IT incident management

Process Definition Document (PDD): template and worked example

Example company (fictional): Tarnby Forsikring A/S, a regional insurer in Aarhus, Denmark (about 1,800 employees and 140 applications).

Document control

Field	Value
Process name	IT incident management
Process owner	[Name, role]
Prepared by	[Name]
Reviewed by	[Names of the people who do the work]
Approved by	[Name, date]
Version	1.0 (as-is)
Status	Draft

How to use this template

This is a complete process definition document (PDD) for IT incident management, also called the incident handling procedure, service desk process or IT support ticket process. It describes how a user's report of something broken becomes a logged ticket, how it is prioritised, how it moves through first, second and third line support, how a major incident is handled differently, and how it is confirmed and closed. The organisation is a fictional insurer, so the roles, systems and numbers are realistic but invented.

Use it as a starting point. Replace the company details, keep the sections, and walk through each step with the service desk agents and engineers who do the work every day. Most teams change the priority matrix, the resolution targets and the number of support lines. If you outsource the first line, mark steps 2 to 7 as performed by the provider and add the contract targets to the controls. The structure follows the incident management practice described in ITIL, but it is not a statement of ITIL certification and it must be adapted to your own service catalogue and contracts.

- Replace the company, the ITSM tool, the telephone system and the monitoring tool with yours. If you do not use ServiceNow, name the screen or queue where each step happens.
- Set your own priority matrix and resolution targets in step 4. They must be agreed with the business, because they drive the staffing of the service desk.
- Decide how many support lines you really have. Small teams often combine second and third line, and then steps 9 and 10 become one step.
- If the service desk is outsourced, mark steps 2 to 7 as performed by the provider and add the contract targets and the reporting duty to the controls.
- Define what makes an incident major in your company and who may declare it. The rule should be written down, with a named incident manager on every shift.
- Check the percentages against three months of tickets. The split by channel, the first-line resolution rate and the reopen rate are usually the most useful numbers.
- Keep the as-is version after you redesign the process. It is the baseline for measuring the improvement.

1. Purpose and scope

This procedure describes how Tarnby Forsikring restores normal IT service as quickly as possible after something breaks or degrades. It gives the service desk, the engineering teams, the incident manager and the users one shared

description of who does what, how priority is set, when an incident is escalated and when it is closed, so that every ticket has an owner, a clock and a record of what fixed it.

In scope

- Incidents reported through the self-service portal, by email or by phone
- Logging, categorisation and prioritisation from impact and urgency
- First-line resolution using knowledge articles
- Functional escalation to second and third line and to external vendors
- The major incident path, including the incident manager role and stakeholder updates
- Resolution, user confirmation, closure and the link to problem management

Out of scope

- Service requests such as new laptops or password resets by approved self-service, which follow the request fulfilment process
- Root cause analysis and permanent fixes, which belong to problem management
- Changes needed to fix an incident, which follow IT change management
- Security incidents such as suspected data theft, which are handled by the security team under their own procedure

2. Process at a glance

Item	Description
Trigger	A user reports that an IT service is unavailable, slow or not working as expected, or monitoring raises an alert.
Starts when	The user submits a report by portal, email or phone and the service desk logs a ticket in ServiceNow.
Ends when	The ticket is closed after the user confirms the fix or after three working days without a reply, and any underlying cause is linked to a problem record.
Inputs	User report with symptoms and affected service, Configuration item and service catalogue entries, Knowledge articles and known error records, Monitoring alerts, On-call rota and vendor contacts
Outputs	Resolved ticket with resolution notes and category, Updated knowledge article where needed, Major incident record and post-incident review, Problem record for repeat or unexplained incidents, Monthly incident report
Volume	About 6,500 incidents a month: roughly 55% by portal, 25% by phone and 20% by email. About 12 are escalated as major incidents each year.
Working hours	Service desk Monday to Friday 07:00 to 18:00 with an on-call engineer outside those hours for priority 1 incidents only

