

DEEP DIVE

→ **Service Operation**

SERVICE OPERATION - INTRODUCTION

Aim of Service Operation:

Ensure that IT services are delivered effectively and efficiently.

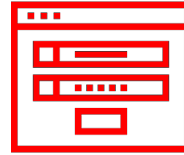
ITIL cannot know what kind of service we are providing and cannot advise on specific details of our service.

Instead, best practices focus on monitoring whether a service is operating, resolving service disruptions and investigating their root causes.

SERVICE OPERATION – PRIMARY BREAKDOWN



Request
Fulfillment



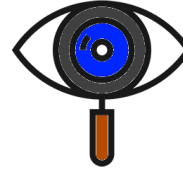
Access
Management



Event
Management



Incident
Management



Problem
Management



Facility
Management



IT Operation
Control

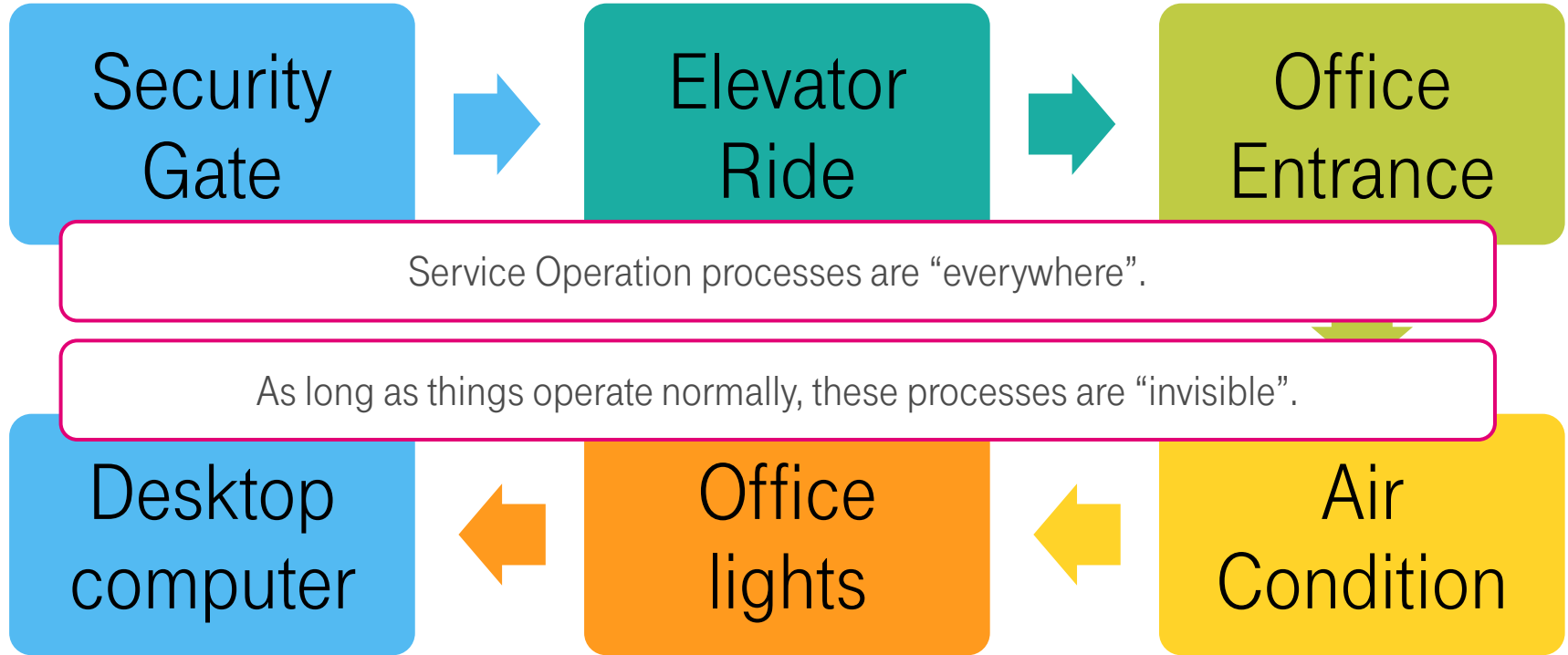


Technical
Management

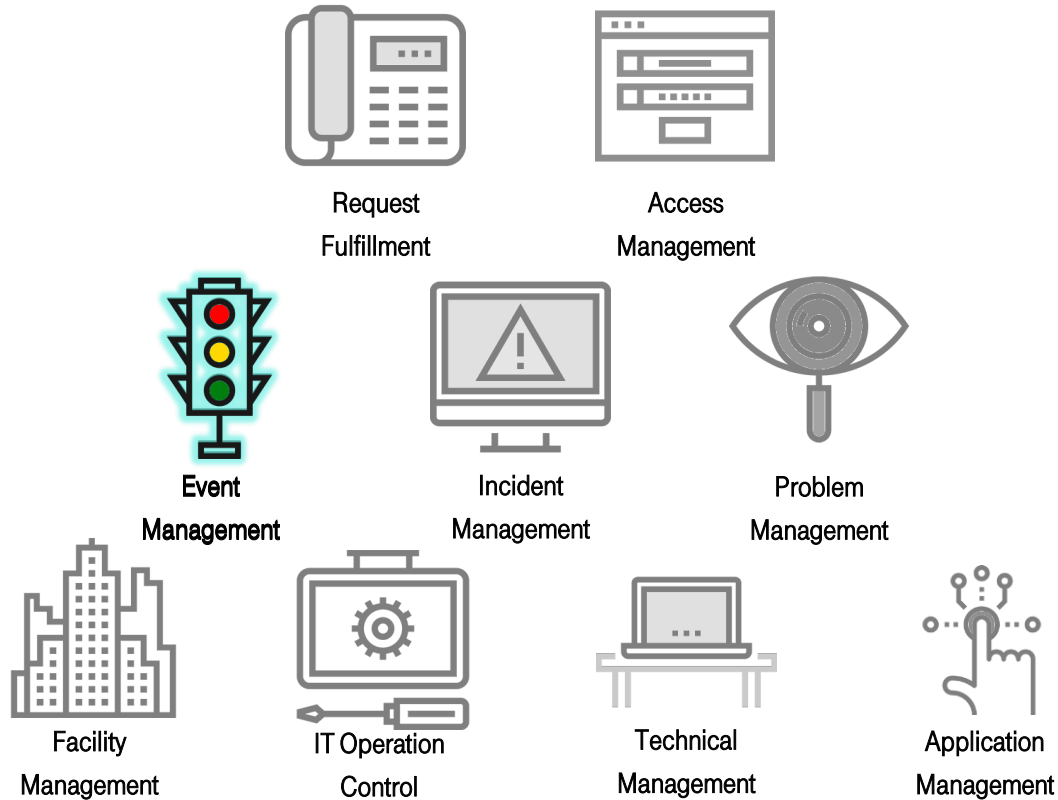


Application
Management

A LOVELY MORNING... OF A T-SYSTEMS EMPLOYEE



SERVICE OPERATION – PRIMARY BREAKDOWN



EVENT MANAGEMENT

Objective:

Ensure that all elements of the infrastructure are constantly monitored.

Monitoring of all CIs generates a huge volume of records about their status.

Manual checking of all records would not be possible.

Event Management filters and categorizes them, separating those which need human intervention.

EVENT MANAGEMENT – WHAT IS AN EVENT

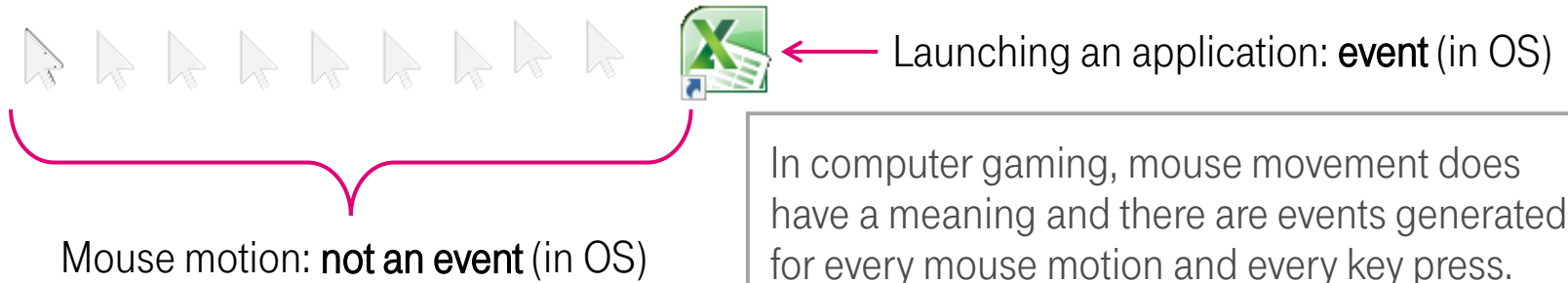
Event:

Any technically discernible occurrence
which could have an impact on the management of an IT service.

Event has to be technically discernible – a technology-based way to recognize the event must exist.

This usually boils down to: an electricity starts/stops flowing through a component,
or a digital message was generated

Event is something that **could** have an impact on an IT service.



EVENT MANAGEMENT

Events are most commonly represented by **messages**.

A component generates a message and sends it to another component (Operating System etc.)

Event messages have precisely defined structure, allowing for machine analysis.

Computer generated messages
(Event log)

Application Excel.exe was started
Storage space is 67% full
Application Game.exe was started
Storage space is 75% full

Human written messages
(Book of complaints)

Why was there no sugar in my coffee?!
Please bring sugar next time...
This restaurant sucks! No sugar!

EVENT MANAGEMENT – TYPES OF MESSAGES

Events

Information

“The device XYZ has been turned on.”

- Typically, no human intervention is needed

Warning

“You have used 80% of your mobile data limit.”
Service has **reached a threshold**.

- Extremely useful for **early interventions**

Exception

“The site you are trying to reach is not responding.”
Service **not operating normally**.

- Usually triggers **Incident Management**

EVENT MANAGEMENT



When a new customer enters, a “time limit” starts ticking in their mind. Unless they are given attention, they may get upset and/or leave

A bell sounds when a new guest enters.

Is it an event?

- Technically discernible?
- Could it have impact on the service?

What type of event is it?

