INCIDENT MANAGEMENT (INC)

WORKFLOW, TIPS & TRICKS

www.i-mokymas.com

info@i-mokymas.com

INCIDENT

- **An Incident is defined as an unplanned interruption or reduction in quality of an IT service (a Service Interruption)**

INC PROCESS DEFINITION

- ***Incident Management*** aims to manage the lifecycle of all Incidents (unplanned interruptions or reductions in quality of IT services).
- The primary objective of this ITIL process is to return the IT service to users as quickly as possible

Take a pause! Write 2-3 examples of incidents according your job experience. Post them to a course forum.

- **Incident Logging and Categorization**

Process Objective: To record and prioritize the Incident with appropriate diligence, in order to facilitate a swift and effective resolution.

- **Initial support by 1st Level Support**

Process Objective: To solve an Incident within the agreed time schedule. The aim is the fast recovery of the IT service, where necessary with the aid of a Workaround.

- **Incident Escalation**

Process Objective: transfer the Incident investigation and resolving to the most appropriate team.

- **Incident Resolution by higher Level Support (Escalation)**

Process Objective: To solve an Incident within the agreed time schedule. The aim is the fast recovery of the service, where necessary by means of a Workaround. If required, specialist support groups or third-party suppliers are involved

- **Handling of Major Incidents**

Process Objective: To resolve a Major Incident with greater urgency. The aim is the fast recovery of the service, where necessary by means of a Workaround.

- **Incident Closure**

Process Objective: To submit the Incident Record to a final quality control before it is closed. The aim is to make sure that the Incident is actually resolved and that all information required to describe the Incident's life-cycle is supplied in sufficient detail. In addition to this, findings from the resolution of the Incident are to be recorded for future use.

INC WORKFLOW SUB-PROCESSES

- **Incident Management Support**

Process Objective: ITIL Incident Management Support aims to provide and maintain the tools, processes, skills and rules for an effective and efficient handling of Incidents.

- **Incident Monitoring**

Process Objective: To continuously monitor the processing status of outstanding Incidents, so that counter-measures may be introduced as soon as possible if service levels are likely to be breached.

- **Incident Evaluation**

Process Objective: To submit the Incident Record to a final quality control before it is closed. The aim is to make sure that the Incident is actually resolved and that all information required to describe the Incident's life-cycle is supplied in sufficient detail. In addition to this, findings from the resolution of the Incident are to be recorded for future use.

- **Pro-Active User Information**

Process Objective: To inform users of service failures as soon as these are known to the Service Desk, so that users are in a position to adjust themselves to interruptions. This process is also responsible for distributing other information to users, e.g. security alerts.

SUPPORTIVE SUB-PROCESSES

INCIDENT RECORD TEMPLATE

- Unique identifier (including main request parameters, i.e. division, service, date/time)
- Name
- Service/Application
- Division/User identifier
- Memo field for user’s notes
- Attachment (if necessary)

- Think and estimate which fields are necessary for your SD template
- Are there exceeding information? Remove it from your template
- Something is missed? Add necessary attributes
- Share your template with a trainer and discuss!

