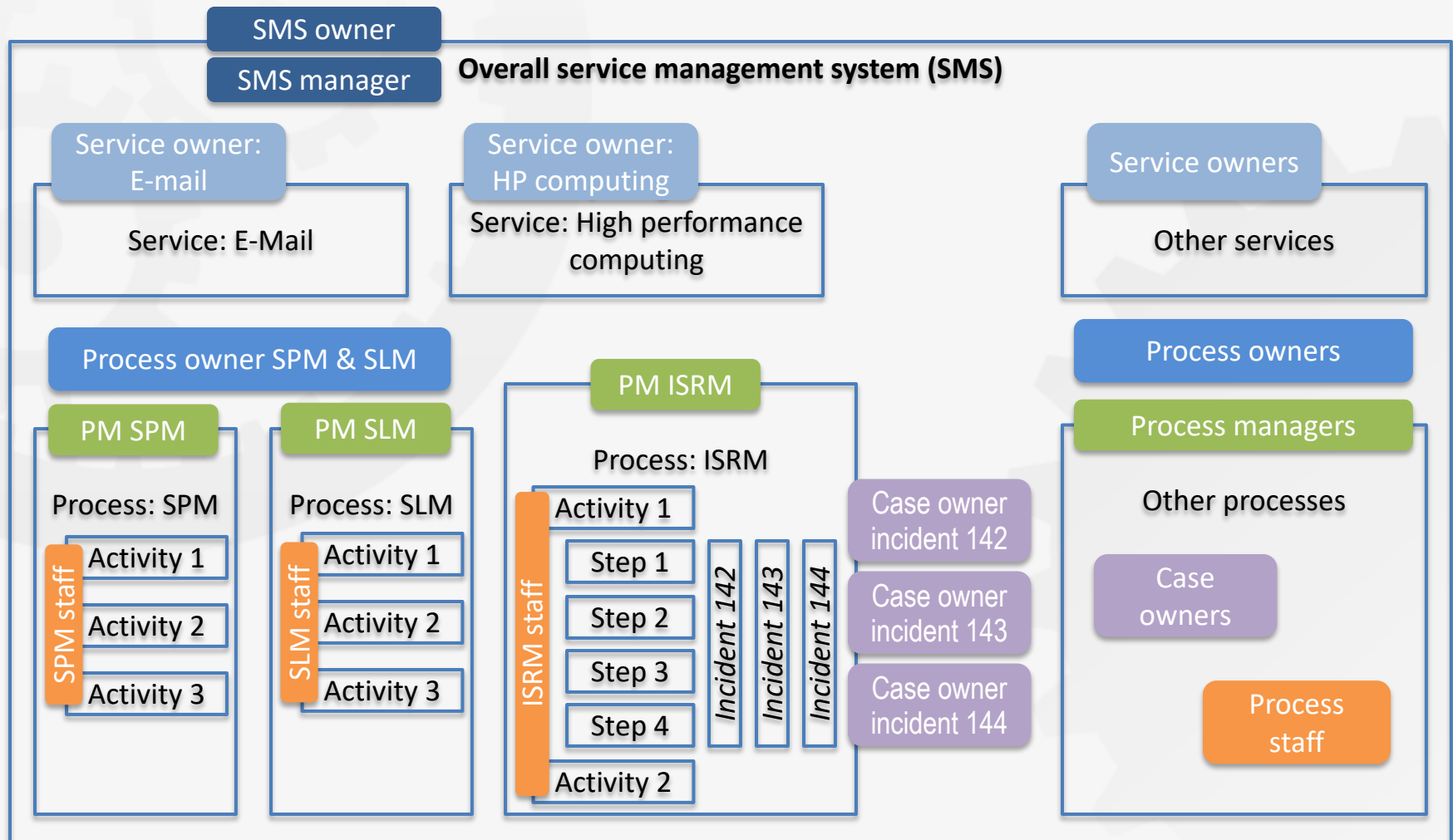
Planning and allocating responsibilities

- The RACI matrix is a tool to describe roles and responsibilities within a specific context in a simplified and easy to grasp manner.

	Role 1	Role 2	Role 3	…
Activity 1	A	R	I	
Activity 2	AI	C	R	
Activity 3	AC	R	C	
…				

RACI: Explanation

- The four letters R, A, C and I stand for the various generic forms of responsibility or participation:
    - Responsible: A person or role actually executing / performing / carrying out a process or activity
    - Accountable: The person or role governing a process or activity by defining and approving goals and providing or acquiring resources and capabilities required so that the process or activity can be carried out effectively
    - Consulted: A person or role whose expertise or other kind of contribution is needed to carry out a process or activity without this person being responsible for the process or activity him-/herself
    - Informed: A person or role who needs to be kept informed about the status and/or results of a process or activity

RACI: Rules

- Every row should contain exactly one "A".
  - The rationale behind this rule is that there should be clear accountability for every activity.
  - At the same time, it might lead to confusion and lack of individual commitment or enforceability, if two or more persons or roles are accountable at the same point in time.
- Every row should contain at least one "R".
  - There should be no activities for which the responsibilities of executing them are undefined.
- It should be avoided that the same person or role is accountable and responsible at the same time, i.e. for the same activity.

Potential carriers of responsibility in an organisation or federation

- Function: number of people, resources and tools supporting a process or an activity
- Department: part of the organizational hierarchy of a company/organization
- Group: people performing similar activities
- Team: formal group, directed towards the achievement of one or more defined objectives
- Role: logical concept that relates responsibilities, activities or behaviours to a person, a team, a group, or a function

ITSM training and awareness

Keywords

ITSM training and awareness program, role-based training, managing competencies

ITSM training and awareness

- Success factors of ITSM:
  - **People**
  - Processes
  - Technology
- Enable people by effective means of …
  - Awareness (Why?)
  - Role-based education and training (How?)
    - Technical skills
    - Personal skills / soft skills
    - Experience
- Manage competencies by …
  - setting up a training and awareness program (annual update, part of the service management plan);
  - maintaining chronological records on competence, education, training and experience.

