Incident Management *Playbook*

Components of effective incident management

WHAT DO YOU NEED?

An effective incident response doesn't begin when an attack is detected—it begins long before, with careful preparation. The ability to respond quickly and decisively depends on having the right structures, policies, and people in place ahead of time.

This playbook is designed to help you build that foundation. Rather than focusing on actions during an incident, it guides you through the steps you need to take before something goes wrong: defining clear ownership, setting up escalation paths, aligning with regulatory requirements like NIS2, and ensuring forensic readiness. This playbook covers four key components of incident management:

Context : Why should you care about incident management?

Initiation: When should you trigger the incident management process?

Process: Which steps should you take, and how should you document them?

People: Who should be involved, and how are roles and responsibilities defined?

Breached? Call our emergency hotline: +31 70 222 0000

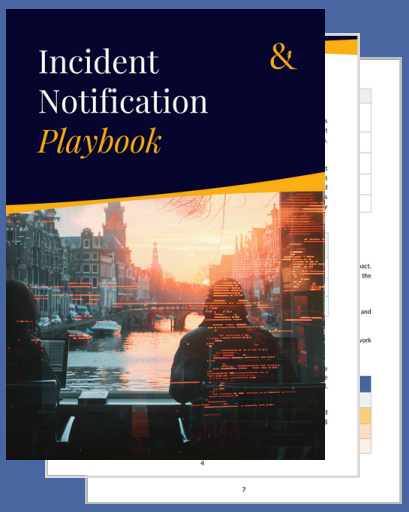
Raison d'être

WHAT YOU'LL LEARN

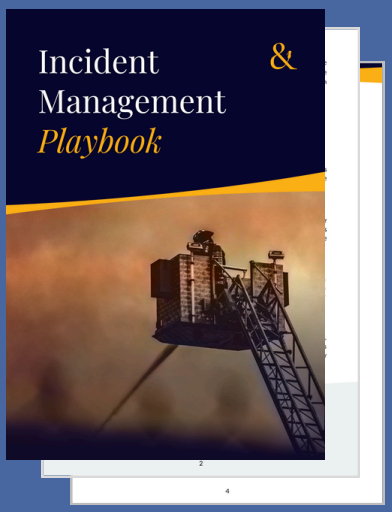
This playbook is your practical guide to incident management, focusing on how to classify, manage, and investigate security incidents. It will help you understand incident classification, assign owners, and set up internal teams based on technical expertise and process needs. Special attention is given to identifying critical assets and their owners, as well as ensuring the availability of logging and telemetry data to support forensic readiness. You'll find structured guidance on stakeholder coordination using tools like the RACI matrix, helping you maintain clarity and control throughout the process.

As the second part of our three-piece series; 1) Notification Management, 2) Incident Management, and 3) Crisis Management, this playbook focuses on the phase after an incident has occurred, when effective management is essential to limit impact and restore operations. It also supports compliance with legal and regulatory obligations such as NIS2, which demand timely reporting and thorough investigation.

Part 1



Part 2



Part 3

Introduction to Incident Management

WHAT DOES IT ENTAIL?

Cyber incidents are no longer rare, isolated events; they have become an operational certainty. This playbook will provide a repeatable, auditable, and NIS2-ready framework for handling those incidents from the moment an alert is raised until normal operations are safely restored. By the end, you will know:

- **How to recognise and classify an incident** so that the right level of response is triggered.
- **Who owns what**—from legal counsel through technical responders to external authorities—and how to reach them fast.
- **Which assets matter most**, who their custodians are, and how to involve third-party hosts when seconds count.
- **How to keep every stakeholder informed** through a clear RACI matrix that prevents both panic and silence.

The result: faster containment, deeper root-cause analysis, fewer regulatory headaches, and a measurable reduction in business impact.

Background

Why should you care about incident management? Well, when a cyber incident hits, the clock starts ticking—not just in terms of technical containment, but for business recovery as a whole. How quickly and effectively an organization can respond often determines whether a disruption is minor or catastrophic.