3. Roles and responsibilities

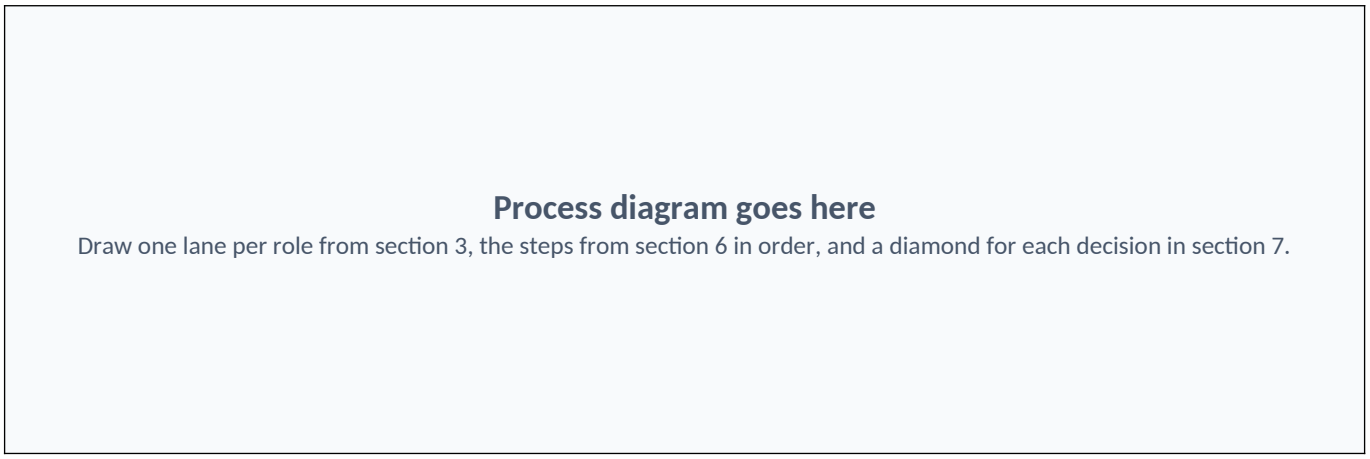
Role	Responsibilities
User	Any employee, agent or branch office worker who finds that an IT service is not working. Reports the incident with enough detail to act on, answers questions and confirms whether the fix worked.
Service Desk Agent	First line. Logs the ticket, categorises it, sets priority, searches the knowledge base, tries the documented fix and escalates when the fix does not work or the target is at risk.
Service Desk Team Leader	Watches the queue and the clocks, reassigns tickets that are stuck, checks the quality of closed tickets and reports monthly.
Second-Line Engineer	Infrastructure, application support and end-user computing engineers who diagnose incidents the service desk could not fix and apply fixes within their own area.
Third-Line Specialist	Senior engineers and application developers who investigate complex faults, read logs and code, and prepare a fix or a workaround.

Role	Responsibilities
Incident Manager	Takes ownership of every priority 1 incident. Opens the bridge call, assigns the resolver groups, decides when to invoke vendors and runs the post-incident review.
Communications Lead	Writes and sends the status updates to business stakeholders during a major incident and keeps the status page current.
Problem Manager	Reviews resolved incidents for repeat patterns, opens problem records and tracks the root cause and the permanent fix.
Vendor Support (external)	Software and hardware suppliers whose support desk is contacted when the fault is in their product. Provides a fix, a workaround or a call-back time.

4. Systems

- ServiceNow: incident records, the self-service portal, knowledge base, SLA clocks and the problem module
- Outlook shared mailbox (it-support@): incoming email, converted to tickets by an inbound action
- Genesys Cloud: telephone queue, call recording and call-back
- Microsoft Teams: major incident bridge and the stakeholder updates channel
- Zabbix: infrastructure monitoring that raises events and creates tickets automatically
- Atlassian Statuspage: internal status page for planned and unplanned outages
- Excel: monthly incident report built from a ServiceNow export

5. Process map



6. Procedure, step by step

#	Step	Who	What happens	System	Output
1	Report the incident	User	Reports the problem through the portal (55%), by phone (25%) or by email (20%). The portal form asks for the affected service, a description, the time it started and a screenshot. Phone and email reports carry less detail and take longer to log.	ServiceNow portal, email, Genesys Cloud	Report received by the service desk
2	Log the ticket	Service Desk Agent	Creates the incident from the call or the email, or accepts the portal ticket, and records the caller, the affected service, the configuration item and a clear summary in the agent's words. Logging a phone ticket takes 3 to 5 minutes. Tickets created by	ServiceNow	Logged incident with a ticket number