Managing organisational change

Keywords

Emotional cycle of change, steps to successful organisational transformation, dos and don'ts of organisational change

Emotional cycle of change

Steps to organisational transformation
according to Kotter and Schlesinger

1. Create a sense of urgency
2. Establish a guiding coalition
3. Develop a vision and strategy
4. Communicate the vision
5. Empower people to act on the vision
6. Create quick-wins
7. Consolidate achievements and create more change
8. Institutionalize the organisational change in the organisation's culture

1. Create a sense of urgency

What to do (core challenge):
- Get people out of the bunker
- Create initial awareness and organisational readiness

What to achieve (desired behaviour / situation):
- People start talking about it and motivating each other

What to avoid (risks):
- No (clear) commitment from top management
- Lip services and smoke grenades

How to move it forward (recommended actions):
- Update policies and plans
- Start communicating

2. Establish a guiding coalition

What to do (core challenge):
- Get the right people in place
- Ensure they are committed to the change and respected by others

What to achieve (desired behaviour / situation):
- A powerful group influences others to accept the change
- Opposing to the change means being against the coalition

What to avoid (risks):
- Lack of trust and confidence in the coalition

How to move it forward (recommended actions):
- Identify skilled and respected individuals from major stakeholder groups

3. Develop a vision and strategy

What to do (core challenge):
- Get the guiding coalition to develop a clear vision and strategy
- As part of the strategy, address the people factor

What to achieve (desired behaviour / situation):
- A clear vision and strategy has been developed by the guiding team

What to avoid (risks):
- Only focus on numbers (finance) and technology
- Too much consultant speak, too little concrete orientation

How to move it forward (recommended actions):
- Set up a strategic plan taking into account the people, process and technology factors

4. Communicate the vision

What to do (core challenge):
- Address all relevant stakeholder groups and make them become a part of the organisational change

What to achieve (desired behaviour / situation):
- People start buying in to the change and behave accordingly

What to avoid (risks):
- Too little, too late communication
- Communication not well aligned to the needs of the audience

How to move it forward (recommended actions):
- Set up a communication plan, based on stakeholder identification
- Communicate according to the plan

5. Empower people to act on the vision

What to do (core challenge):
- Remove the obstacles that would stop people from acting towards the vision

What to achieve (desired behaviour / situation):
- More people feel able to act on the vision

What to avoid (risks):
- Too many (notorious) objection raisers left exerting influence on others

How to move it forward (recommended actions):
- Launch an awareness campaign, motivate people
- Provide professional training (role-based)

6. Create quick-wins

What to do (core challenge):
- Produce enough short-term achievements quickly enough to energize and motivate the change helpers, enlighten pessimists and build momentum

What to achieve (desired behaviour / situation):
- Momentum builds, while fewer people resist the organisational change
- Cynics and pessimists are defused

What to avoid (risks):
- Quick-wins, although they have been achieved, are not visible enough

How to move it forward (recommended actions):
- Prioritize tasks in support of quick-wins
- As soon as achievements have been realised, communicate broadly

7. Consolidate achievements and create more change

What to do (core challenge):
- Continue with the same energy and effort after first achievements have been made

What to achieve (desired behaviour / situation):
- People remain motivated and energized
- Further change is pushed forward towards the overall vision

What to avoid (risks):
- The momentum gets lost, people rest on their laurels
- Resources are taken away after high-priority quick-wins were achieved

How to move it forward (recommended actions):
- Keep up top management commitment and involvement
- Keep up planning and communicating

8. Institutionalize the organisational change

What to do (core challenge):
- Create effective supporting structures as the roots for new ways of operating

What to achieve (desired behaviour / situation):
- New behaviour continues

What to avoid (risks):
- Fall-back to "old traditions"

How to move it forward (recommended actions):
- Refresh awareness from time to time
- Monitor, evaluate and further improve on an ongoing basis

Dos and don'ts of organisational change

Do

- Understand the baseline and vision
- Communicate effectively
- Identify impacts
- Get stakeholders to participate in decision-making
- Put the right people in the right roles
- Provide easy access to relevant information

Don't

- Micro-manage everything
- Try to achieve consensus for every decision
- Only focus on technology
- Over-complicate things
- Pretend there are no risks / difficulties / losers
- Ignore after-effects of failed changes to people

Planning and implementing new or changed services

Keywords

Service design and transition package (SDTP), service acceptance criteria

Planning new or changed services: Requirements according to FitSM-1

PR1 Service Portfolio Management (SPM)
REQUIREMENTS
• (…)   • 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.   • (…)

- Important facts:
  - The design and transition of new or changed services is coordinated under the control of the service portfolio management process.
  - Plans for a new or changed service should be "bundled" into a service design and transition package (SDTP)

Planning new or changed services: Service design and transition package (SDTP)

Definition following FitSM-0:
Service design and transition package (SDTP):

Entirety of plans for the design and transition of a specific new or changed *service*

Note: An SDTP should be produced for every new or changed service. It may consist of a number of documented plans and other relevant information, available in different formats, including a list of requirements and service acceptance criteria (SAC), a project plan, communication and training plans, technical plans and specifications, resource plans, development and deployment schedules / timetables, etc.

- Relationships between the SDTP and a business case:
  - The SDTP may be based on the information from a business case for a new or changed service.
  - The business case should be referenced from the SDTP.

Possible structure of a service design and transition package (SDTP)

(Reference to) business case	*(see section "Creating a business case for a service")*
Service requirements	Functional requirements
	Usability-related requirements
	…
Service architecture	Enabling service components
	Enhancing service components
Service acceptance criteria (SAC)	Functional criteria
	Usability-related criteria
	…
Service transition plan(s)	Communication plan
	Development and deployment plan
	…

Why service requirements & service acceptance criteria?

- Create a common understanding between the service provider and customers / other stakeholders of expectations regarding the new / changed service
- Avoid conflicts between the service provider and customers / other stakeholders by clearly stating the conditions under which the new or changed service is deployed into the live environment.
- Create Basis for quality assurance during the design and transition phase

Typical categories of service requirements & service acceptance criteria

Category	Example
Functional	• The service supports the following use cases as specified: (…)
Technical	• The client runs on the following operating systems: (…)
Information security and data protection-related	• All data transmitted over public networks encrypted according to encryption standard (…)
Usability-related	• SSO supported, user experience guidelines fulfilled as specified: (…)
Organisational	• Support staff and users have been trained, (…)
Availability, continuity and performance-related	• Service continuity plans have been updated, load test performance meets service level target (…)

Agenda of this training

- FitSM Foundation & Advanced wrap-up
- ITSM-related frameworks and standards
- Understanding the organisational context of managing and delivering services
- Leadership and governance
- Planning and implementing services and ITSM (PLAN, DO)
- ➢ **Monitoring, reviewing and improving services and ITSM (CHECK, ACT)**