- a) ~~Information,~~
- b) Warning, or
- c) ~~Exception?~~

EVENT MANAGEMENT

Maintenance of Event Monitoring Mechanisms and Rules

- Makes sure monitoring tools are fully functional
- Improves tools to keep up with the changing technology

Event Filtering and 1st Level Correlation

- Filtering: Filters out those events which don't need intervention
- 1st Level Correlation: Passing remaining events to proper operators and experts

2nd Level Correlation and Response Selection

- (2nd Level) experts analyze the warning/exception message
- Based on the analysis, they may open an Incident Record which then goes through Incident Management process

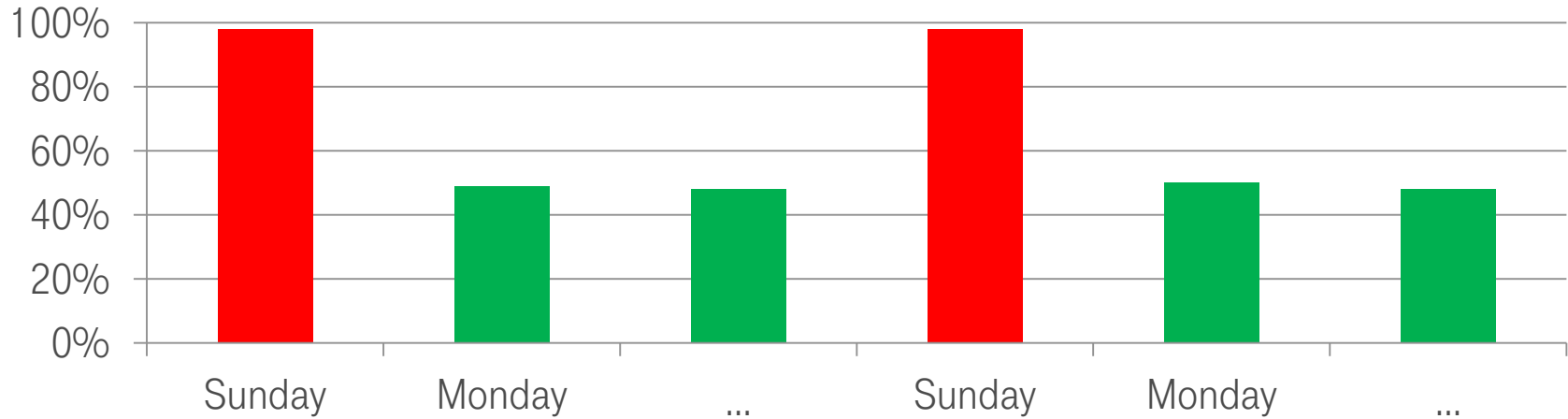
EVENT MANAGEMENT

Event Review and Closure – fourth subprocess of Event Management

Objectives:

