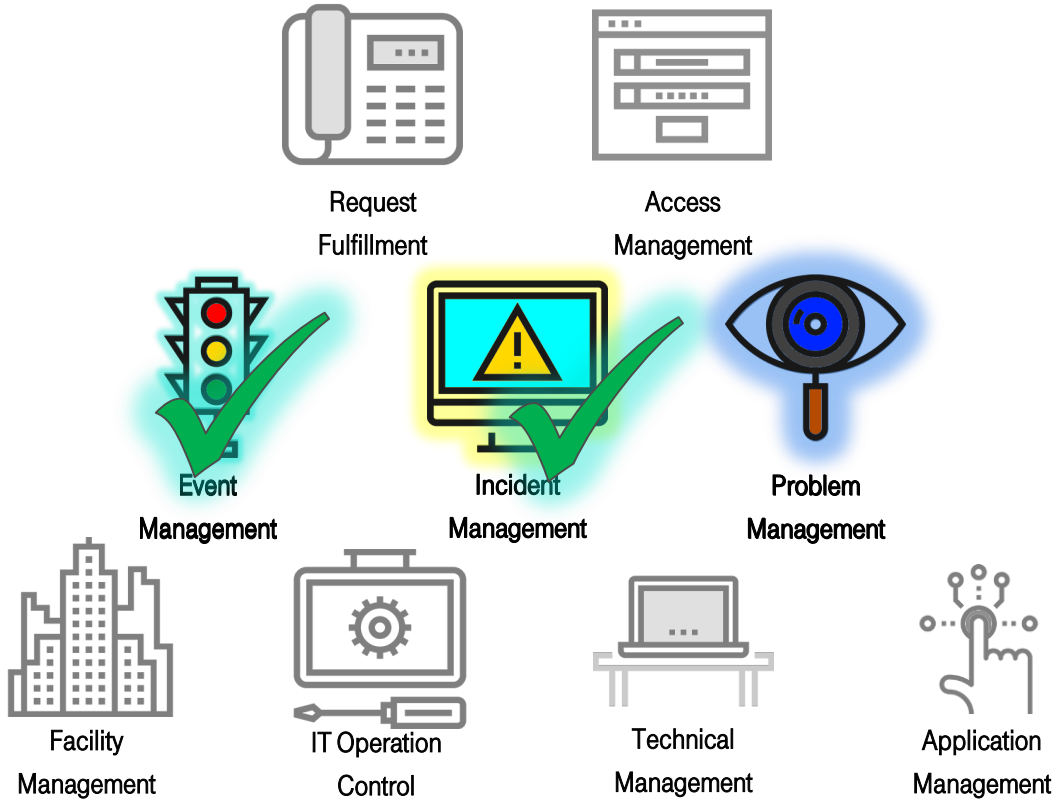
DEEP DIVE

→ Service Operation

SERVICE OPERATION – PRIMARY BREAKDOWN



PROBLEM MANAGEMENT - TERMINOLOGY

Problem Management = *the Crime Scene Investigation of ITIL*

Problem: The **root cause of** one or several real or potential **incidents**.

The root-cause is typically not known when the Problem is first recorded in a Problem Record.

Goal of PRM: Discover and describe, in detail, the root cause of these incidents.

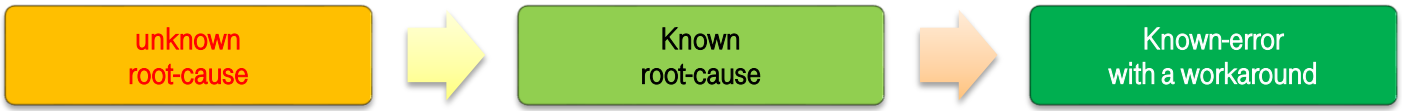
For discovered root causes, we want to develop a workaround (explained in previous chapter).

A root-cause paired with a workaround is **known error**.

Known Error Database (KEDB): Collection of known errors.

If a workaround is not necessary, an Incident Model may be created: Guide for resolving these incidents.

Problem Record:



PROBLEM MANAGEMENT - TERMINOLOGY

- Suggestion to add a record to the database.
- Can be realized as a flag or status.

PROBLEM MANAGEMENT – SOURCES OF PROBLEMS

Problem Management manages the lifecycle of all problems.

Objective of Problem Management is to prevent incidents from happening, and to minimize the impact of (future) incidents.

How is Problem Management triggered?

Major Incident	• INM: “Handling of Major Incidents” • A problem record must be created to discover the root-cause and suggest a way to eliminate it.
Incident with unknown root-cause	• If we don’t know what caused the incident, we must investigate. • This applies also to cases where we can resolve the incident (perhaps by rebooting).

PROBLEM MANAGEMENT – SOURCES OF PROBLEMS

MAJOR

- INM: “Handling of Major Incidents”
- A problem record must be created to discover the root-cause and suggest a way to eliminate it.

UNKNOWN

- If we don’t know what caused the incident, we ust investigate.
- This applies also to cases where we can resolve the incident (perhaps by rebooting).

REPEATED

- If incidents keep recurring, we should spend time to investigate a way to get rid of their root-cause.

VULNERABLE

- If we learn of a vulnerability that could result in incidents in the future, we use Problem Management to create a patch and design a way to apply it to all affected systems.

PROBLEM MANAGEMENT

Problem is the root-cause of incidents.