LOGGING TIPS

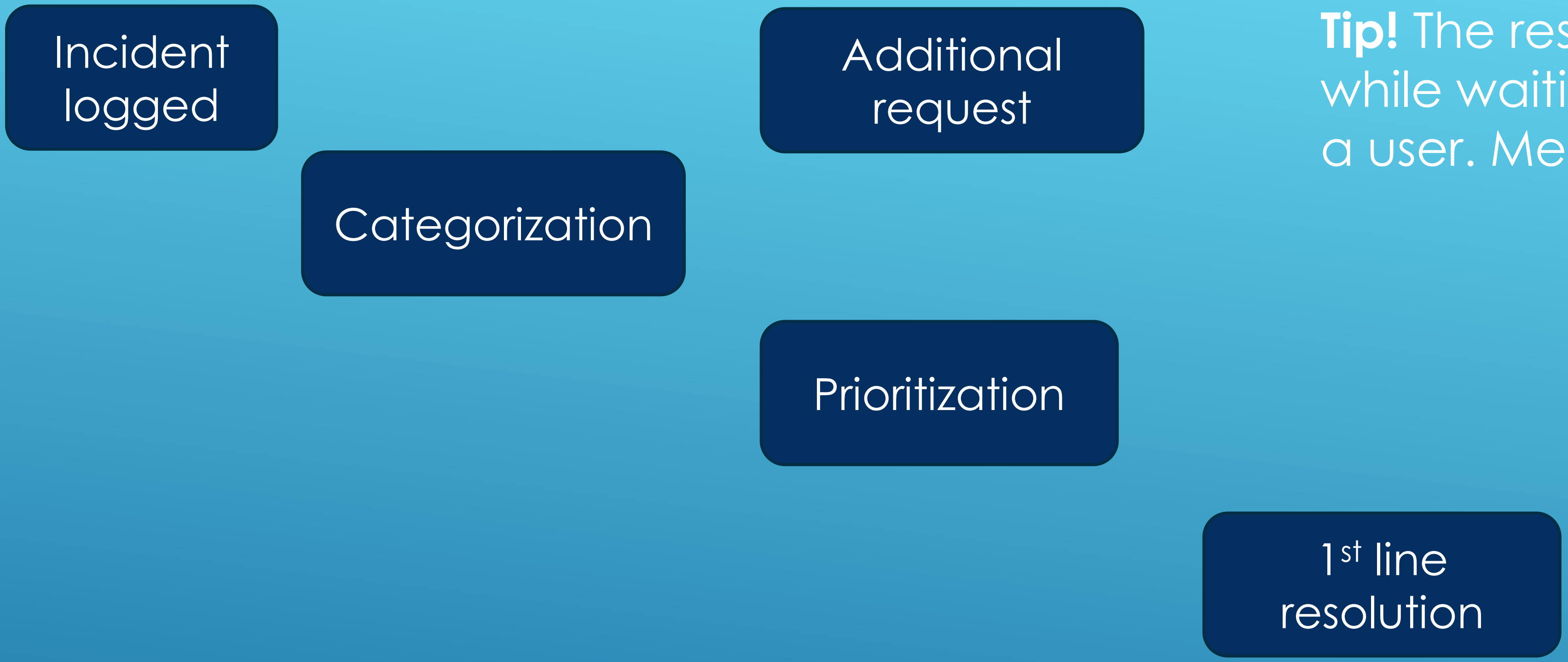
- Event management is the main source of proactive incident discovery
- Each user request MUST be logged
- Users should be provided by at least TWO technically independent tools to send requests (for example, Web form and cell phone)

- Which tools does your service desk use for users requests?
- Which tools do you consider the most appropriate?
- Why?
- Post your description at the course forum and discuss with the trainer.

CALL CENTER – HELP DESK DIFFERENCES

	Call center	Help/Service Desk
Requests logging	Yes	Yes
Incident initial diagnosis	No	Yes
Incidents initial support	No	Yes
Incident ownership	No	Yes