Monitoring, reviewing and improving ITSM (CHECK, ACT)
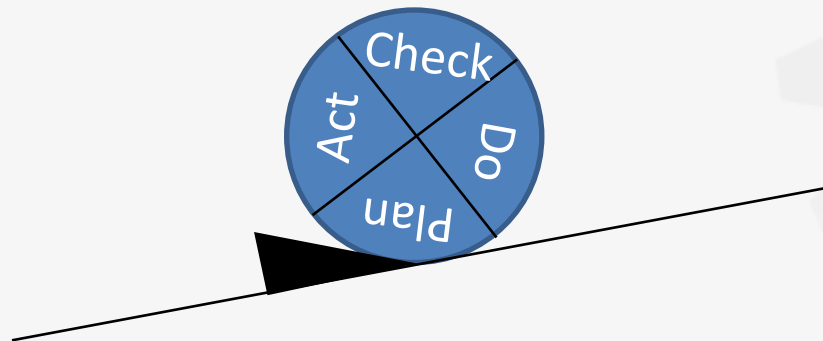
Monitoring, reviewing and improving ITSM: Overview

- Requirements according to FitSM-1
- Compliance, effectiveness and efficiency
- Key performance indicators
- Managing an audit programme and conducting audits
- Capability and maturity assessment

Planning and implementing 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.
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).

Conformity, effectiveness and efficiency

Keywords

Conformity / compliance, effectiveness and efficiency

Conformity, effectiveness and efficiency

- **Conformity (compliance):**
  - Question: Are requirements fulfilled and specifications met?
  - Examples for sources of requirements: legislation, policies, defined processes and procedures, …
- **Effectiveness:**
  - Question: Are intended goals / objectives achieved?
  - Examples of goals to be achieved: service level targets (from SLAs), operational targets (from OLAs), process goals, …
- **Efficiency:**
  - Question: Given the achieved level of effectiveness, is the level of consumption of resources appropriate?
  - Examples of resources: financial resources (money), human resources (manpower), technical resources (capacities), …

Example: Car wash

Conformity (compliance)

- Does the car match the allowed specifications of the car wash facilities?
- Does the car driver follow the instructions provided by the car wash company?
- Does the operator of the car wash facilities push the right buttons?

Effectiveness

- Has the car been cleaned and all soiling removed to a degree sufficient from the car owner's perspective?

Efficiency

- Given the achieved level of cleanliness, is the amount of water, chemicals, energy, manpower and time consumed appropriate?

Conformity, effectiveness and efficiency

Efficiency
- The consumption of financial, human and technical resources is being monitored, evaluated and optimized.
- Resource consumption is appropriate for the achieved level of effectiveness.

Effectiveness
- Goals connected to policies and processes are actually achieved.
- Services are provided according to agreed SLAs.

Conformity (compliance)
- Policies providing overall direction and rules are adhered to.
- Processes and procedures are carried out according to specifications in practice.

Compliance vs. conformity

- Sometimes, compliance and conformity are separated (see: COBIT):
  - **Conformity:** Adherence to internal regulations and requirements, such as they are defined by …
    - Policies
    - Processes
    - Procedures
  - **Compliance:** Adherence to external requirements, such as:
    - Laws
    - Standards
    - Contracts

Key performance indicators

Keywords

SMART measurements, critical success factors (CSFs) and key performance indicators (KPIs)

SMART measurements

Definition following FitSM-0:
Key performance indicator (KPI):
Metric that is used to track the performance, effectiveness or efficiency of a service or process

- SMART KPIs:
  - **S**pecific: targeting an area of improvement, indicative of the level achievement of of a *critical success factor*
  - **M**easurable: defined way measure and/or calculate the KPI
  - **A**chievable: target areas for KPIs are achievable
  - **R**elevant: matters, unexpected results warrant further investigation
  - **T**ime-framed: has defined measurement interval
- Critical success factors (CSFs): Limited number of factors, representing the key areas, where "things must go right", for overall goals to be attained

See: Bullen, C. V., & Rockart, J. F. – A primer on critical success factors

Example: CSF and KPI

Critical success factor for the process of incident and service request management (ISRM): Sufficient staffing so that incidents can be resolved within the allowed resolution time according to agreed SLAs.

?

Connected KPI: Percentage of incidents where the time to resolution exceeded the maximum allowed resolution time according to SLAs (i.e. one or more SLAs have been violated).

?

Example (continued)

Month	Value
Jan	20%
Feb	19%
Mar	19%
Apr	17%
May	16%
Jun	11%
Jul	8%
Aug	3%
Sep	4%
Oct	5%
Nov	5%
Dec	5%

KPI: Percentage of incidents where the time to resolution exceeded the maximum allowed resolution time according to SLAs (i.e. one or more SLAs have been violated).

Based on these numbers, what would be **valid conclusions?**

Managing an audit programme and conducting audits

Keywords

Audit-related terminology, principles of auditing, audit types, internal vs. external audits, managing an audit programme, conducting an audit

What is an audit?

An **audit** is a …

systematic, independent and documented process

for

obtaining audit evidence and evaluating it objectively

to

determine the extent to which the audit criteria are fulfilled.

Major points to be considered when preparing and conducting an audit:

– Systematic = clear audit plan
– Independent = auditor does not audit his/her own work
– Documented = defined process + records of audit activities performed