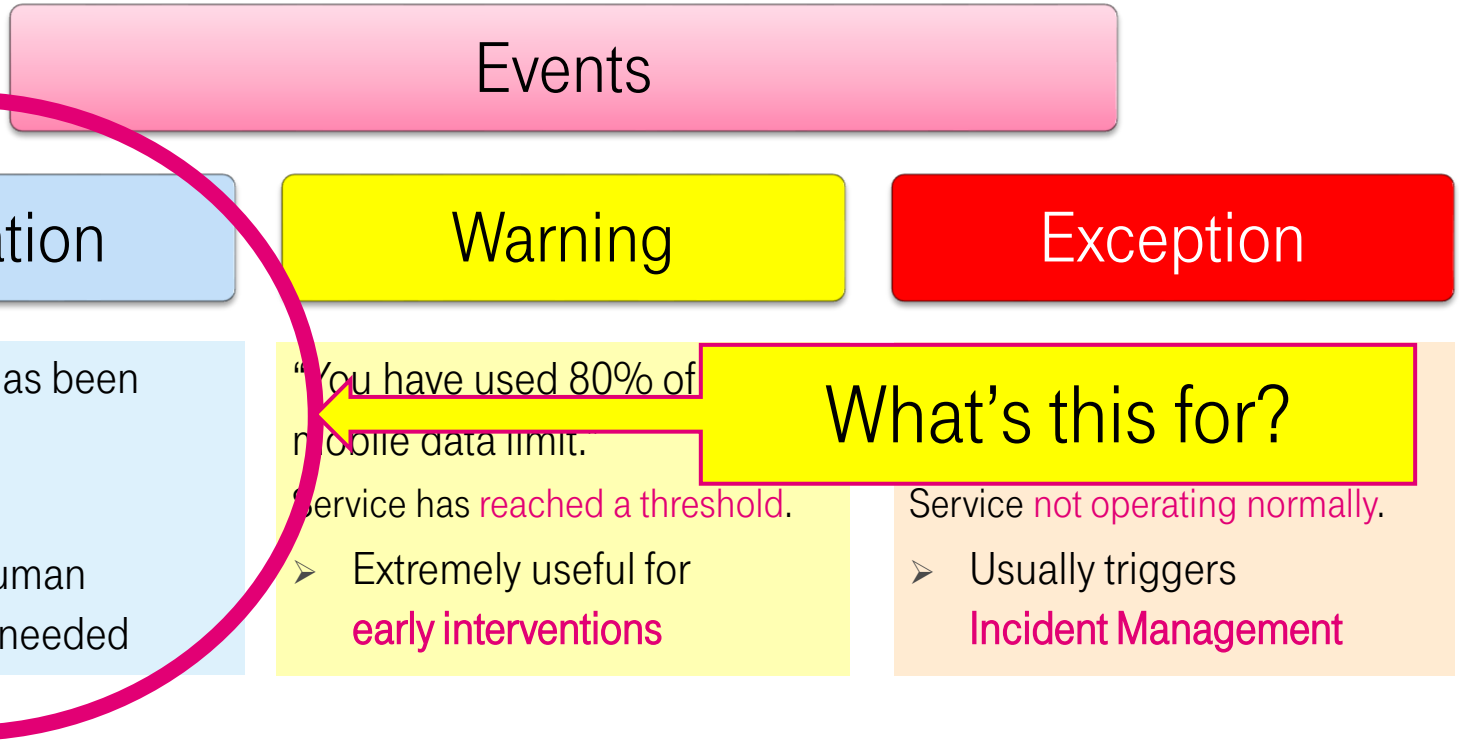
It turns from a mystery, which requires a detective work, into an engineering task of fixing the broken element.

Each phase may require different type of expert.

Problem Manager – the role responsible for managing day-to-day PRM operation – should not hesitate to assign multiple experts to a single problem.

Common mistake: “You discovered it, you solve it!”

PROBLEM MANAGEMENT & EVENT MANAGEMENT RELATION



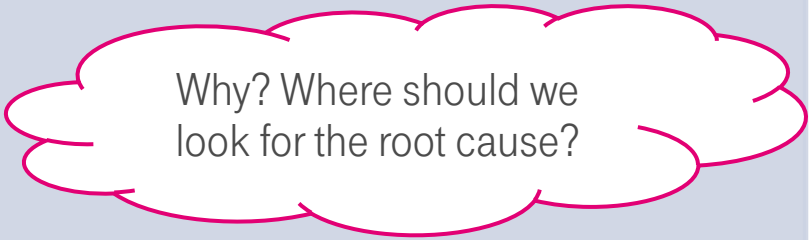
PROBLEM MANAGEMENT & EVENT MANAGEMENT RELATION

Information Events are extremely useful for Problem Management

Information Events = clues for investigating.

Without Info-Events

10:30:25 – Server is shutting down due to insufficient memory. All data lost.



With Info-Events

10:27:15 – User ADMIN logged in.

10:28:40 – User ADMIN launched virus.exe

10:30:25 – Server is shutting down due to insufficient memory. All data lost.