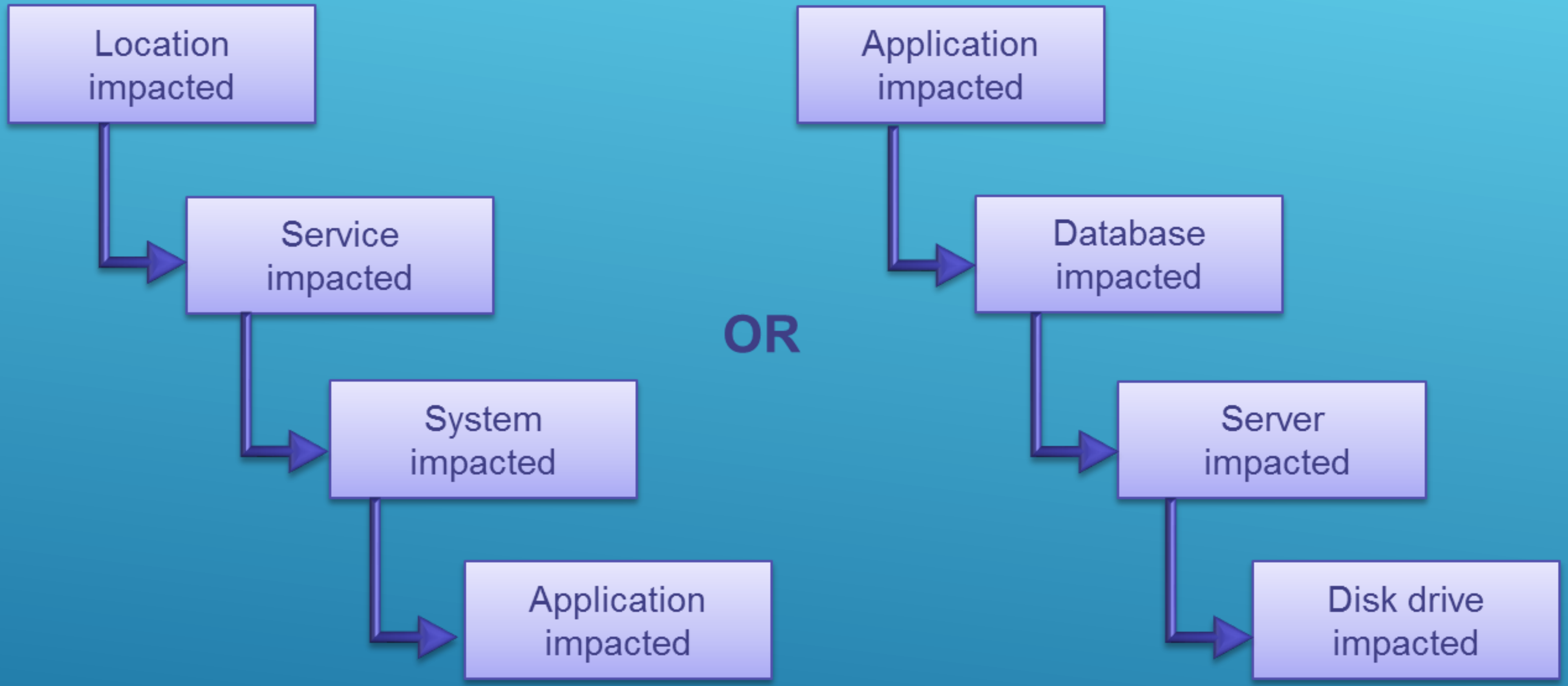
INITIAL SUPPORT



Tip! The resolution time stops while waiting an answer from a user. Mention this in an SLA

Tip! Usually 1st line operator uses Knowledge base for resolution, and is not allowed for any other actions

CATEGORIZING



Location impacted

Service impacted

System impacted

Application impacted

OR

Application impacted

Database impacted

Server impacted

Disk drive impacted

Tips!

- Defining categories is a project with high business involvement
- Automate categories in the SD system

- Give examples of categories in your IT organization
- Share them with a trainer and other mates and discuss.

IMPACT, URGENCY

Urgency	Description
High (H)	•The damage caused by the Incident increases rapidly. •Work that cannot be completed by current staff is highly time sensitive. •A minor Incident can be prevented from becoming a major Incident by acting immediately.
Medium (M)	•The damage caused by the Incident increases considerably over time.
Low (L)	•The damage caused by the Incident only marginally increases over time. •Work that cannot be completed by staff is not time sensitive. •There no enough resources for the work

IMPACT	Description
High (H)	• A large number of staff are affected and/or not able to do their job. • A large number of customers are affected. • The financial impact of the Incident exceeds a threshold. • The damage to the reputation of the business is likely to be high. • Someone has been injured.
Medium (M)	• A moderate number of staff are affected and/or not able to do their job properly. • A moderate number of customers are affected. • The financial impact of the Incident is in agreed area
Low (L)	• A minimal number of staff are affected and/or able to deliver an acceptable service. • A single customer is affected. • The financial impact is low. • The damage to the reputation of the business is likely to be minimal.

PRIORITY

Impact				
		H	M	N
Urgency	H	1	2	3
	M	2	3	4
	L	3	4	5

Priority Code	Description	Target Response Time	Target Resolution Time
1	Critical	2 minutes	1 Hour
2	High	10 Minutes	4 Hours
3	Medium	1 Hour	8 Hours
4	Low	4 Hours	24 Hours
5	Very low	1 Day	1 Week