135

Principles of auditing

Integrity

Evidence-based approach

Fair presentation

Independence

Due professional care

Confidentiality
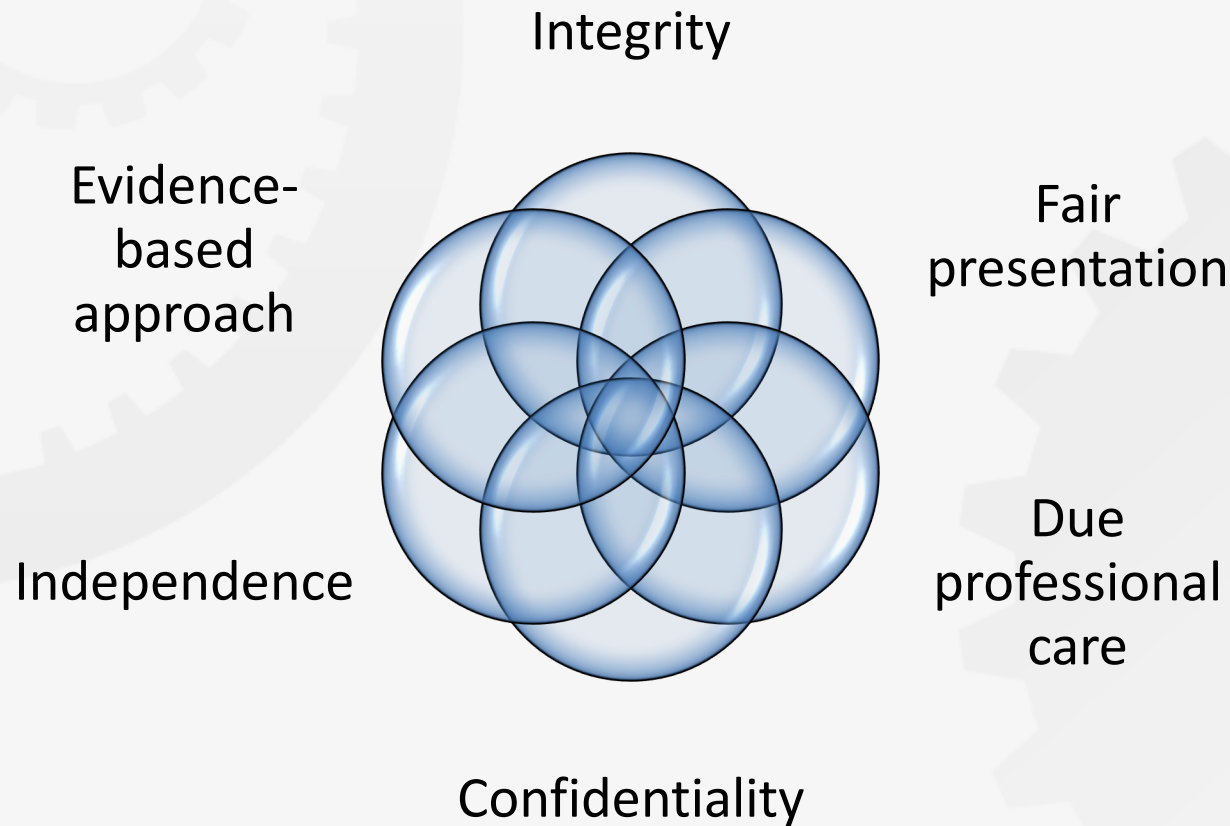
Audit types

- System audit
- Process audit
- Product audit

Internal and external audits

- Internal audit:
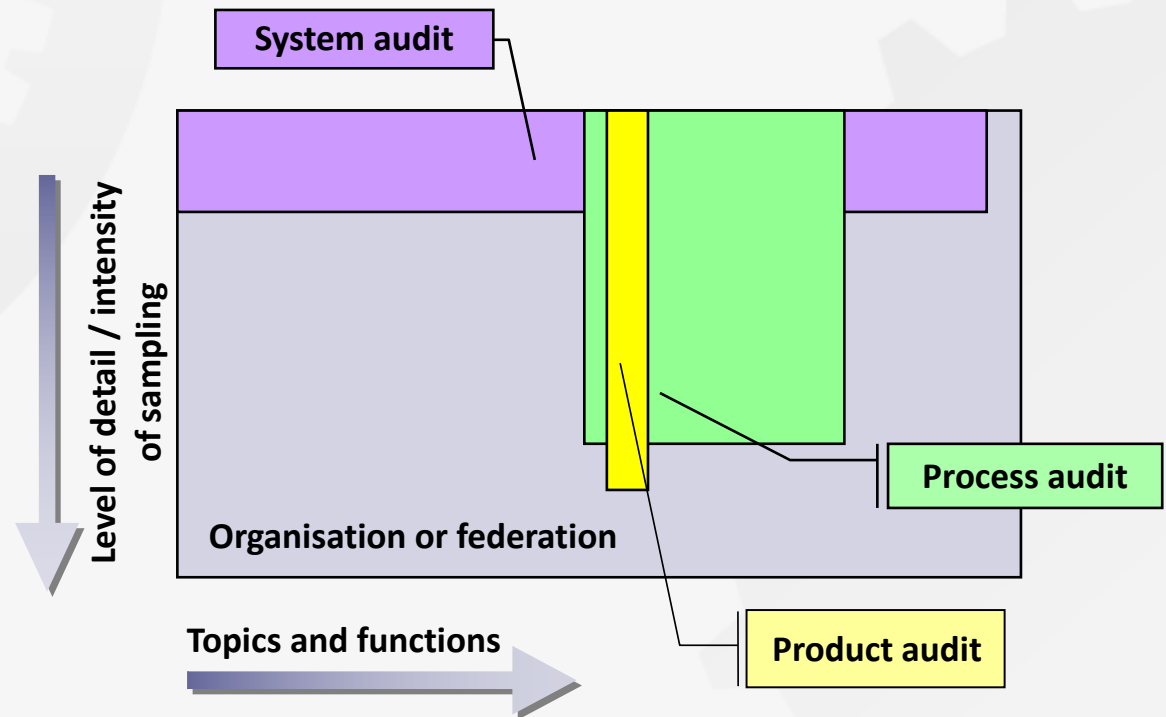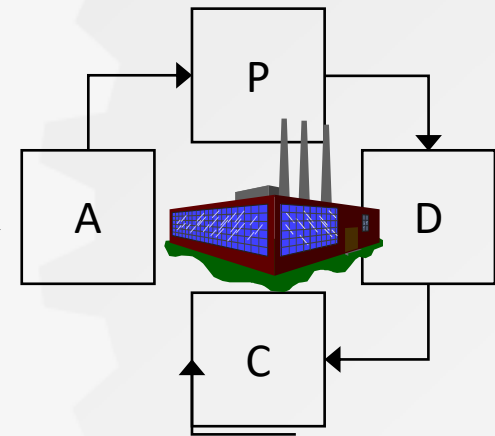 - Conducted under the direct responsibility and control of an organisation or federation within their own boundaries

- External audit:
  - Conducted under the responsibility and control of an external organisation
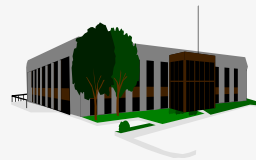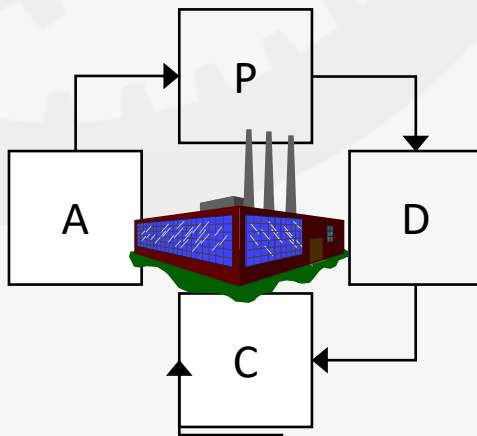
ISO 19011: Overview and key facts

