ITSM TOOLKIT · V1.0

Practitioner Starter Kit

Field-tested templates and a one-page incident management overview for enterprise IT operations.

BUILT BY ITSM PRACTITIONERS

Lou DeLuna · IT Service Delivery Leader
kcitsmtoolkit.com

ABOUT & METHODOLOGY

Built from real operations.

The ITSM Toolkit is a working library of frameworks, templates, and operating models created by an IT Service Management practitioner with two decades of experience leading enterprise operations. Every artifact in this kit is shaped by one rule: **if it doesn't survive a live incident bridge, it doesn't belong here.**

What it helps you do

- Stabilize incident management and reduce escalation noise
- Improve major incident response with clear roles and cadence
- Run honest post-incident reviews that drive measurable change
- Communicate with executives without theatrics
- Scale service delivery without unnecessary complexity

Translation layer

Framework	Real-world application
ITIL 4	Incident prioritization that teams actually follow.
ISO/IEC 20000	Governance that doesn't stall execution.
COBIT	Control without bureaucracy overload.

> *“This kit reflects the systems relied on during real outages, real escalations, and real operational turning points.”*

ONE-PAGE OVERVIEW

Incident Management at a Glance

Purpose: Restore normal service operation as quickly as possible and minimize the adverse impact on business operations.

Lifecycle

Stage	Goal	Key Output
Detect	Identify and capture the incident.	Ticket created with impact & urgency.
Triage	Assess scope, classify priority, route.	Priority assigned (P1–P4).
Respond	Mobilize resources, contain, restore.	Service restored or workaround active.
Communicate	Keep stakeholders informed on cadence.	Status updates per priority cadence.
Resolve	Confirm restoration with the business.	Resolution code & user confirmation.
Review	Learn and improve.	PIR for P1/P2; trend analysis ongoing.

Operating principles

- **Restoration first, root cause second.** Stop the bleeding before debugging.
- **Separate emotion from severity.** Volume of complaints ≠ business impact.
- **Single source of truth.** One bridge, one ticket, one comms channel.
- **Cadence over chatter.** Scheduled updates beat ad-hoc noise.
- **Every P1/P2 earns a PIR.** Improvement is non-negotiable.

Common anti-patterns to avoid

- Priority inflation driven by the loudest stakeholder
- Engineers debugging in silence while the business waits in the dark
- PIRs that name people instead of fixing systems
- Untracked workarounds that quietly become permanent

TEMPLATE

Priority Matrix (P1–P4)

Use Impact × Urgency to assign a priority. Treat the matrix as the default, not the ceiling — document any override with a one-line rationale.

Impact ↓ / Urgency →	High	Medium	Low
High	P1	P2	P3
Medium	P2	P3	P3
Low	P3	P3	P4

Priority	Definition	Target Response	Update Cadence
P1 — Critical	Critical service down or severe degradation; significant business impact.	15 min	Every 30 min
P2 — High	Major function impaired; workaround limited or unavailable.	30 min	Every 60 min
P3 — Moderate	Non-critical issue; workaround available; limited impact.	4 hours	Daily
P4 — Low	Minor issue, request, or cosmetic defect.	Next business day	On change

Targets shown are illustrative starting points. Calibrate against your service catalog, contractual SLAs, and operating hours.

TEMPLATE

Major Incident: Roles & Cadence

Bridge roles

Role	Responsibility
Major Incident Manager (MIM)	Owns the bridge. Drives cadence, decisions, and clarity. Single point of accountability for restoration.
Technical Lead	Coordinates engineering teams, sequences diagnostic and recovery actions, owns the technical timeline.
Communications Lead	Drafts and issues stakeholder updates on cadence. Shields engineers from inbound noise.
Executive Liaison	Translates status for leadership. Surfaces business impact, decisions needed, and risk.
Scribe	Captures timeline, decisions, and actions in real time — the basis for the PIR.

Communication cadence

Trigger	Audience	Channel	Cadence
MI declared	All stakeholders + execs	Email + status page	Within 15 min
Active response	Stakeholders	Status page / email	Every 30–60 min
Executive checkpoint	Leadership	Bridge / call	Hourly
Service restored	All stakeholders	Email + status page	Within 15 min
PIR published	Affected business + IT	Document + meeting	Within 5 business days

TEMPLATE

Post-Incident Review (PIR)

Use this skeleton for every P1 and P2. Focus on systems and decisions, not individuals. Every PIR must produce at least one assigned, dated action.

Section	Content
Incident summary	One paragraph: what happened, who was affected, duration, business impact.
Timeline	Chronological log of detection, escalation, key decisions, actions, and restoration. Include timestamps.
Impact	Users affected, services degraded, transactions lost, revenue or SLA exposure, reputational risk.
Root cause(s)	Technical root cause, contributing factors, and the underlying systemic issue. Use 5-Whys or fishbone if useful.
What went well	Behaviours, tools, or decisions that accelerated restoration.
What didn't	Gaps in detection, response, communication, or tooling. Be specific, not personal.
Action items	Owner, due date, and acceptance criteria for each. No action without a name and a date.
Follow-up	Where the actions will be tracked and when status will be reviewed.

TEMPLATE

Stakeholder Communication

Three message types cover most of the lifecycle. Keep each one short, factual, and free of speculation.

1. Initial notification

Field	Content
Subject	[P1 / P2] <Service> — service disruption
What is happening	Plain-language description of the issue and observable symptoms.
Who is affected	Locations, business units, or user groups impacted.
What we are doing	Current action; resources engaged; bridge active.
Next update	Specific time the next update will be sent.

2. Status update (recurring)

Field	Content
Status	Investigating / Identified / Mitigating / Monitoring
What changed	Concrete progress since the previous update.
Current impact	Who is still affected and how.
Workaround	If available, clear instructions; otherwise state “none at this time.”
Next update	Specific time. Always set a next time.

3. Resolution

Field	Content
Status	Service restored at <timestamp>.
What was done	Brief description of the corrective action.
Residual risk	Any monitoring still in place or known limitations.
Next steps	PIR scheduled; how affected parties can report lingering issues.

Tone: factual, calm, and consistent. Avoid blame, jargon, and speculation. If you don't know, say so — and say when you'll know more.

USE & ADAPT

Make it yours.

These templates are starting points, not a contract. Adapt cadence, thresholds, and language to fit your operating model, regulatory environment, and the maturity of your teams.

Recommended next steps

- Pilot the priority matrix with one service area; tune thresholds after 30 days.
- Run a tabletop exercise using the bridge roles and cadence template.
- Adopt the PIR skeleton for the next two P1/P2 events and compare insight quality.
- Wire your existing stakeholder lists into the three communication templates.

Disclaimer. The frameworks and templates in this kit are general in nature and informational. They align with established ITSM practice (ITIL 4, ISO/IEC 20000, COBIT) but should be adapted to your organization's specific operating model, regulatory requirements, and technical environment.

About the author. Lou DeLuna — IT Service Delivery Leader and ITSM practitioner with 20+ years building, scaling, and stabilizing enterprise IT operations. linkedin.com/in/loudeluna