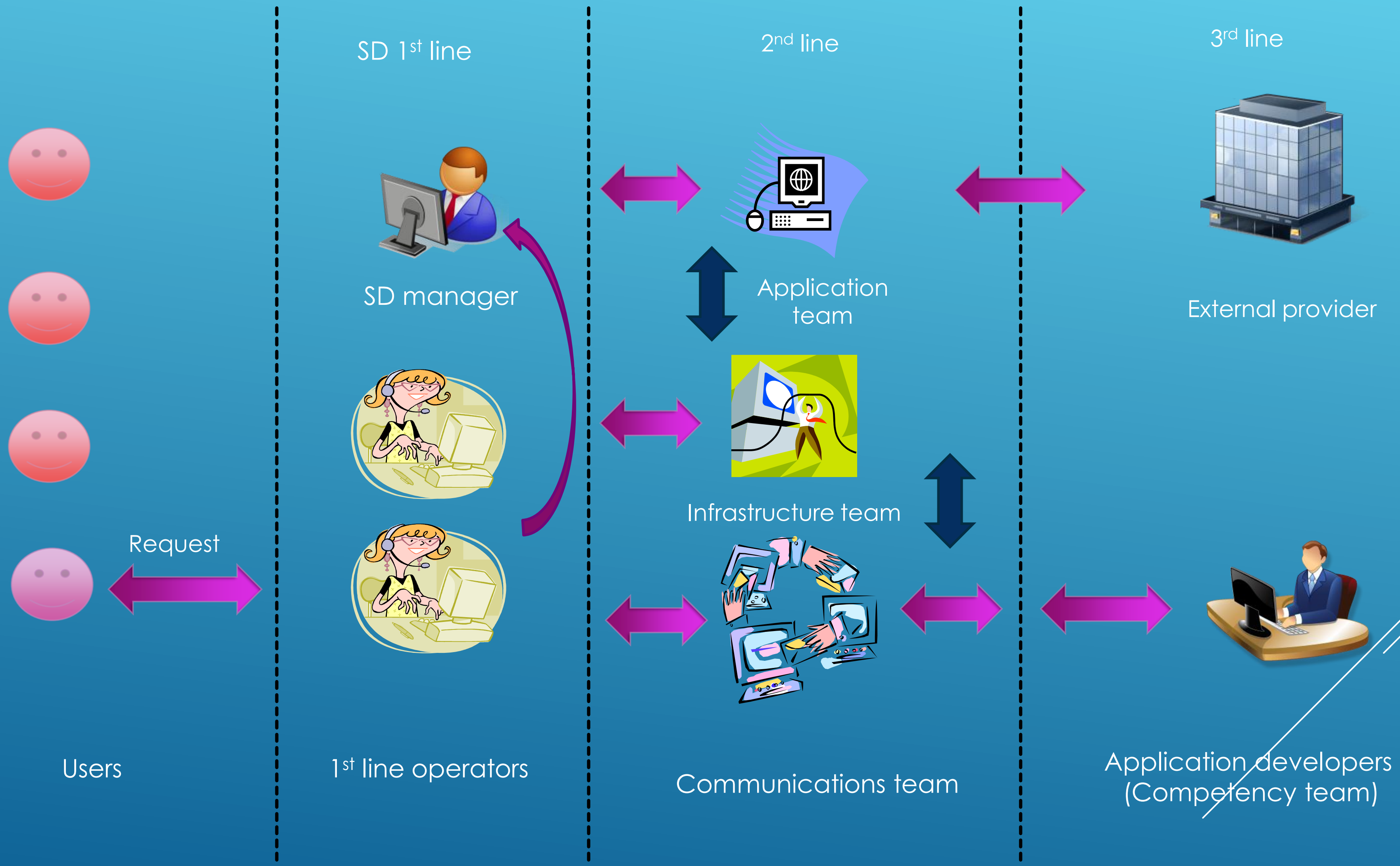
ESCALATION PROCEDURE

- Functional escalation – transfer an incident to the most appropriate team according to the functional skills and responsibilities
- Hierarchic escalation – transferring an incident to a manager for high level decision (i.e. attract more resources for high urgency incident)

Tips!