Check if events were handled appropriately and may be closed

Perform regular analysis of even trends and patterns

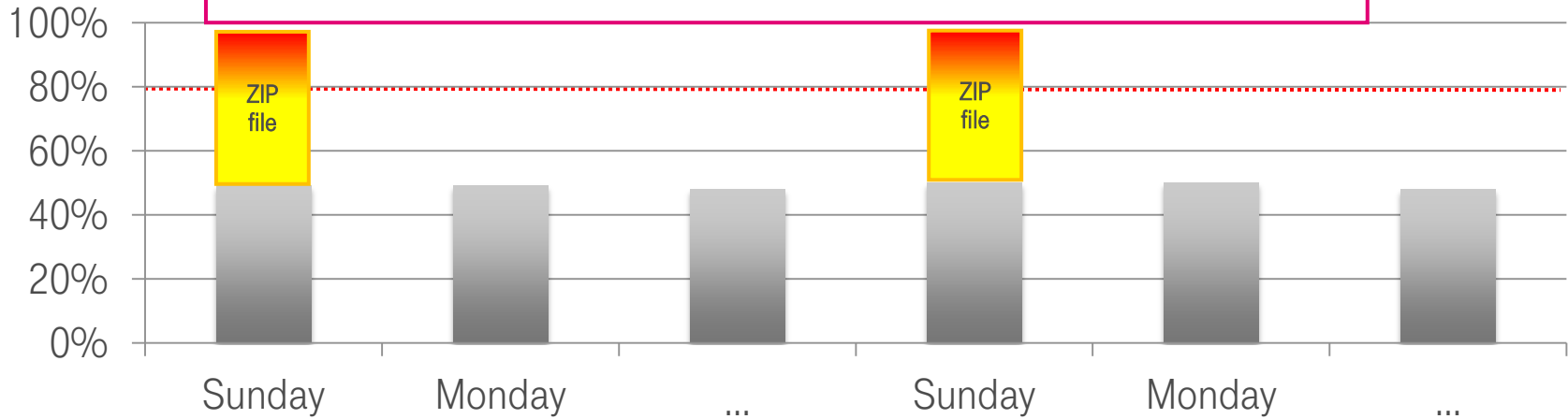


EVENT MANAGEMENT

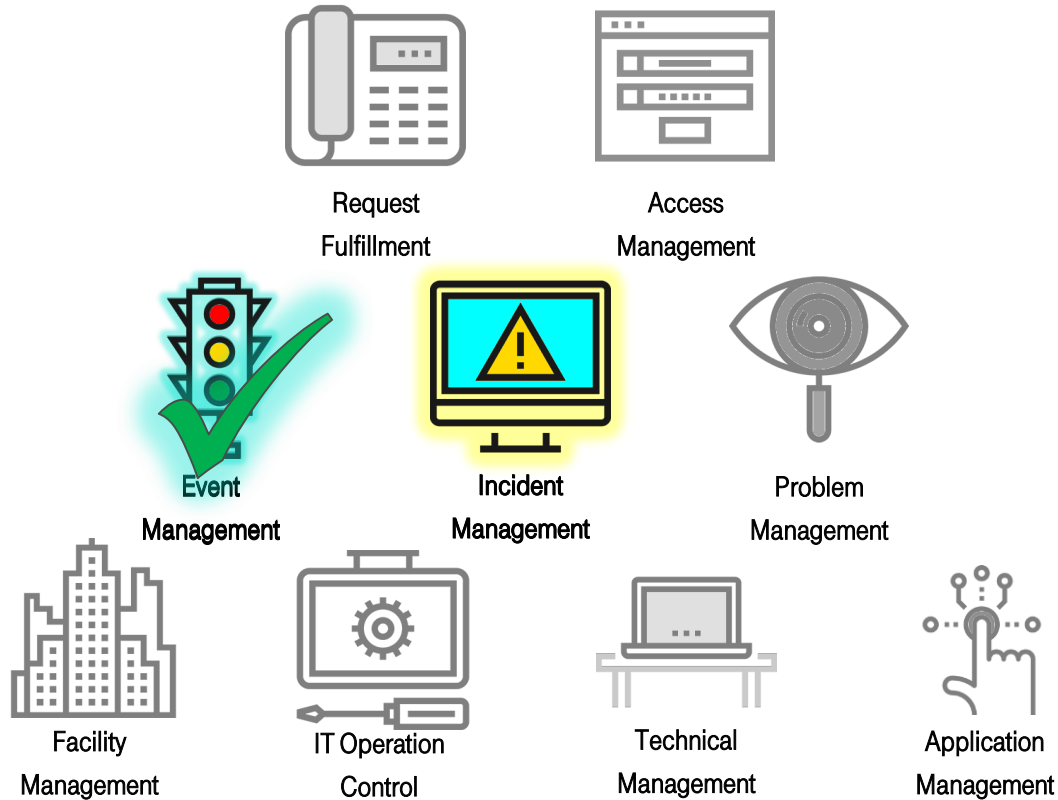
Event Review and Closure – fourth sub-process of Event Management

Backup procedure (Sunday evening):

1. Create a compressed file, containing EVERYTHING on the system drive.
2. Store this compressed file on the system drive. ← Warning generated
3. Move the resulting file to a backup location.



SERVICE OPERATION – PRIMARY BREAKDOWN



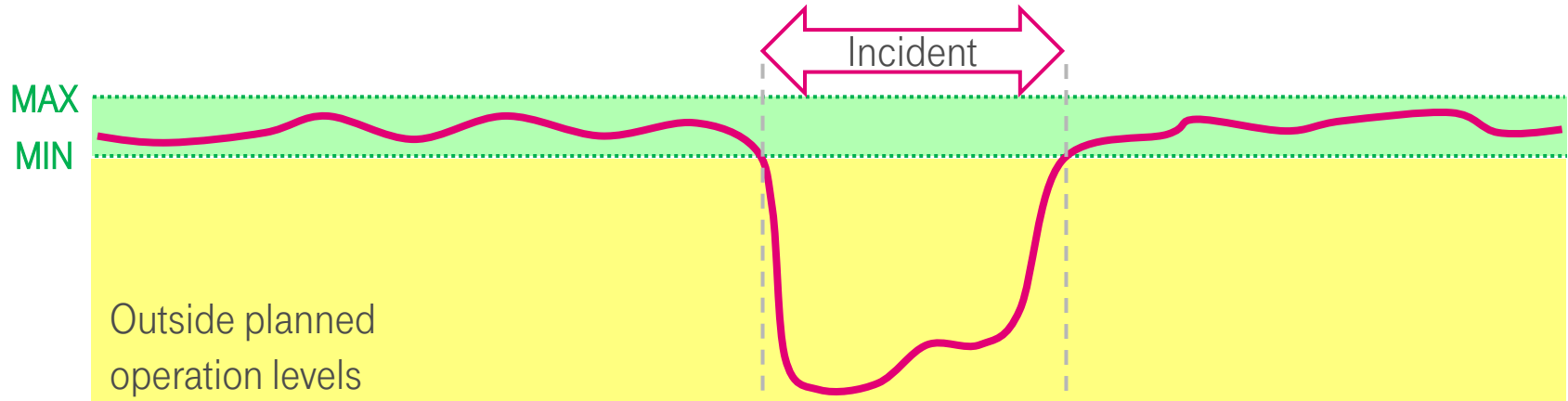
INCIDENT MANAGEMENT

Incident Management governs the lifecycle of all incidents.