Incident management is the bridge between detection and recovery. It ensures that key decisions are made with speed and clarity, that the right people are involved from the start, and that the organisation can maintain control even in high-pressure situations. And as regulations like NIS2 and DORA raise the bar for cyber resilience and reporting, organisations must not only be ready to act, but able to prove it.

The impact of NIS2

The EU's NIS2 Directive will significantly tighten the screws on incident handling and reporting. Organisations deemed *Essential* or *Important* will have just 30 days after the start of an incident to submit a detailed report, including root cause analysis, to the relevant authority. This requires companies to have strong incident readiness, forensic readiness, and incident management processes in place. An overview of the ambitious incident reporting timelines can be seen in *Figure 1* below. Late or incomplete submissions could carry hefty administrative fines and, under upcoming Dutch implementation (Cyberbeveiligingswet), potential public disclosure of non-compliance.

Figure 1 - NIS2 incident reporting timelines

Initiating the incident management process

As soon as an incident has been reported, the incident notification process transfers into the incident management process. This means that at this point in the incident, it has been registered and assigned a classification level. Depending on the severity of the incident, it may be necessary to further escalate the incident when it turns into a crisis. This flow is shown in *Figure 2* on the next page.

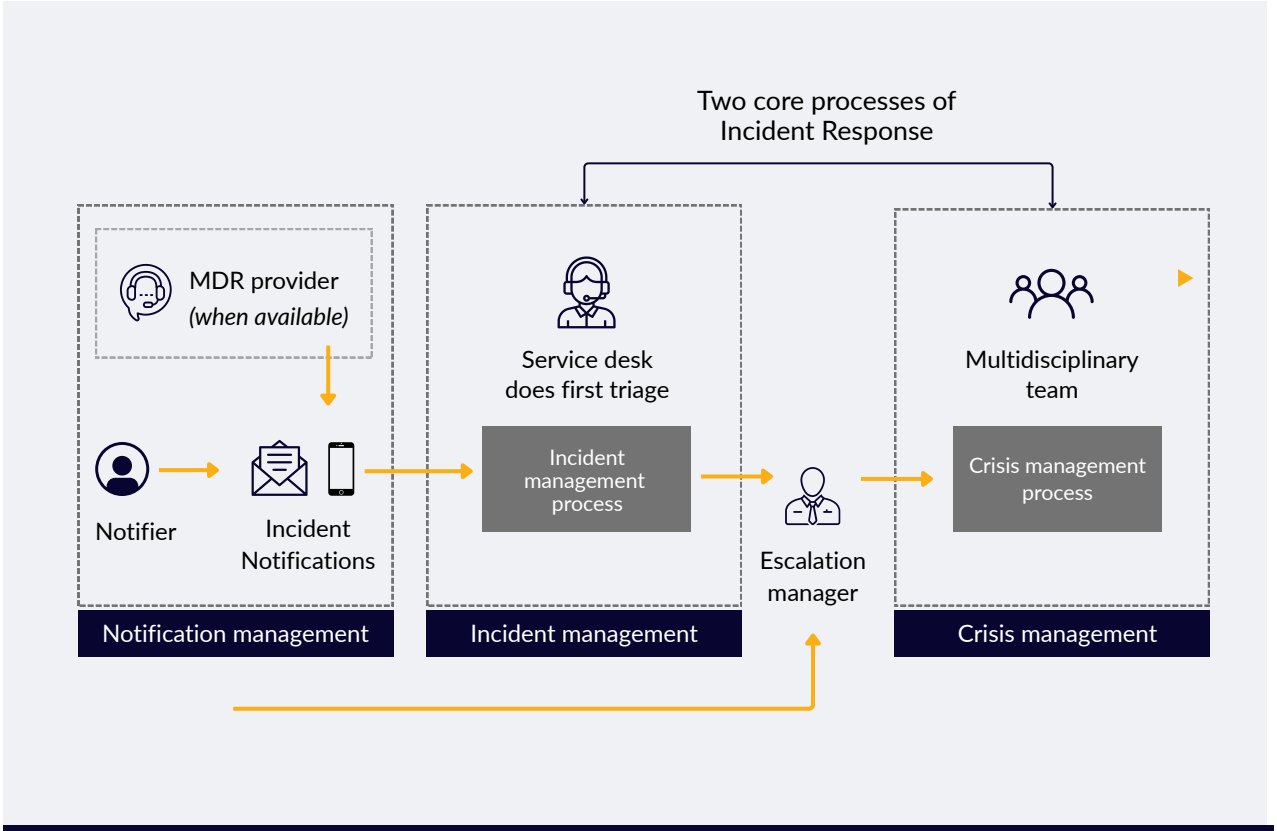


Figure 2 - General incident management process

Crisis Management

More about crisis management procedures and processes will be discussed in the Crisis Management Playbook. If the incident is priority 1 or 2, it is escalated to an escalation manager - this could be a separate role or a shared responsibility with, for instance, the IT manager - who will then kickstart the crisis management team. If the incident has a priority of 3, 4, or 5, it will be handled by the incident management team.

Incident Management Checklist

WHAT DO YOU NEED TO DO?

Setting up an incident management process

This section outlines the things you need to do to ensure that there is an incident management process in place. This overview can be found in *Table 1*. The table indicates the identifier, a description of the item, whether it has been implemented (including date/time), what the risk indication is if it is not implemented, and how an item compares to the corresponding safeguards of CIS control 17. While it's recommended to implement each individual action item, you may not be able to do so due to time constraints or conflicting business priorities. *Table 1* is therefore a reminder and to-do list to check if each individual component has been documented or will have to be.