PROBLEM MANAGEMENT – PROCESS STEPS

Problem is reported	• A Suggested New Problem is entered, or Major Incident handling opens Problem Record • Analytical tool (such as TSSK's RADAR) identifies a group of recurring incidents
Problem Categorization And Prioritization	• The record is properly prioritized and categorization is done so that it may be passed to the right experts.
Problem Diagnosis and Resolution	• The root-cause is discovered and documented. Workaround or solution is discovered. • A Change is triggered to implement the solution if necessary.
Problem Closure And Evaluation	• Known Error Database is updated. • If a Change was submitted for implementation, Problem Closure waits for the Change Closure.

PROBLEM MANAGEMENT – PROCESS STEPS

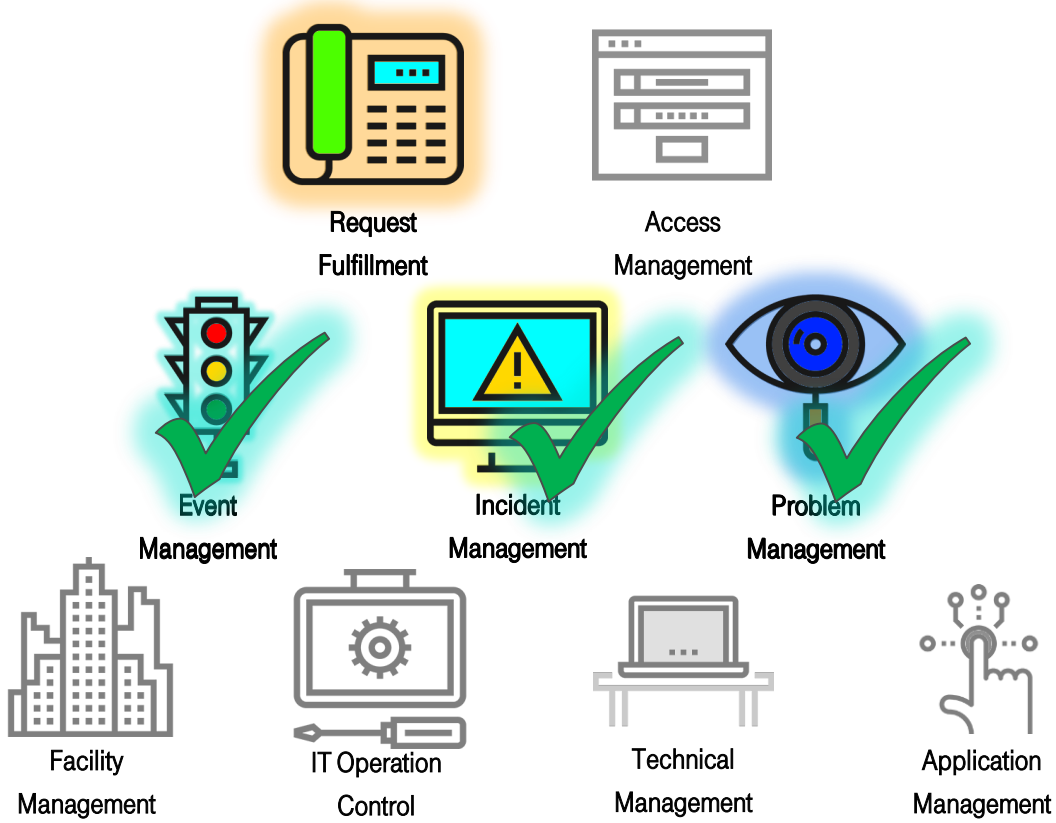
Additional process steps

Major Problem Review – review whether a Major Problem was permanently solved.

Proactive Problem Identification – aims to identify incidents before they occur, and to identify recurring incidents.

Proactive Problem Management is a sign of process maturity – the organization redirects some of its resources away from development of new features or supporting regular operation, and towards stability and availability of the service.

SERVICE OPERATION – PRIMARY BREAKDOWN



REQUEST FULFILLMENT

Request Fulfillment fulfills **service requests**.

Service Requests are typically simple changes

- Resetting a password
- Scheduling a standardized report

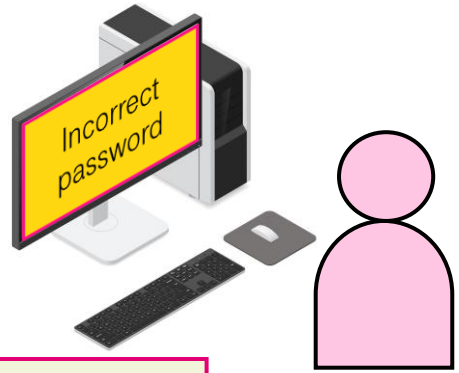
Historically evolved from incidents.

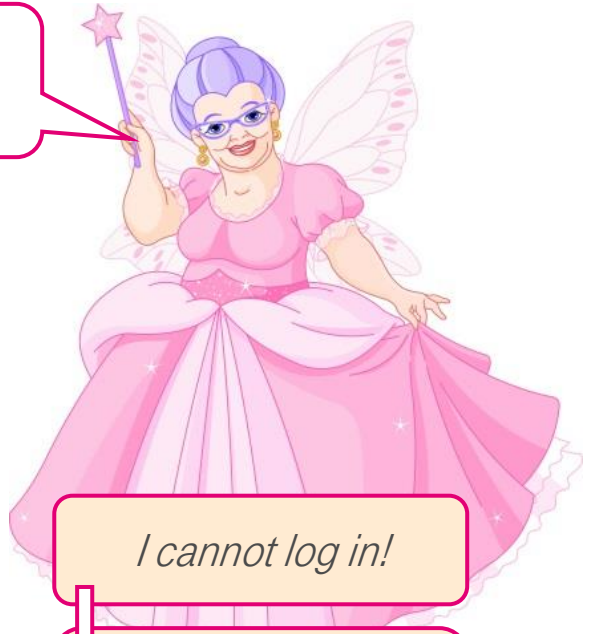
Only people who know a password can use the service

This one doesn't know, and wasn't let in...