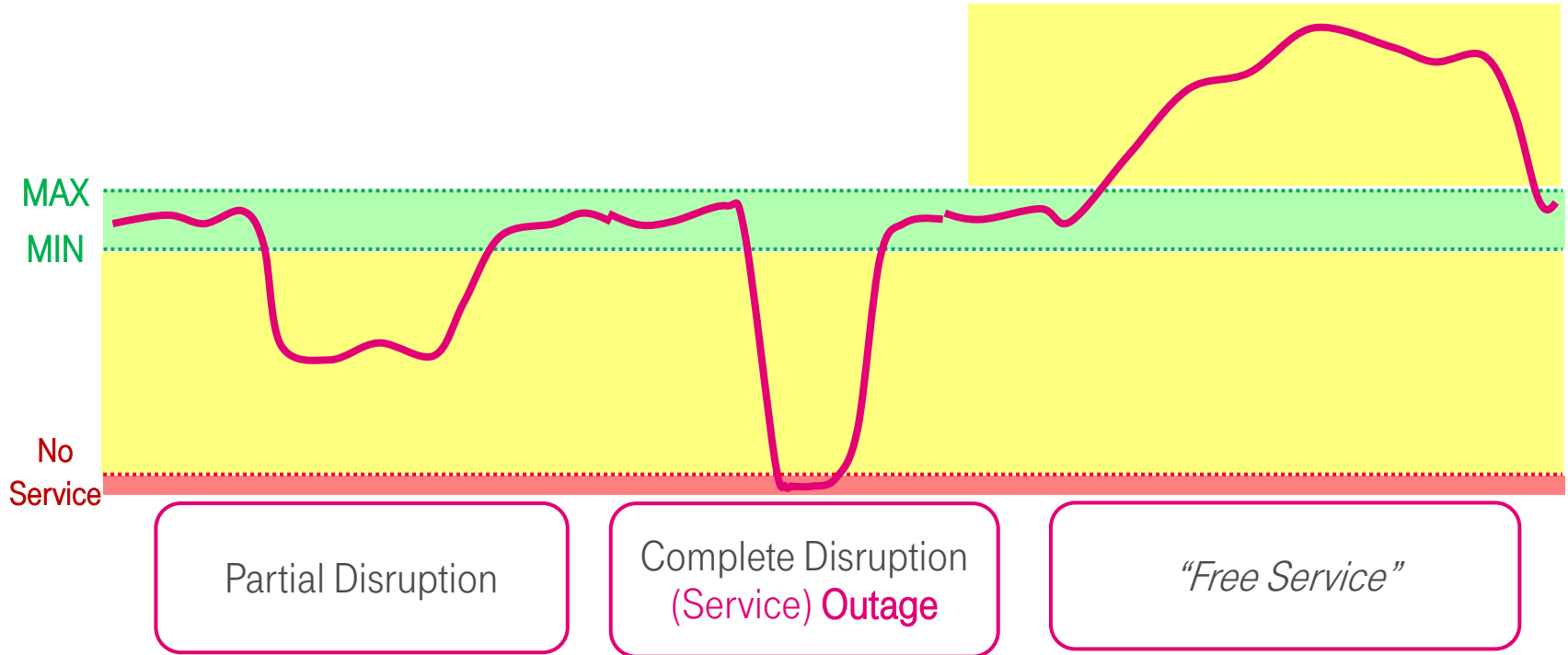
Incident:

Any unplanned disruption of normal service operation.

alternatively: Each case when service is operating outside planned operation levels.



INCIDENT MANAGEMENT – TYPES OF DISRUPTION



INCIDENT MANAGEMENT

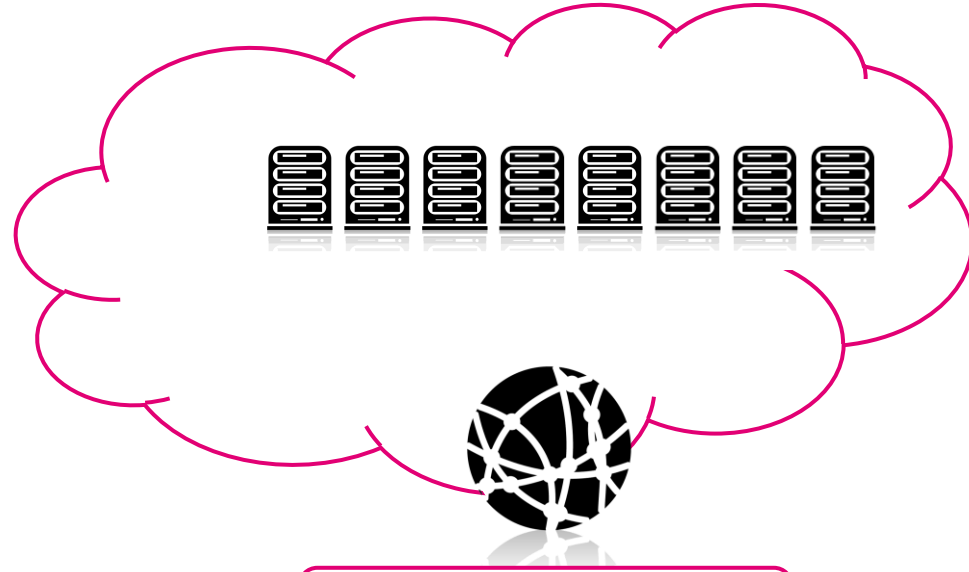
Discovery of incidents:

