Incident Management

(*Intsidendihaldus*)

incident - an unplanned interruption to a service or reduction in the quality of service
Objective of the Incident Management process is to recover from the incidents and return to normal service as quickly as possible.
Incident Life Cycle

detect
register & classify
initial support
possible escalation
investigate, diagnose
repair, recover, restore
close
Incident Management

- Incidents
  - Classification
  - Detection
  - Incident DB

Problem Management

- Problem DB
  - Workarounds
  - Known Error DB
  - Analysis & Diagnosis
  - Solution, Change Proposal
  - Known Errors

Change Management

- Changes

Source: itSMF
Detecting the Incident

event from monitoring system
er user reports to service desk
incidents discovered by IT staff
Classifying the Incident

are we dealing with an actual incident?
  ➔ false alarm
  ➔ no need to take action

incident type
  ➔ fault
  ➔ service request
  ➔ need for assistance
Classifying the Incident

incident category
- hardware, software, network, people, process, documentation...

incident sub-category
- specific to your system
  - hardware - workstations, servers
  - software - operating system, application
Classifying the Incident

components affected by the incident

➔ service...

➔ ...or a physical component (configuration item)

➔ user :)

incident symptoms as described by users

➔ should not be basis for diagnosis
Initial Support

recurring incidents
obvious problems
simple assistance
incident-specific workflows

complicated incident, need for more technical assistance - escalate to next tier of support
Initial Support

recurring incidents

- is there an existing solution (workaround)?
- it is a recurring incident for you, but not always for the end user
- recurring incident is a potential problem
Investigation & Diagnosis

first time incidents

➔ first, check component status
  ➔ monitoring, events, logs
  ➔ test scripts

➔ only then, try to reproduce user's problem
  ➔ steps to reproduce
  ➔ is reproduceable?
Investigation & Diagnosis

abnormal component status
→ consult documentation for maintenance tasks
→ replace, restart

reproducible problem
→ perform real-time monitoring

no apparent cause - escalate to problem management
Resolution

- assist the user
- apply workaround
- perform maintenance tasks
- request change
Service Desk

Central point of contact between IT and users

- incident management
  - including user assistance
- communication
- educating the users
  - by providing help documentation
Incident Prevention

first contact with Service Desk is usually made only when there are some issues using the system

➔ ideally, a steady, trusted communication channel to users should be established

➔ help documentation

➔ information about oncoming changes
End User Assistance

difficulty using the system
  ➔ user is new to the system
  ➔ rarely used function
  ➔ badly designed system

service desk provides (real-time) assistance
pre-compiled help documentation can be used
Communicating

→ sensitive and critical changes
→ sensitive and critical maintenance
→ added functionality, new systems

→ multiple sysadmin teams, same communication channel
  → same format

... + improved awareness in service desk
Communicating

from users
  ➔ incident reports
  ➔ service requests
  ➔ feedback

system administrators
  ➔ workarounds,
  ➔ change and maintenance announcements
  ➔ detail inquiries
Documenting

- logging/documenting of incidents is essential
- helps with recurring incidents
- helps new service desk workers to “catch up”
- incident records are needed for incident and problem managers
- user self-training tutorials
- internal training
Types of End User Support

phone and instant messaging

→ one of the most expensive methods

→ mostly for incident registration and initial support

→ possibility to redirect

→ number of users simultaneously served is limited
Types of End User Support

self-service ticket systems

➔ interface to self-register incidents
  ➔ lower classification quality
  ➔ must re-classify?
  ➔ register through service desk, monitor the progress through ticket system
➔ high number of users simultaneously served
➔ incident management
Types of End User Support

- local support persons (per organizational unit)
- system-specific support persons
- direct support from system administrators
  - for specific, complex incidents and problems
- provider/vendor support
Types of End User Support

electronic tutorials
  - easy to change
  - relatively cheap to maintain
  - may not be accessible during the incident

printed tutorials
  - easy to read due to higher resolution
  - usable without a working computer
  - costly to produce, hard to change
System Administrators and Service Desk

- “support for user support”
- participating in writing the tutorials
- providing the input for user-IT communication
- direct support in the case of complex incidents
- service desk can be viewed as a monitoring resource
Tools for Service Desk

- incident (ticket) management systems
- remote assistance tools
- monitoring systems
- configuration management systems
Problem Management

(*Probleemihaldus*)

problem is an unknown cause of an incident
Problem Management

the main responsibility of Problem Management is to find root causes of incidents. The objective is to prevent future incidents from happening and to reduce the impact of future incidents.
Incident, Problem, Known Error

Incident, Recurring Incident, Potential Incident

Problem Management

Problem (Probleem)
unknown cause of the incidents

Known Error (Viga)
probleem või intsident, mille põhjus on teada

Workaround (Ajutine lahendus)

Change Proposal
Incident Management

*incidents* → *incident DB*

classification
detection

Problem Management

*problems* → *known errors*

analysis & diagnosis

solution, change proposal

*known errors* → *problem DB*

*problem DB* → *problem DB*

workarounds

*workarounds* → *known errors*

*Known Error DB* → *problems*

*Known Error DB* → *changes*

*changes*

Change Management
Problem Management

formal or creative process?

→ one of the most complicated processes
→ critical for providing a good service
→ experience required
→ suitable mindset required
incident, problem, known error DB

collect and elaborate on info

monitoring & docs

problem

diagnosis, finding the root cause

providing solutions

known error

specific tests

workaround solution

NOT OK

testing the solutions

OK

testing the solutions

change proposal new database records
From Incident to Problem

- recurring or high-impact incident is escalated
- incident investigation data is forwarded
  - classification
  - ability to reproduce
  - monitoring data, component status
  - which components are affected
  - which users are affected
- overall system status
Detailed Investigation

- check the failing components
- check all the dependencies
- check the logs
  - change debug/log levels
- simulate in test system

- syscall/library call trace (*koodijälitamine*)
- network sniffing (*võrgu pealtkuulamine*)
- memory/data (*andmetõmmised*)
Finding the Root Cause

- common denominator of various symptoms
- eliminating possible causes...
  - ...using logs
  - ...detail observations and tests
  - ...considering the area of impact
Finding the Root Cause

➔ connection to any recent changes?
  ➔ review all the recent changes?
➔ are there any external influences?

➔ use your experience
➔ ☺️ fantasize
➔ ☺️ perform a ritual (rain dance, sacrifice) ☺️
Providing the Solution

→ standard solutions (documented by provider)
→ solutions based on other people's experience
  → may not be a good solution
  → may not apply on our case
→ temporary workarounds

→ final solution - a (formal) change to system
Applying the Solution

- critical, because it affects the system
- think before doing (damage)
- all the steps of the solution must be justified and backed by clear evidence
- use the change management process
Testing the Solution

are the symptoms gone?
user feedback
monitoring feedback
compare data from real-time monitoring
Problem Solving: Mindsets

→ different stages need different mindsets
  → bold, creative
  → critical, strategic

→ switching between the mindsets is an art on its own
Problem Solving using Web Search

GIYF!

- how would someone describe such problem?
- searching by the error message
  - same error message may have different root causes
  - most useful when error messages are in English
  - specific error messages will find you nothing
- start with generic search, then specify