- Establish clear and precise triggers for escalation
- After incorrect escalation from the 1st line don't move an incident back. 2nd line resolves this incident
- Establish reminder rules:
    - After 70-75% time according to SLA passed send a reminder
    - After 85-90% time according to SLA passed provide a hierarchic escalation
    - Maximum number of functional escalations to prevent ping pong

ESCALATION EXAMPLE



SD 1st line

2nd line

3rd line

SD manager

Application team

External provider

Request

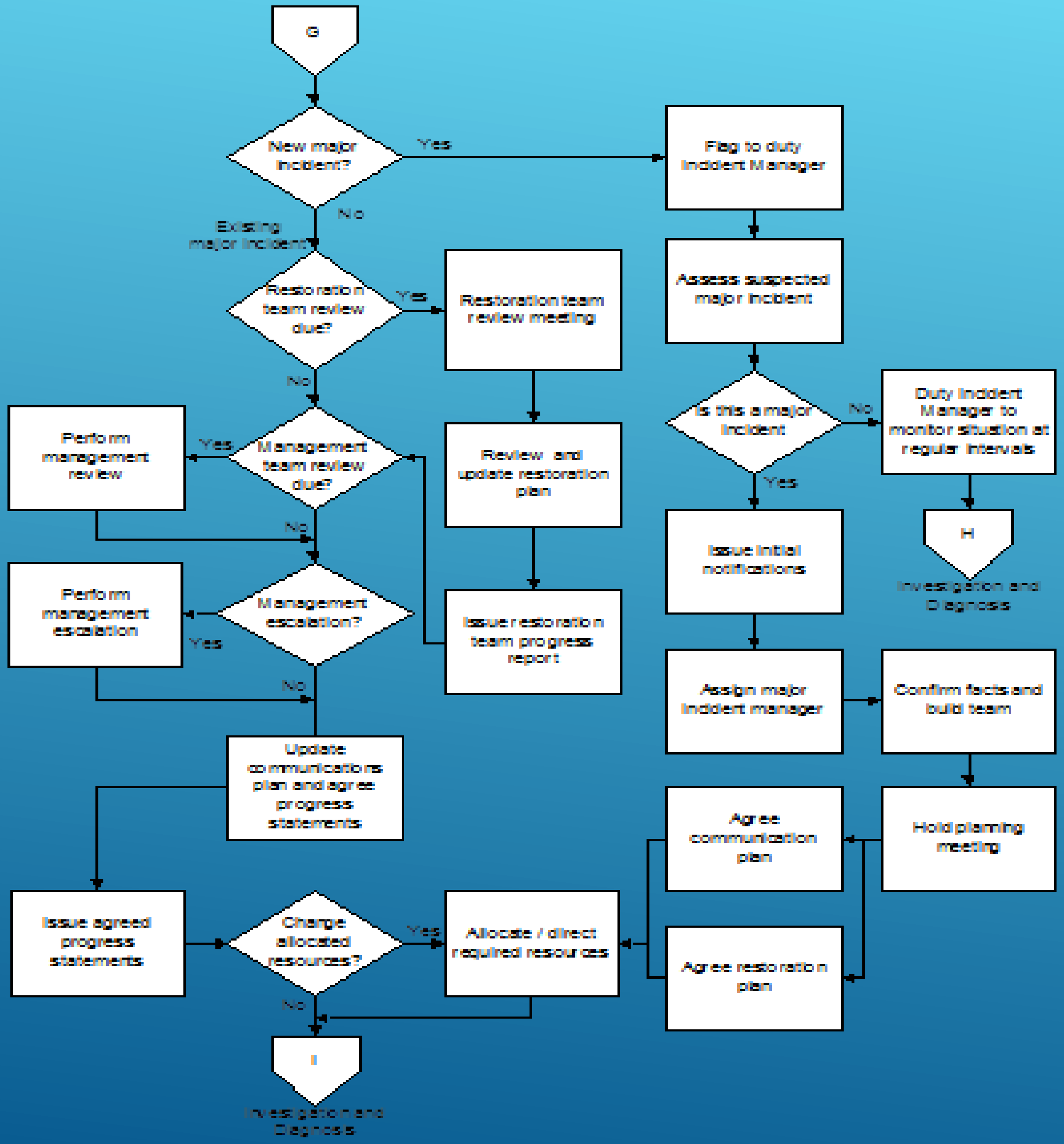
Infrastructure team

Users

1st line operators

Communications team

Application developers
(Competency team)


G
New major incident?
Yes
No
Existing major incident
Flag to duty Incident Manager
Assess suspected major incident
Restoration team review due?
Yes
No
Restoration team review meeting
Review and update restoration plan
Issue restoration team progress report
Is this a major incident
No
Yes
Duty Incident Manager to monitor situation at regular intervals
H
Investigation and Diagnosis
Perform management review
Yes
Management team review due?
No
Perform management escalation
Yes
Management escalation?
No
Issue initial notifications
Assign major incident manager
Confirm facts and build team
Hold planning meeting
Agree communication plan
Agree restoration plan
Update communications plan and agree progress statements
Issue agreed progress statements
Change allocated resources?
Yes
No
Allocate / direct required resources
I
Investigation and Diagnosis