- Monitoring (**Event Management**)
- Customer/user complaint



Classic Systems

Failure is apparent
to customer

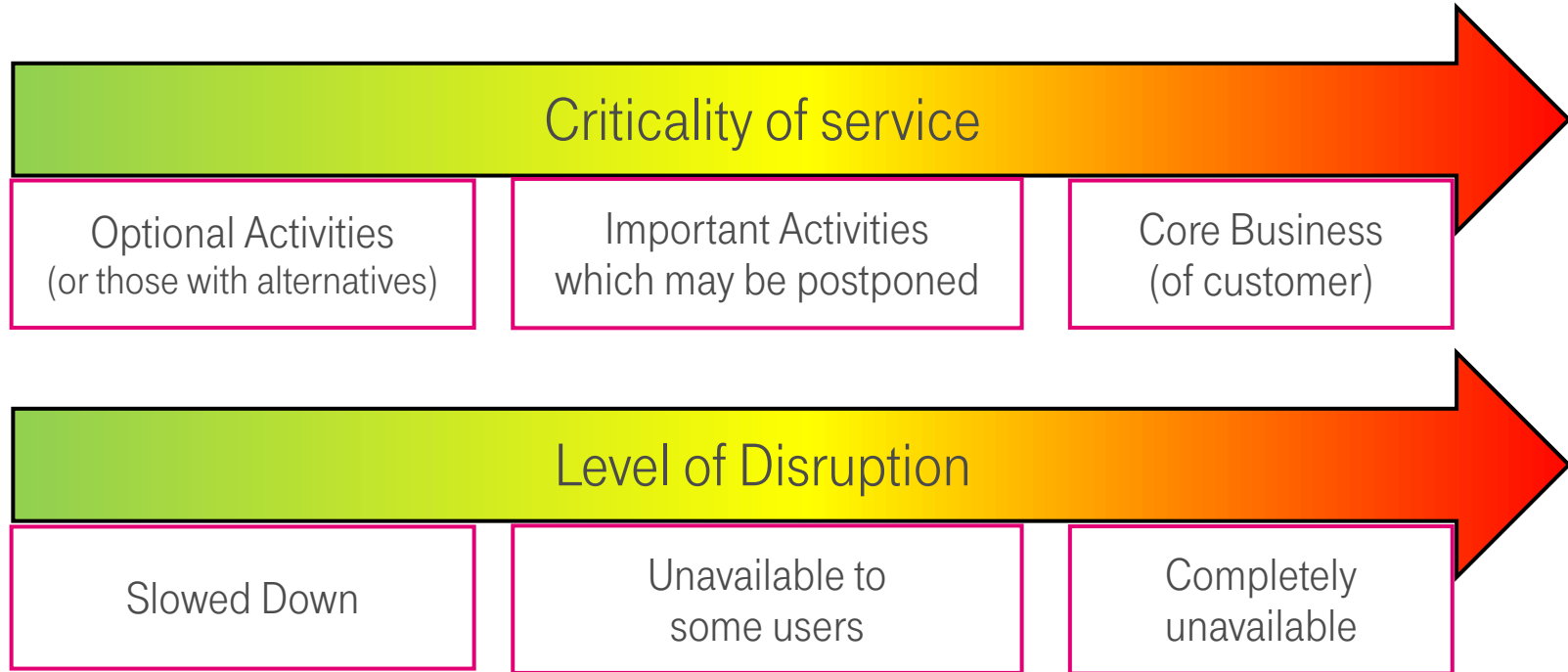


Cloud Systems

Failure remains hidden
(another system steps in)



INCIDENT MANAGEMENT

- Incident Prioritization allows deciding on urgency/sequence of solving multiple incidents