The service is working exactly as intended!

It's not an incident!





I cannot log in!

The service is not working!

It's an incident!

REQUEST FULFILLMENT

Request Fulfillment is very similar to Standard (Model) Changes.

Users submit Request for Service → **Logging and Categorizing**.

Request Models provide clear step-by-step instructions for Request Operator.

Ongoing background processes:

Request Fulfillment Support – ensures functionality of tools and availability of know-how. May be realized as a **Service Portal**.

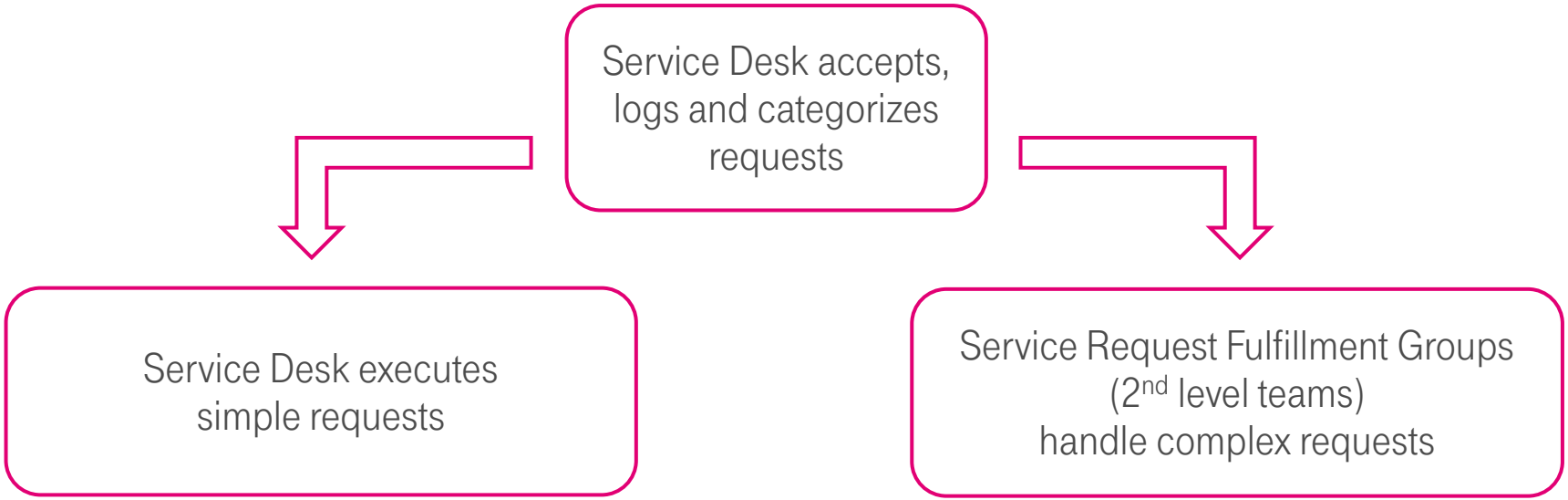
Request Monitoring and Escalation – ensures that requests do not breach their expected execution/delivery time.

REQUEST FULFILLMENT

Submitted Requests for Service are handled by 3 processes:

Logging and Categorization	• Usually performed automatically by self-service systems (Service Portals)
Request Model Execution	• Operator follows a Request Model to fulfill the request • Early steps: Authorization, later steps: Execution
Request Closure and Evaluation	• Checks if user is satisfied with the result • Analysis is performed to allow improvement

REQUEST FULFILLMENT



Unlike in Incident Management, changes are **not** submitted to execute configuration updates:
These updates (change of password etc.) are done directly in Request Fulfillment.