#	Step	Who	What happens	System	Output
			monitoring arrive already logged.		
3	Categorise and check for duplicates	Service Desk Agent	Selects the category and subcategory from the service catalogue, then searches open incidents for the same service and symptom. About 8% of tickets are duplicates of an incident already open and are linked to the parent ticket instead of being worked separately.	ServiceNow	Categorised ticket, duplicates linked to a parent
4	Set priority from impact and urgency	Service Desk Agent	Chooses impact (one user, a team or branch, the whole company or customers) and urgency (work continues with a workaround, work is blocked, a deadline is at risk). ServiceNow derives priority 1 to 4 from the matrix and starts the resolution clock: 1 hour for P1, 4 hours for P2, 2 working days for P3 and 5 working days for P4. Vague tickets are not left at a default priority.	ServiceNow	Priority and resolution target set
5	Identify a possible major incident	Service Desk Agent	If the ticket is priority 1, or several callers report the same service within 15 minutes, phones the Incident Manager on duty and flags the ticket as a candidate for a major incident. About 1 in 540 incidents is declared major. Other tickets continue to step 6.	ServiceNow, Microsoft Teams	Major incident candidate flagged, or ticket continues
6	Try the first-line fix	Service Desk Agent	Searches the knowledge base and known error records, follows the matching article with the user, for example clearing a cache, resetting a session or reinstalling a client, and records what was tried. About 62% of incidents are resolved at this step in 10 to 25 minutes.	ServiceNow knowledge base	Fix applied, or first-line steps recorded
7	Escalate to second line	Service Desk Agent	If the first-line fix fails, assigns the ticket to the correct second-line group with the steps already tried, the exact error text and the user's availability. Escalation within the first 30 minutes is expected for P1 and P2. About 31% of incidents reach second line.	ServiceNow	Ticket assigned to a second-line group
8	Diagnose and fix	Second-Line Engineer	Takes the ticket within 30 minutes for P1 and P2 or the same working day for others, reproduces the fault, checks monitoring and logs, and applies a fix within their own area, for example restarting a service, repairing a profile or replacing a device. Most second-line tickets take 1 to 6 hours of elapsed time.	ServiceNow, Zabbix	Fix applied, or diagnosis notes recorded
9	Escalate to third line or a vendor	Second-Line Engineer	If the cause is in application code, a database or a vendor product (about 7% of all incidents), reassigns the ticket to third line or opens a case with the vendor, and records the vendor case number and the agreed call-back time.	ServiceNow	Ticket with third line or vendor case reference
10	Investigate and resolve	Third-Line Specialist	Reads logs, traces the fault and prepares a fix or a workaround. If a code or configuration change is needed, raises a change request instead of editing production directly. A workaround is recorded as such, because the incident can	ServiceNow	Fix, workaround or change request

#	Step	Who	What happens	System	Output
			be resolved while the cause remains.		
11	Provide a vendor fix	Vendor Support	Replies to the case with a fix, a patch or a workaround. Vendor response is the largest source of delay: P1 cases are answered within 1 hour under contract, other cases within 1 to 3 working days.	Vendor portal, email	Vendor fix or workaround
12	Run the major incident	Incident Manager	Confirms that the incident is major, opens the Teams bridge, assigns resolver groups, keeps a timeline of actions and decides when to invoke vendors or a rollback. Checks every 30 minutes that someone owns each open action. Closes the bridge only when service is restored.	Microsoft Teams, ServiceNow	Major incident record with timeline
13	Send stakeholder updates	Communications Lead	Posts the first update within 15 minutes of the declaration and then every 30 minutes, in plain language: what is affected, what is being done and when the next update comes. Business owners of the affected service receive a direct message.	Statuspage, Microsoft Teams, email	Status updates sent and logged
14	Record the resolution	Second-Line Engineer	The resolver writes the cause (as far as known), the fix, the configuration item affected and the resolution code, then sets the ticket to Resolved. Tickets resolved without a note are the most common quality finding at the monthly review.	ServiceNow	Resolved ticket with resolution notes
15	Confirm the fix with the user	Service Desk Agent	Contacts the user by the original channel, asks whether the problem is gone and records the answer. For major incidents the agent also checks one affected branch before the bridge is closed. About 60% of confirmations are done by an automatic email that asks the user to click yes or no.	ServiceNow, Genesys Cloud	User confirmation or a reopened ticket
16	Confirm or reopen	User	Confirms that the fix works, or replies that it does not. About 6% of resolved tickets are reopened. If there is no reply, the ticket closes automatically after three working days.	ServiceNow portal, email	Confirmation or reopen request
17	Review and close	Service Desk Team Leader	Closes confirmed tickets, checks a sample of 5% each week for complete categorisation, a usable resolution note and the right priority, and turns good resolutions into knowledge articles. Reopened tickets go back to the resolver group with the user's comment.	ServiceNow	Closed ticket, new or updated knowledge article
18	Link to problem management	Problem Manager	Each week reviews the incidents that were resolved with a workaround, that repeated three times in 30 days or that were major. Opens a problem record, links the incidents and assigns an owner for root cause analysis. About 25 problem records are opened a month.	ServiceNow problem module	Problem record linked to incidents, or no action

7. Decision points and business rules

- Is the report complete enough to log? No (about 15% of phone and email reports): the agent asks for the missing detail before categorising (step 2).