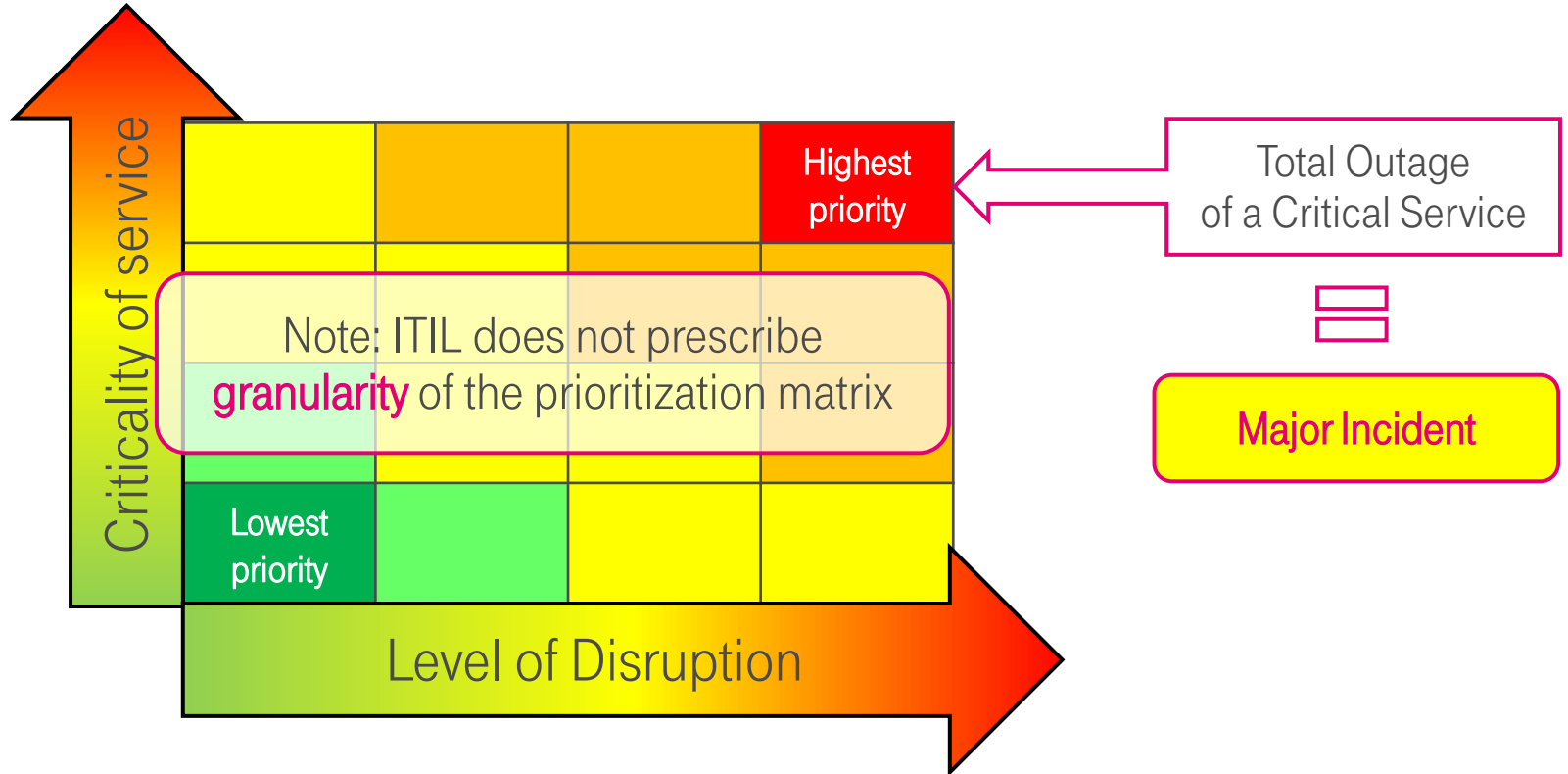


INCIDENT MANAGEMENT

- The same component may have different criticalities for different customers!

		
Telemarketing Company	<ul style="list-style-type: none">• Operators cannot make coffee during breaks (Nuisance)• Alternative: Drink water• Criticality: Low	<ul style="list-style-type: none">• Operators cannot contact customers.• No sales can be made (Critical problem)• Criticality: High
Cafeteria	<ul style="list-style-type: none">• Baristas cannot make coffee for customers (Critical problem)• Alternative: None• Criticality: High	<ul style="list-style-type: none">• Customers cannot make a reservation (minor reduction of sales)• Criticality: Low

INCIDENT MANAGEMENT



INCIDENT MANAGEMENT – MAJOR INCIDENTS

- Major Incident is a complete outage of a critical service.
- During contract negotiation, which services will be considered critical is agreed between service provider and customer.
- SLAs typically specify limits of number and total duration of Major Incidents (during reporting period)
- Exceeding these limits may result in significant financial penalties.
- Major Incidents have the highest possible priority.
- Service providers set for themselves very strict time limits for **reaction** and **resolution** (of Major Incidents).

INCIDENT MANAGEMENT

Incident Logging And Categorization

- An Incident Record, or ticket, is created
- The record contains description of the symptoms of the incident
- Incident is categorized based on the symptoms; this may later change as new information is discovered.

Handling of Major Incidents

- Special sub-process for Major Incidents

Immediate Incident Resolution by 1st Level Support

- Service Desk and 1st level operators have a collection of guidelines for solving common issues.

"Have you tried turning it off and on again?" – Please don't do this in T-Systems

INCIDENT MANAGEMENT

Incident Resolution by 2nd Level Support

- 2nd Level = multiple specialized expert functions
- These functions investigate the symptoms, discover the cause and resolve the incident
- If a configuration change is required, **Change Management** is triggered via **Emergency Change**

Incident Monitoring and Escalation

- Regularly checks progress of all open incidents and escalates as necessary.
- Please be aware of cultural differences which may hinder this critical process.