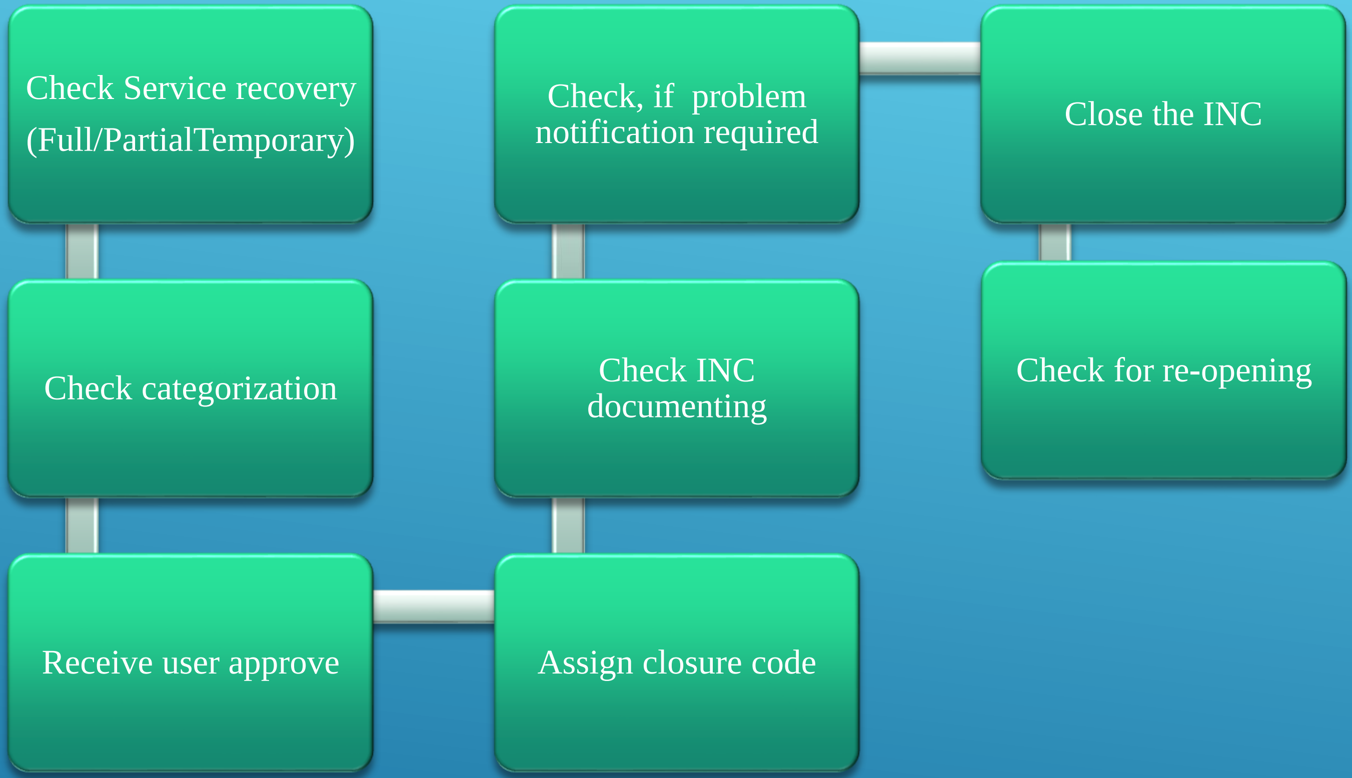
MAJOR (CRITICAL) INCIDENTS SPECIFICS

- Forum discussion: Why the special major incident procedure is necessary?