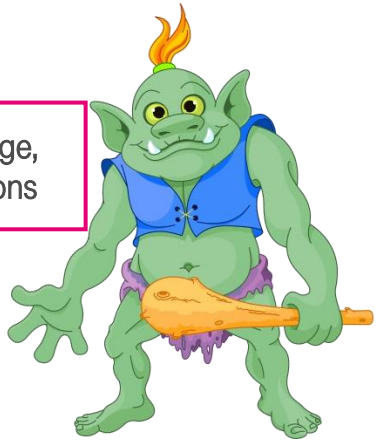
SERVICE OPERATION – PRIMARY BREAKDOWN

Fairy godmother granting wishes

Request Fulfillment

Access Management

Troll guarding a bridge, asking tricky questions



Event Management

Incident Management

Problem Management

Facility Management

IT Operation Control

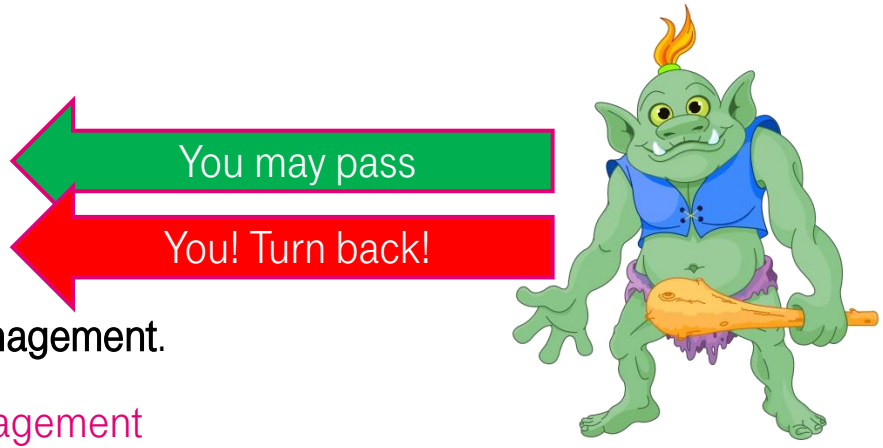
Technical Management

Application Management

ACCESS MANAGEMENT

Access Management aims to ensure:

- ✓ That authorized users can use the service fully
- ✘ That everyone else cannot use it at all



Can also be called **Rights Management** or **Identity Management**.

Remember: Service Design: Information Security Management

→ defines **policies** (rules) for accessing information

→ defines **named privilege** (or named right) that represents each policy

Access Management implements and executes these **policies**

ACCESS MANAGEMENT

Remember: **Service Design**: Information Security Management

→ defines **policies** (rules) for accessing information

→ defines **named privilege** (or named right) that represents each policy

Access Management implements and executes these **policies** ⇨

```
If (User:Role =
Recruiting
Specialist) →
Allow access to:
HiringTool
```

Role: Recruiting Specialist

✓ Can access candidate info

ACCESS MANAGEMENT

What is the most common security hole in Access Management?

- The Access Management systems do not check if the need for the rights is still valid.

In the Recruiter example:

- A person begins as a recruiting specialist.
- Moves to a different position after 6 months.
- If Access Management is not properly implemented:
  Still has access to confidential information of candidates.

Removal of access rights: **revocation**. “The rights have been revoked.”

ACCESS MANAGEMENT – BIGGEST CHALLENGE

What's the right balance between perfect security and acceptable usability?

Theoretically, the rights could have been revoked in the middle of an activity.

Should a computer system check once per second...

... and erase the screen if the rights are revoked?

Or is checking rights at the beginning of a session enough?

Different approaches are needed according to sensitivity of content:

→ Reading a poem online

→ Accessing nuclear launch codes

ACCESS MANAGEMENT – SUB-PROCESSES

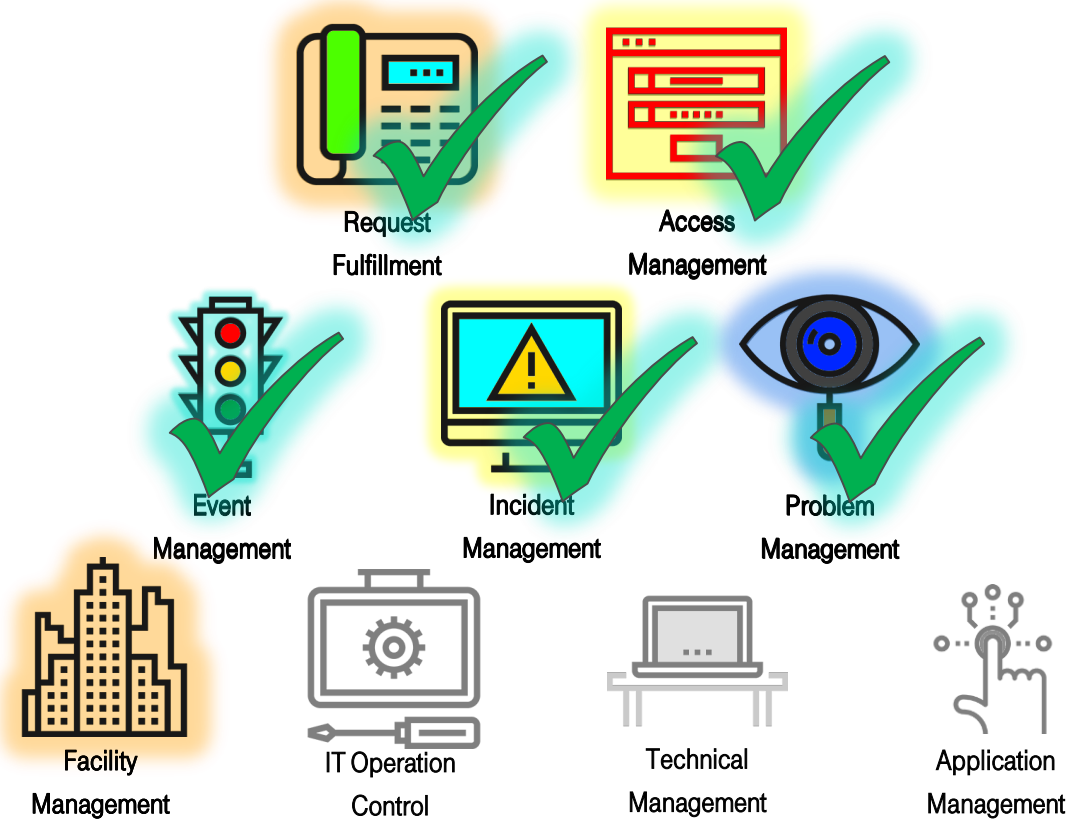
Maintenance of Catalogue of User Roles and Access Profiles	• Checks if available rights allow proper usage. • Checks if some users have rules they no longer need.
Processing of User Access Requests	• Adds, modifies or revokes access rights, depending on the particular request. • Is connected to the systems for which access rights are managed.