- **Guidelines for auditing management systems**
- Subject: Principles and processes of managing an audit programme and conducting management systems audits
- Editor: ISO (International Organization for Standardization)
- Application domain / recipients: Any organisation operating and maintaining a management system (including quality management systems, environmental management systems, service management systems and information security management systems)
- Form of publication: Print, digital documents (PDF)

ISO 19011: Topics

- Topics addressed:
  - Terms and definitions
  - General audit principles
  - Managing an audit programme
  - Performing an audit
  - Competence and evaluation of auditors

Terms defined in ISO 19011

- Audit
- Audit criteria
- Audit evidence
- Audit findings
- Audit conclusion
- Audit client
- Auditee
- Auditor
- Audit team
- Technical expert
- Observer
- Guide
- Audit programme
- Audit scope
- Audit plan
- Risk
- Competence
- Conformity
- Nonconformity
- Management system

Managing an audit programme
according to ISO 19011

```
┌─────────────────────────────────────────────┐
│  Establishing the audit programme objectives │      (ISO 19011, section 5.2)
└─────────────────────────────────────────────┘
                    ↓
┌─────────────────────────────────────────────┐
│      Establishing the audit programme        │
│  •  Roles and responsibilities               │
│  •  Competence of the AP manager             │
│  •  Extent                                    │      (Section 5.3)
│  •  Risks                                     │
│  •  Procedures                                │
│  •  Resources                                 │
└─────────────────────────────────────────────┘
                    ↓
┌─────────────────────────────────────────────┐
│     Implementing the audit programme          │
│  •  Objectives, scope and criteria for        │
│     individual audits                         │
│  •  Audit methods                             │      (Section 5.4)
│  •  Audit team members                        │
│  •  Audit activities                          │
│  •  Records                                   │
└─────────────────────────────────────────────┘
                    ↓
┌─────────────────────────────────────────────┐
│        Monitoring the audit programme         │      (Section 5.5)
└─────────────────────────────────────────────┘
                    ↓
┌─────────────────────────────────────────────┐
│        Improving the audit programme          │      (Section 5.6)
└─────────────────────────────────────────────┘
```
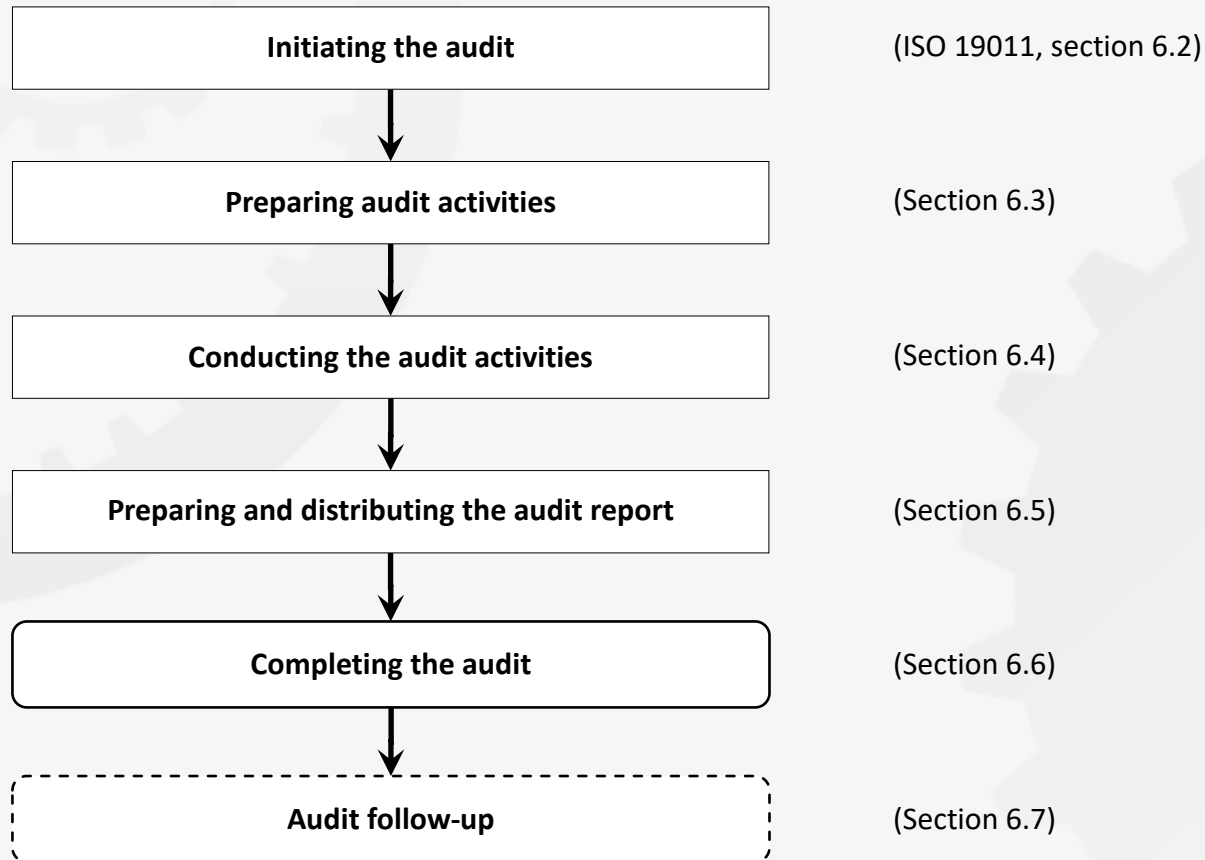
Performing an audit
according to ISO 19011

|	
Initiating the audit	(ISO 19011, section 6.2)
↓	
Preparing audit activities	(Section 6.3)
↓	
Conducting the audit activities	(Section 6.4)
↓	
Preparing and distributing the audit report	(Section 6.5)
↓	
Completing the audit	(Section 6.6)
↓	
Audit follow-up	(Section 6.7)

Initiating the audit

- Establish initial contact with the auditee
  - Contact may be formal or informal
  - Responsible: lead auditor (audit team member)
- Determine the feasibility of the audit
  - Sufficient and appropriate information for planning and conducting the audit?
  - Adequate cooperation from the auditee?
  - Sufficient time and resources?