RESOLVING INCIDENTS

- Who can close an Incident in your IT organization?
- Why?
- Share your considerations at the course forum and discuss

- Resolution – a solution is found and tested
- Recovery – a solution is stored in a knowledge base and implemented



Check Service recovery (Full/PartialTemporary)

Check categorization

Receive user approve

Assign closure code

Check INC documenting

Check, if problem notification required

Close the INC

Check for re-opening

Examples of closure codes

- Fully resolved
- Workaround implemented
  - Notify PRB
- Partially resolved
  - Open new INC
- Temporal solution
  - Notify PRB or/and
  - Open another INC

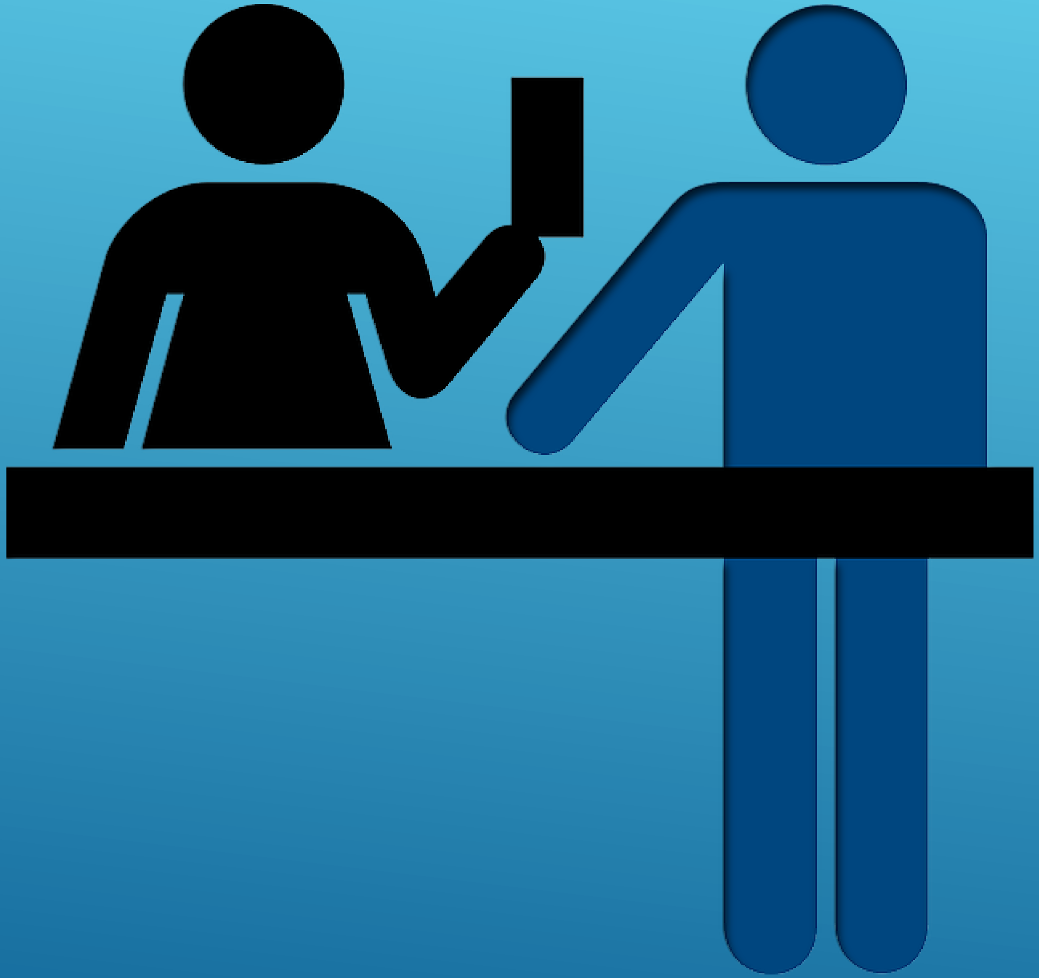
CLOSURE

- Inform users about Incidents and resolution time
- Communicate with users on additional information about their requests
- Inform users when incident is resolved
- Receive user (power user) confirmation on incident resolvement
- Estimate user/customer satisfaction

COMMUNICATING WITH USERS

- Establish INC re-open rules
- Regular reporting on metrics achieved (learn how to build SD KPIs at my course:)
- Examine customer/user satisfaction
- Analyze incidents to discover problems (PRB responsibility)
- Analyze major incidents for better solutions and identifying a problem
- Fix and share lessons learned

POST-CLOSURE ANALYSIS PRACTICES



MAIN ROLES

- Service Desk manager
- Incident process manager
- 1st line operator
- Incident analytic
- Incident resolver
- Power user (0-line support)