T-Systems makes frequent use of Who-Is-Who as its Access Management system.

When we try logging into any of the connected tools, a remote authentication query is performed.

This query results in either “Yes, the user can log in and should have rights [X] and [Y]”, or “No, do not let this user in.”

SERVICE OPERATION – PRIMARY BREAKDOWN



FACILITIES MANAGEMENT

Facilities Management manages the physical environment that houses all the IT infrastructure.

Objective:

Ensure the environment is optimal for the IT infrastructure.

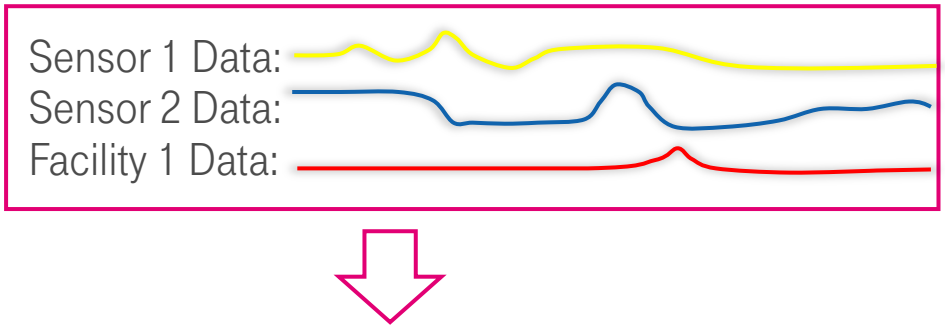
F.M. takes care of:

- Cooling, heating, air flow
- Access to buildings (in cooperation with Access Management)
- Environmental Monitoring: fire sensors, gas leak sensors, seismic sensors...

Process owner: Facilities Manager

Individual buildings may have Facility Managers assigned to them.

FACILITIES MANAGEMENT



Concerns identified

Submitted to other processes (John McClane in ventilation shaft)

Solved by Facilities Management (Replacement of faulty component)

FACILITIES MANAGEMENT

- Cooperates closely with
  - → Service Continuity Management
  - → Business Continuity Management

- Cooperates on the development of disaster recovery plans, such as in case of fire.

- Directly linked to Health And Safety Regulations.

FACILITIES MANAGEMENT

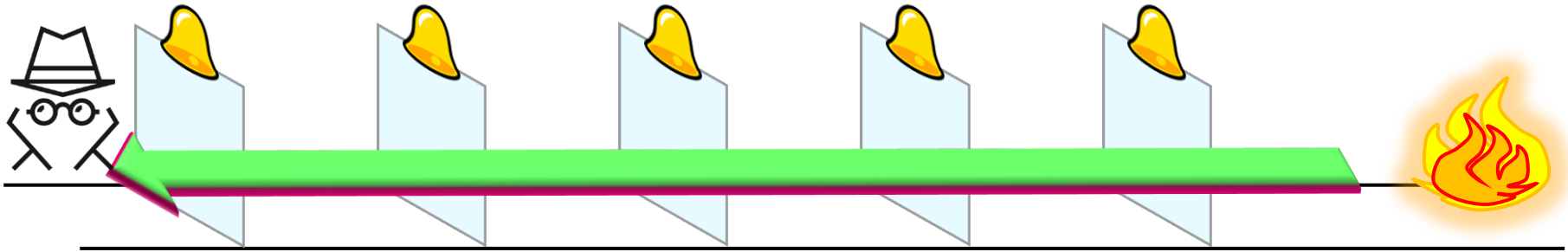
- Access Management's big challenge: Balancing access control with usability
- Facilities Management's big challenge: Balancing Health And Safety regulations with Security

  → How to delay attackers or thieves who want to penetrate our security...