Initiation

Preparation

Audit activities

Audit report

Completion

Follow-up actions
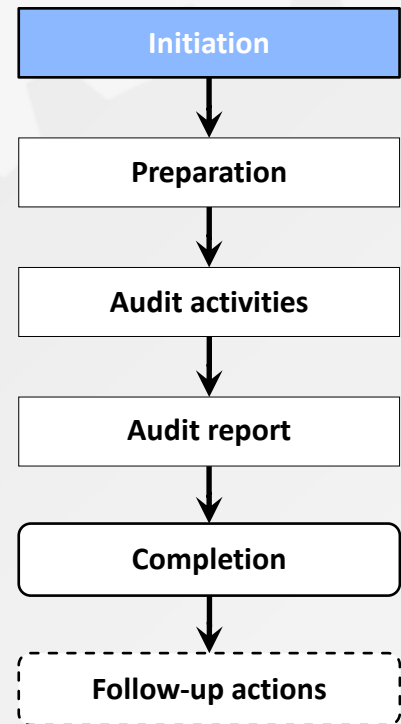
Preparing the audit activities

- Perform document review in preparation for the audit
  - Documentation of the management system (e.g. policies, process descriptions)
  - Records of activities performed
- Assign work to the audit team
  - Define and assign roles in the audit team
  - Consider the level of competence and experience of each auditor when assigning work
- Create an audit plan (see next slide)
- Prepare working documents

Initiation

Preparation

Audit activities

Audit report

Completion

Follow-up actions
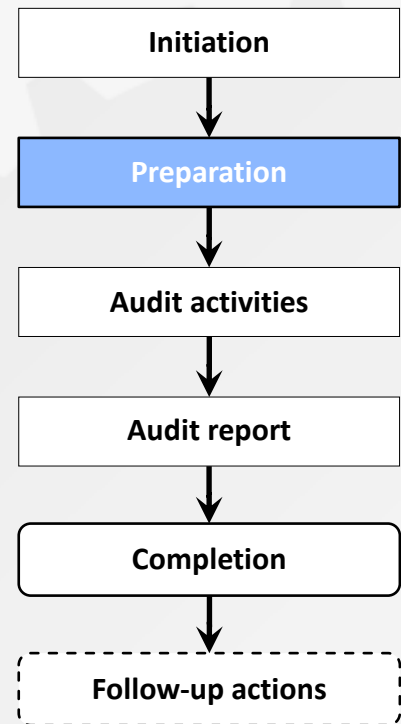
Preparing the audit activities

- Roles in an audit team:
  - (Lead) auditor
  - (Co-) auditor
  - Technical expert (person who provides specific knowledge or expertise to the audit team)

Initiation

Preparation

Audit activities

Audit report

Completion

Follow-up actions

Preparing the audit activities

- Typical contents of an audit plan:
  - Audit objectives
  - Audit scope
  - Audit criteria
  - Logistics (locations, dates, times) of audit activities
  - Audit methods to be used
  - Roles and responsibilities of the audit team members
- Examples of working documents:
  - Checklists
  - Forms to record audit evidence (including minutes of interviews) and findings

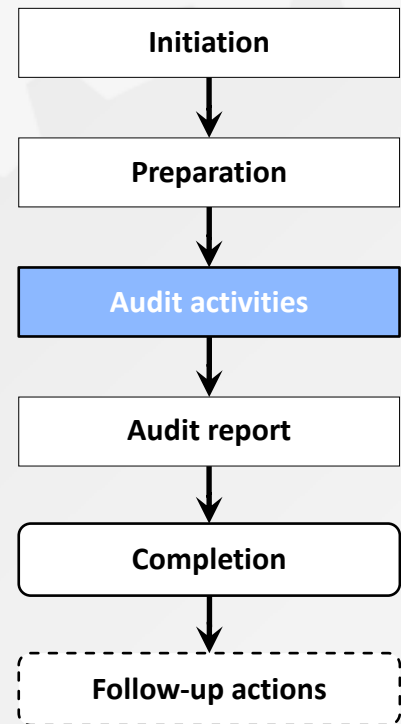| Initiation |
| :---: |
| Preparation |
| Audit activities |
| Audit report |
| Completion |
| Follow-up actions |
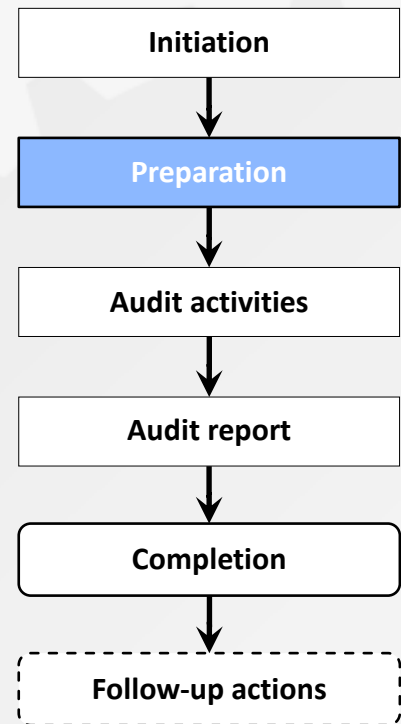
Conducting the audit activities