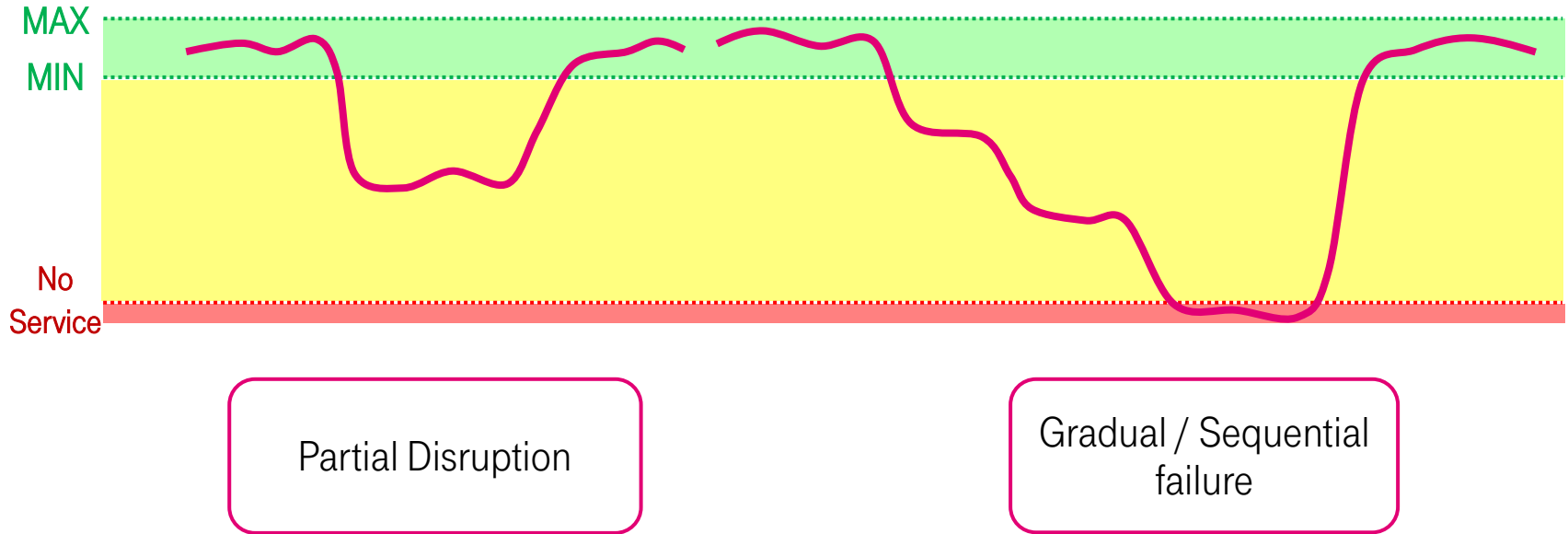
Pro-Active User Information

- If an incident may start affecting additional users or customers in the near future, this process informs such users in advance, allowing them to take mitigating action (such as saving unsaved documents, reorganizing their schedule etc.)

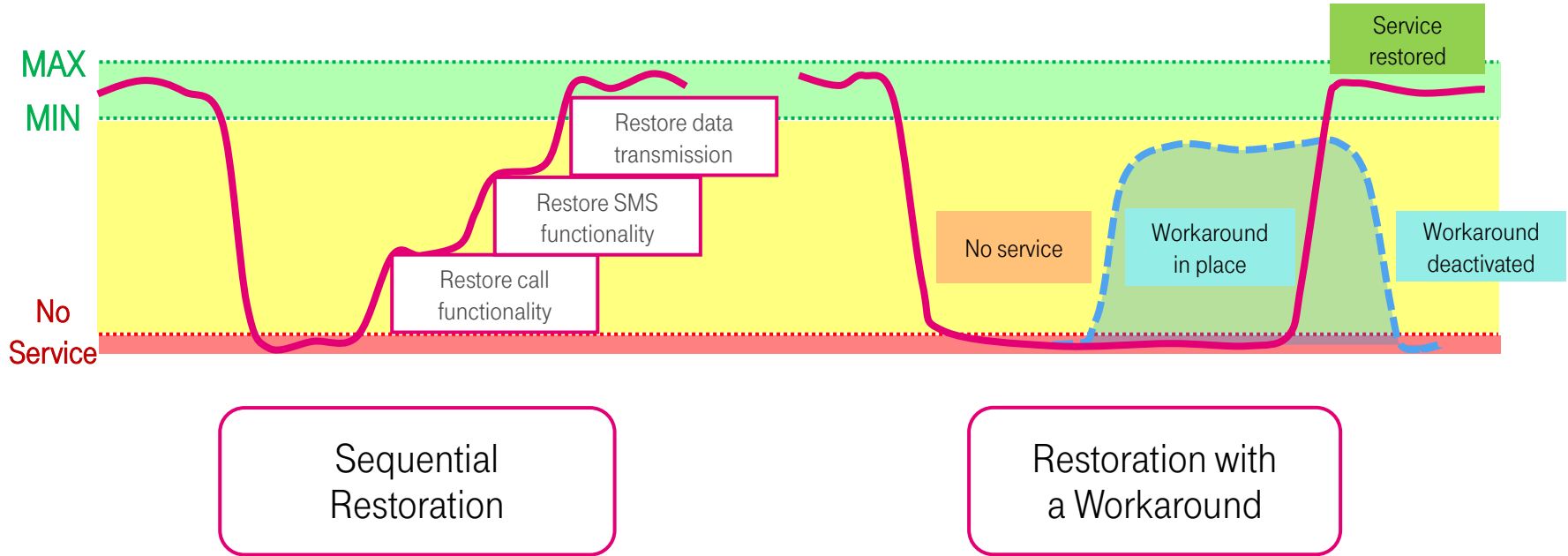
Incident Closure and Evaluation

- After verifying that the service disruption is resolved, closes the incident record.
- Performs additional actions: Triggers documenting the resolution as a guideline for future incidents, opens a Problem Ticket for deeper investigation...

INCIDENT MANAGEMENT – TYPES OF INCIDENTS



INCIDENT MANAGEMENT – TYPES OF INCIDENTS



INCIDENT MANAGEMENT – RESOLUTION WITH A WORKAROUND

Workarounds – temporary, *improvised*, fixes.

Ex. A pontoon bridge across a river near a bridge destroyed by natural disaster.

Properties of workarounds:

- Can be provided much faster than full restoration of original element
- Limited functionality (as compared to original element)
- Lowered capacity
- Lower standard of security or safety

Workarounds must not become permanent solutions.

Having workarounds prepared for expectable disasters and major incidents significantly reduces impact and damage to reputation.

INCIDENT MANAGEMENT – SUMMARY

Incident is any unplanned **service disruption** – any unplanned deviation from normal operation levels.

Disruption may be partial or complete. Complete disruption = **Service outage**.

An outage of critical service = **Major Incident**. **Handling of Major Incidents** is used for their resolution.

Goal of Incident Management is

- ✓ to **resolve incidents**...
- ✓ ... in a **coordinated manner** ...
- ✓ ... and **without causing** unnecessary **adverse effects** on other services.

Resolution ≠ Solution

Incidents may be resolved by **1st Level Support** (faster, less costly) or **2nd Level Support**.

If resolution needs **changing the configuration** of the infrastructure, a **change** will be used

If the root-cause of the incident is not known or discovered, **Problem Management** will be triggered.

SERVICE OPERATION – PRIMARY BREAKDOWN