- Is the ticket a duplicate of one already open? Yes (about 8%): link it to the parent and update the user from the parent (step 3).
- How high are impact and urgency? The matrix sets priority 1 to 4, which sets the resolution target and the escalation timing (step 4).
- Is it priority 1, or are several users reporting the same fault? Yes: call the Incident Manager at once (step 5).
- Did a knowledge article fix it? Yes (about 62%): resolve at first line. No: escalate to second line with the steps tried (steps 6 and 7).
- Is the cause in code, a database or a vendor product? Yes (about 7%): third line or vendor case (step 9).
- Does the fix need a change to production? Yes: raise a change request and record the incident as resolved by workaround only if service is restored (step 10).
- Did the user confirm that the fix works? No (about 6%): reopen the ticket and return it to the resolver group (step 16).
- Did the incident repeat, end in a workaround or count as major? Yes: open a problem record (step 18).

8. Exceptions

- A VIP or branch manager calls with a priority 3 problem (about 4%): the priority is set by impact and urgency, not by the caller's seniority, but the team leader may assign an engineer directly.
- Incident outside service desk hours (about 3%): only P1 reaches the on-call engineer. Other reports are logged by the portal and picked up at 07:00.
- User cannot be reached for confirmation (about 9%): two attempts on different days, then the ticket is resolved and closes automatically after three working days.
- Resolution target missed because a vendor has not replied (about 2%): the clock is paused only with the team leader's approval and the reason is recorded.
- Security concern appears during diagnosis (about 1%): the ticket is handed to the security team and the incident manager is informed.

9. Controls

- Every incident has a category, a priority, an owner group and a resolution note before it can be closed. ServiceNow blocks closure when a field is empty.
- Priority is derived from the impact and urgency matrix and cannot be changed by the resolver without a written reason.
- Every priority 1 incident has a named incident manager and a timeline, and a post-incident review within 5 working days.
- Pausing an SLA clock needs team leader approval and a recorded reason. The reasons are reviewed monthly.
- The team leader reviews a 5% sample of closed tickets every week and records the result.
- Access to close and reopen tickets is limited to the service desk and resolver groups. Users cannot close tickets they did not raise.

10. Known issues today

- Phone and email reports often miss the affected service and the time the problem started, so agents ask the same questions every time.
- Priority is sometimes set by the caller's tone rather than by impact and urgency, which overloads second line with P2 tickets.
- Knowledge articles are out of date and about 1 in 5 first-line searches finds nothing useful.

- Tickets bounce between second-line groups when the category is wrong, and the user is not told.
- Vendor cases are tracked in email, so the call-back time is not visible in the ticket.
- Resolution notes such as 'fixed' give the problem manager nothing to work with.

11. RACI matrix

R = responsible (does the work), A = accountable (owns the outcome), C = consulted, I = informed.

Activity	User	Service Desk Agent	Team Leader	Second Line	Third Line	Incident Manager	Comms Lead	Problem Manager
Report and log the incident	R	A/R	I					
Categorise and set priority	C	R	A			I		
First-line fix	C	A/R	I					
Diagnose and fix at second line	C	I	A	R	C			
Investigate at third line or with a vendor		I	I	A	R	C		
Run a major incident	I	C	C	R	R	A	R	I
Communicate to stakeholders	I	C				A	R	
Confirm resolution and close	R	R	A	I				
Link to problem management		I	C	C	C	C		A/R

12. KPIs

KPI	Definition	Target
Resolution within target	Share of incidents resolved within the target for their priority, measured per priority and not as one blended figure.	[set]
First-line resolution rate	Share of incidents resolved by the service desk without escalation. Today about 62%.	[set]
Reopen rate	Share of resolved incidents the user reopened. Today about 6%.	[set]
Average time to first response	Average minutes between the ticket being logged and the first human contact with the user, split by channel.	[set]
Major incidents and their duration	Number of major incidents in the month and the average minutes from declaration to restoration.	[set]
Tickets with a usable resolution note	Share of the weekly sample whose resolution note names the cause and the fix. The target is 95%.	[set]

13. Revision history

Version	Date	Author	Change
1.0	[date]	[name]	First as-is version

Free template from processfix.ai. You may copy and adapt it. The company in the example is fictional.