- Overview of audit activities:
  - Conduct the opening meeting
  - Assign roles of guides and observers
  - Collect and verify information / audit evidence
  - Generate audit findings
  - Prepare audit conclusions
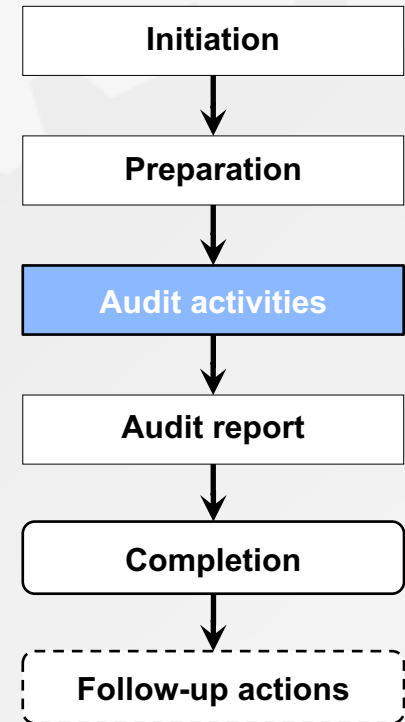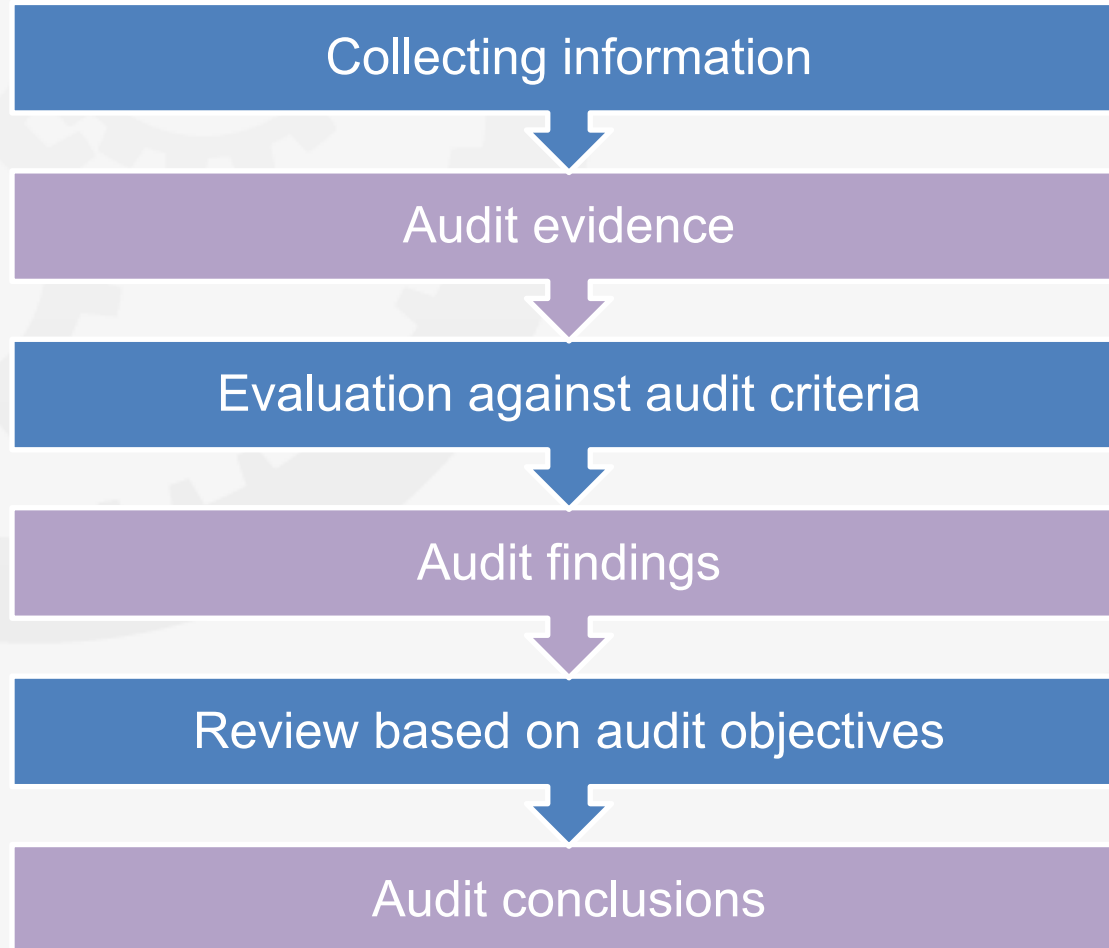 - Conduct the closing meeting

Initiation

Preparation

Audit activities

Audit report

Completion

Follow-up actions
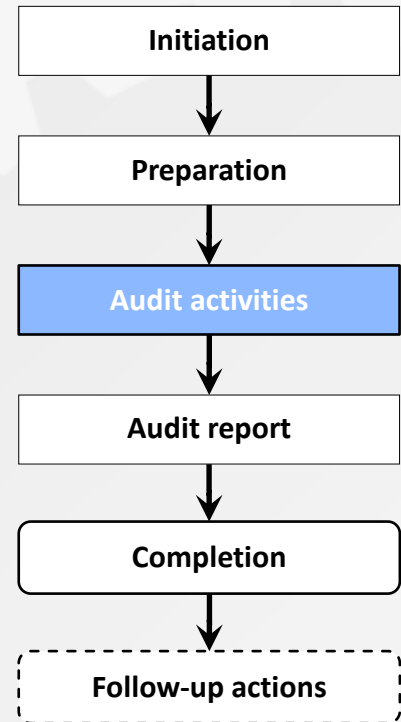
Conducting the audit activities

- ## Methods of collecting and verifying information / audit evidence:
  - On-site document reviews
    - Focus: Completeness, correctness, consistency and currentness of documentation
    - Important: Adequate sampling
  - Interviews
    - Ensure availability of the "right" persons
    - Carefully select questioning techniques (e.g. open vs. closed questions)
  - Observations of facts

Initiation

Preparation

Audit activities

Audit report

Completion

Follow-up actions

Conducting the audit activities

Collecting information

↓

Audit evidence

↓

Evaluation against audit criteria

↓

Audit findings

↓

Review based on audit objectives

↓

Audit conclusions

Initiation

↓

Preparation

↓

Audit activities

↓

Audit report

↓

Completion

↓

Follow-up actions

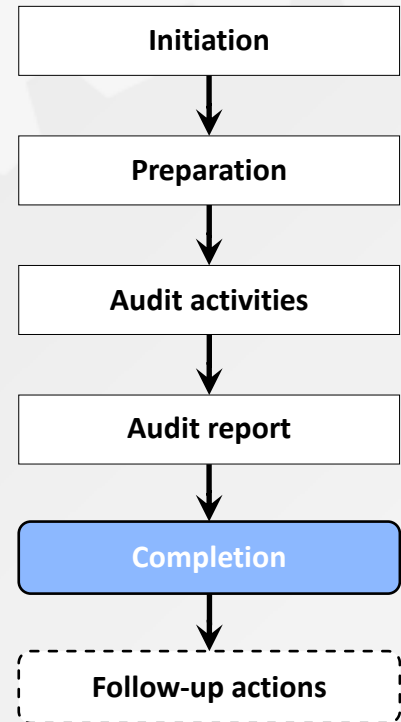# Preparing and distributing the audit report