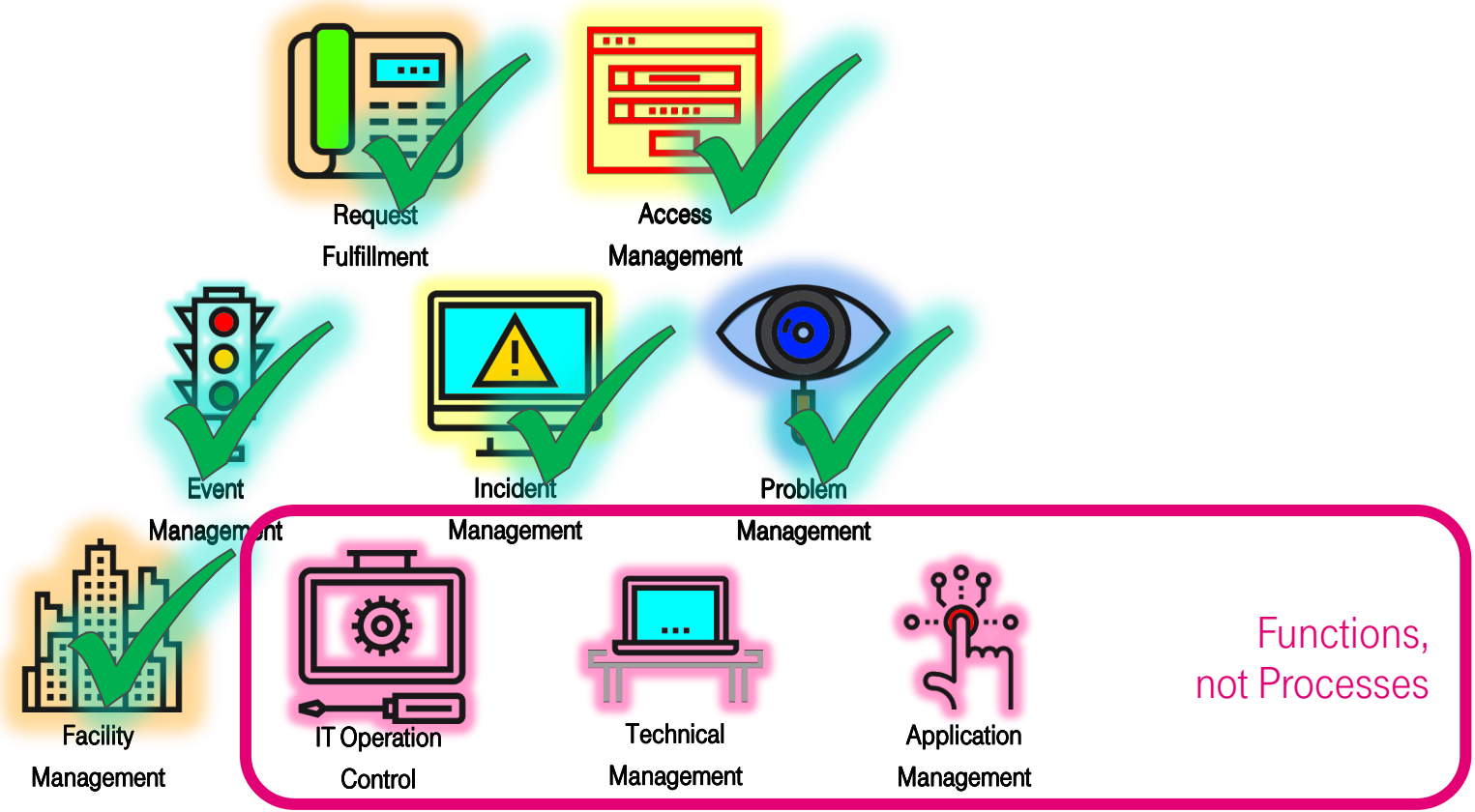
  → ... but allow trapped employees escape in case of fire?

Attackers breaking the first door will activate alarm (still enough time to stop them)

Possible solution: Serializing security elements



SERVICE OPERATION – PRIMARY BREAKDOWN



IT OPERATIONS CONTROL

The function **IT Operations Control** is responsible for

- monitoring
- controlling

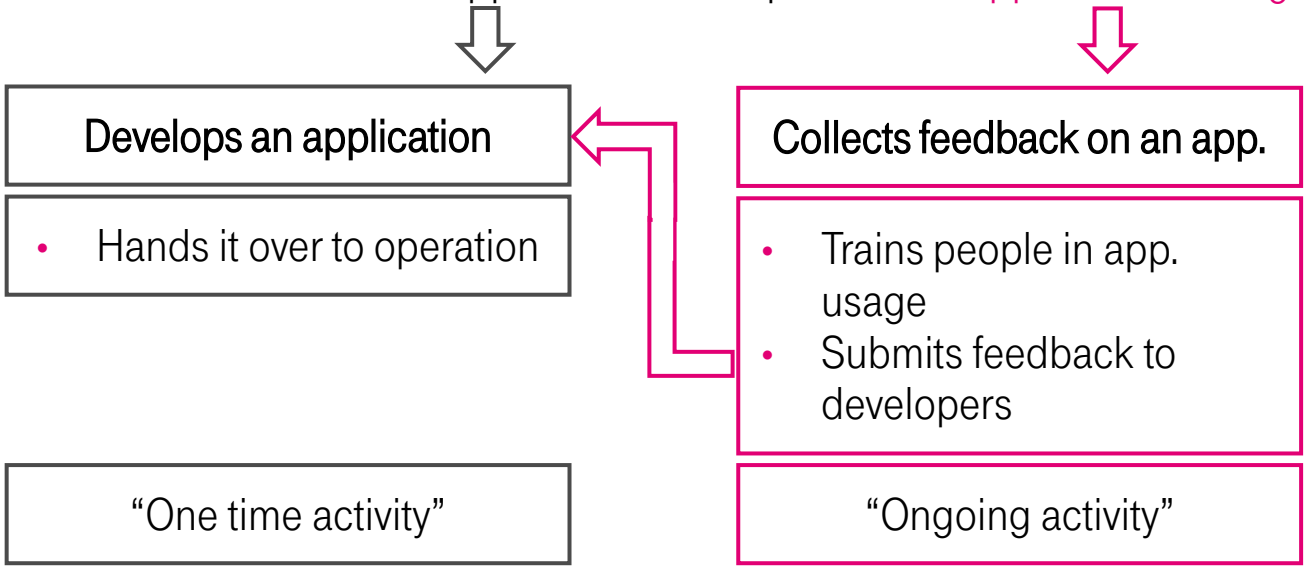
of the services and their underlying infrastructure.