- Typical contents of an audit report:
  - Audit objectives
  - Audit scope
  - Audit criteria
  - Identification of the audit client, audit team and auditees's participants in the audit
  - Locations, dates and times of performed audit activities
  - Audit findings
  - Audit conclusions
  - Statement on the degree to which audit criteria were fulfilled

| Initiation |
| Preparation |
| Audit activities |
| **Audit report** |
| Completion |
| Follow-up actions |
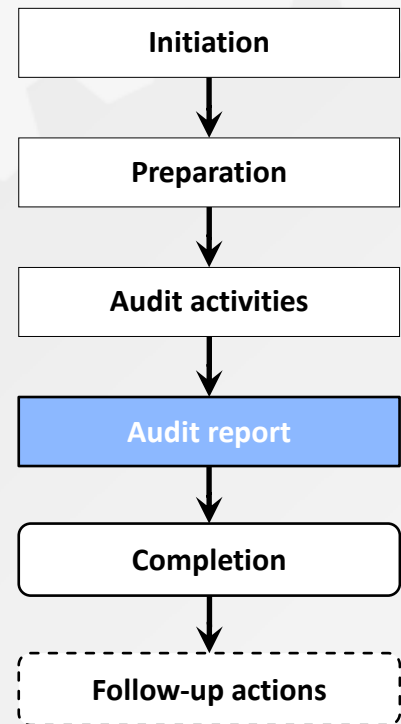
Completing the audit

- The audit is completed after all planned audit activities have been carried out.
- Disclosure of documentation and information obtained during the audit remains a duty of the audit team
- In the case of audits conducted by external auditors, the audit report is "owned" by the audit client

```
┌─────────────────────┐
│     Initiation      │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│     Preparation     │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│   Audit activities  │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│    Audit report     │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│     Completion      │
└─────────────────────┘
          │
          ▼
┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐
   Follow-up actions
└ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
```

![FitSM - Standards for lightweight IT service management]

Capability and maturity assessment

Keywords
Capability and maturity levels, task- and output-related capabilities

Capability vs. maturity

Capability:
- How good / effective are you at a single process or activity?
- How complete / consistent / well-maintained is a specific output?

Maturity:
- How good / effective is your overall management system, based on the specific capabilities in each process?

There are two different general categories of capability:
- Task capability
- Output capability

A typical capability / maturity model

Bundesarchiv, Bild 183-1990-0321-031 / CC-BY-SA 3.0

Brendan Bush Photography

Capability Level 4:
Managed

Capability Level 3:
Defined

Capability Level 2:
Repeatable

Capability Level 1:
Ad-hoc

Capability levels for tasks

|	
0 – Unaware	No awareness of the task, significant lack of understanding
1 – Ad-hoc	Aware of the task, but execution is uncontrolled and reactive, responsibilities are not always clear and outcome varies depending on individual efforts.
2 – Repeatable	The task is performed in a way that the intended outcomes are repeatedly achieved most of the time. Responsibilities are generally understood, and activities performed follow an intuitive understanding of how to fulfil them, but this may vary from individual to individual. There is insufficient documentation to support consistent achievement of desired goals, such as documented roles and procedures.
3 – Defined	Roles and responsibilities are clearly defined. Documentation, such as roles, procedures and templates is sufficient to support consistent achievement of desired goals. However, process compliance, effectiveness and efficiency are not comprehensively measured and audited to support a structured approach to continual improvement.
4 – Managed	The effectiveness of the service management activities is measured and monitored based on meaningful performance indicators. Nonconformities are detected by regular reviews and audits. Any nonconformity or lack of effectiveness is evaluated and used as an input for continual improvement.

Capability levels for outputs

0 – Non-existent	The required output (e.g. documentation) does not exist. / The intended achievement has not been reached.
1 – Initial	Some parts of the required output / achievement have been produced / reached. However, core elements are missing.
2 – Partial	Most of the core elements of the required output have been achieved, but still the output is not complete.
3 – Complete	The required output has been achieved, and all required elements have been considered.
4 – Aligned	The required output is clearly and visibly aligned to other outputs / elements of the service management system, i.e. a high level of consistency and compatibility has been reached (e.g. documents contain references to other documented information).

FitSM-6: Maturity and capability assessment scheme

- FitSM-6 is an easy-to-use tool (Excel-based) to assess the capability levels of ITSM processes and derive the overall maturity level of the SMS in a specific context of application
- Per requirement in FitSM-1: State descriptions for each of the capability levels (except levels 0 and 4) – for the specific context of the given requirement

7 general aspects, 14 ITSM processes → 85 requirements (3 to 8 per process) → 255 capability level state descriptions (3 per requirement)
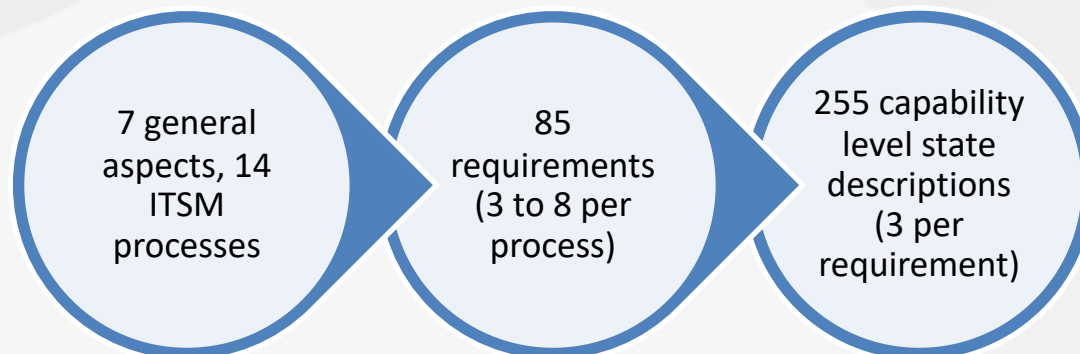
Management reviews

Keywords

Reviewing the adequacy, conformity, effectiveness and efficiency of the service management system (SMS)

Management reviews: 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:
    ○ (...)
    ○ Conduct management reviews at planned intervals
• (...)

- ## What is a management review?
  - Regular (often annual) review of the SMS by the SMS owner or another member of top management
  - Key questions:
    - Are policies and processes adequate and purposeful?
    - Which level of conformity has been achieved?
    - Is the SMS effective and efficient in its practical application?

Management reviews: Inputs

- Customer feedback
- Information on service performance and process conformity
- Current and forecast demand of resources and capabilities
- Results from recent risk assessments
- Results and follow-up actions from audits
- Results from a recent maturity assessment
- Results and follow-up actions from previous management reviews
- Information on changes that could potentially affect the SMS and the services
- Already identified opportunities for improvement

Management reviews: Outputs

- Record / report of the management review, including:
  - Overall assessment of the SMS
  - Identification of focal areas for improvement
- Plan(s) of follow-up actions
- Changes on the governance level, including:
  - New or changed policies
  - Changes in the provision / allocation of resources
- Changes to the audit programme
- Communication plan(s)