This is limited to routine daily tasks:

- Backups and Restoration of data
- Managing printers and phones
- Maintaining IT equipment of a service provider organization

APPLICATION MANAGEMENT

Note the difference between Application Development and Application Management



Application Management owner: **Application Analyst**

→ Understands the application and explains it to others

→ Doesn’t “own” the application

APPLICATION MANAGEMENT – SKILLS INVENTORY

Application Management is in charge of Skills Inventory

→ A catalogue of skills needed to deliver the service

Wine Manipulation Skill

- Opening a bottle
- Selecting proper glass
- Pouring wine

TECHNICAL MANAGEMENT

Technical Management: A clone of Application Management, but for technologies.

Technical Management studies and analyses new technologies, then trains people how to operate them.

Scope of work:

- Preparation of trainings for new technologies (servers, routers and switches, storage systems, cables...)

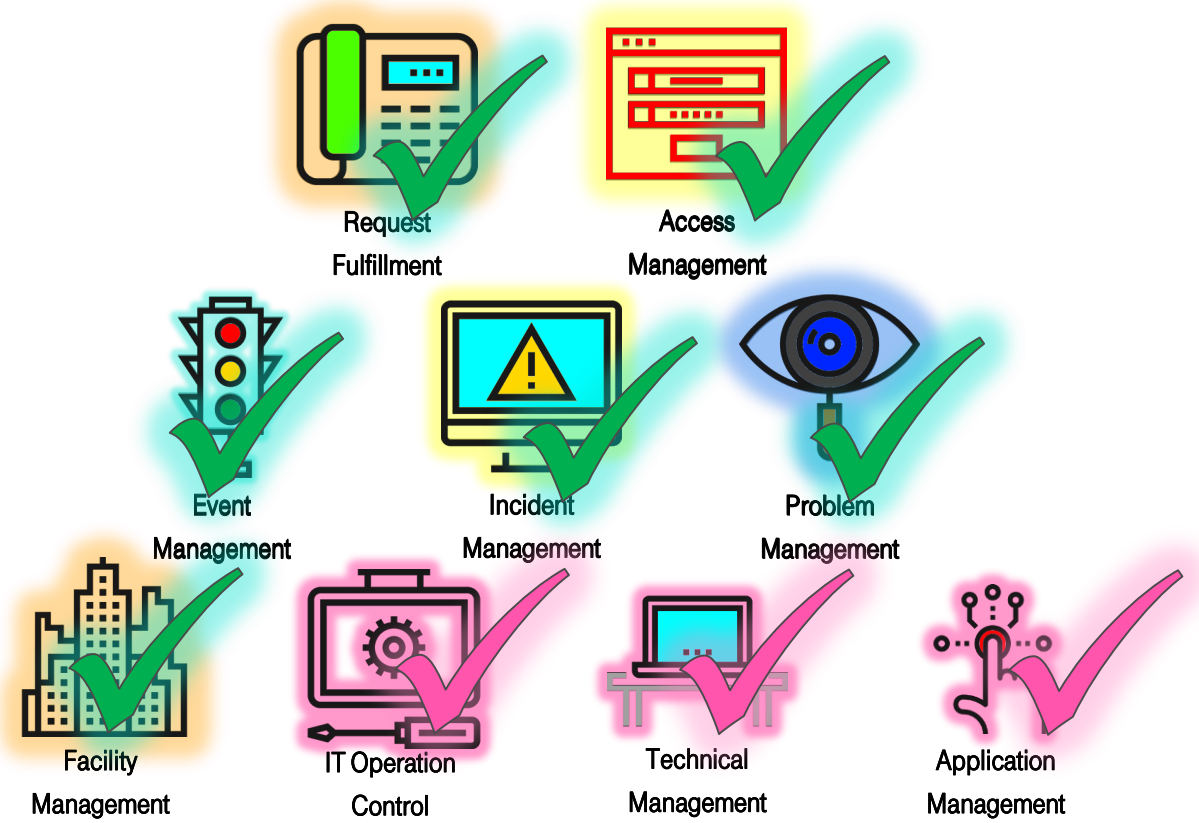
Technical Management teaches people to operate the technology in an efficient manner and without errors.

Technical Management owner: **Technical Analyst**

→ Understands the technology and explains it to others

→ Doesn't "own" the technology

SERVICE OPERATION – PRIMARY BREAKDOWN



SERVICE OPERATION - SUMMARY

- ✓ Service Operation governs the day-to-day operation of our service.
- ✓ Customers are **raising requests** → Request Fulfillment.
- ✓ Some requests require **access** → Access Management.
  We must not forget to revoke the rights when no longer needed.
- ✓ Event messages notify us about service disruptions.
- ✓ We open **Incidents** to **restore normal operation**.
- ✓ Unknown solution, unknown root cause, major incident → **problem record** → **Problem Management**.
- ✓ **Facility Management** ensures stable environment.
- ✓ **Application Management** and **Technical management** support optimal performance of software and hardware.

DEEP DIVE

→ Service Operation