#	Action	Finish date	Comments	CIS Control safeguard
IM01	An incident classification scheme is available			17.9
IM02	Create a process to classify the incident and assign an owner to this process			17.3, 17.5
IM03	*If applicable:* Create a list of escalation managers with contact information			17.2, 17.5
IM04	Create a list of crisis management touchpoints with contact information			17.2, 17.5
IM05	Create a list of critical business and IT assets, along with their owners (external and/or internal)			17.9
IM06	Create a technical cheat sheet or battlecard for the most common incidents containing initial do's and don't's.			17.3
IM07	Practice the entire incident management process on a regular basis.			17.7

Table 1 - Incident classification checklist

Incident Management Teams

WHO IS INVOLVED?

Setting up the incident management team

An incident playbook is only as strong as the people who can put it into action. The Incident Management Team is the engine room of the response: a cross-functional group that owns every minute from detection through recovery and post-mortem. This page explains who must be on that team, when they are activated, and how you keep their details at your fingertips—no matter what time the phone rings. In the Notification Playbook you have created a classification model. Based on this model ranging from Low to High, the composition of the incident management team might differ. In smaller organisations, a single individual may be responsible for multiple roles. *Table 2* below provides an outline as to which expertise could be involved in effectively handling the corresponding incidents.

Classification	Command Role	Core Specialists	Extended Specialists	Governance & Oversight
Low	Incident handler	SOC analyst, relevant SysAdmin	-	-
Medium	Senior incident handler	Network & Endpoint leads, DFIR analyst	Legal, privacy, comms	CISO
High	Crisis manager (executive level)	All technical leads, Forensics lead	PR/Comms lead, HR, Finance, supply chain manager	CEO/Board

Table 2 - Classification & team composition

Who to contact

Now that you know which expertise to involve, it is time to start calling. Therefore, this section provides an overview of the internal team(s). Depending on the continents and time zones where the organization is located, the incident response team can be divided into one or multiple teams. *Table 3* provides an overview of the process owner for the incident management process and his/her backup.

	Incident management process owner	IM process owner backup
Name		
Telephone number		
Email address		

Table 3 - Overview of the incident management process & backup

Internal team

The internal team consists of multiple people in different roles. Please note that IT Director does not actively work on incidents and is only informed and consulted. This section provides an overview of the entire internal incident management team, including roles and contact information.

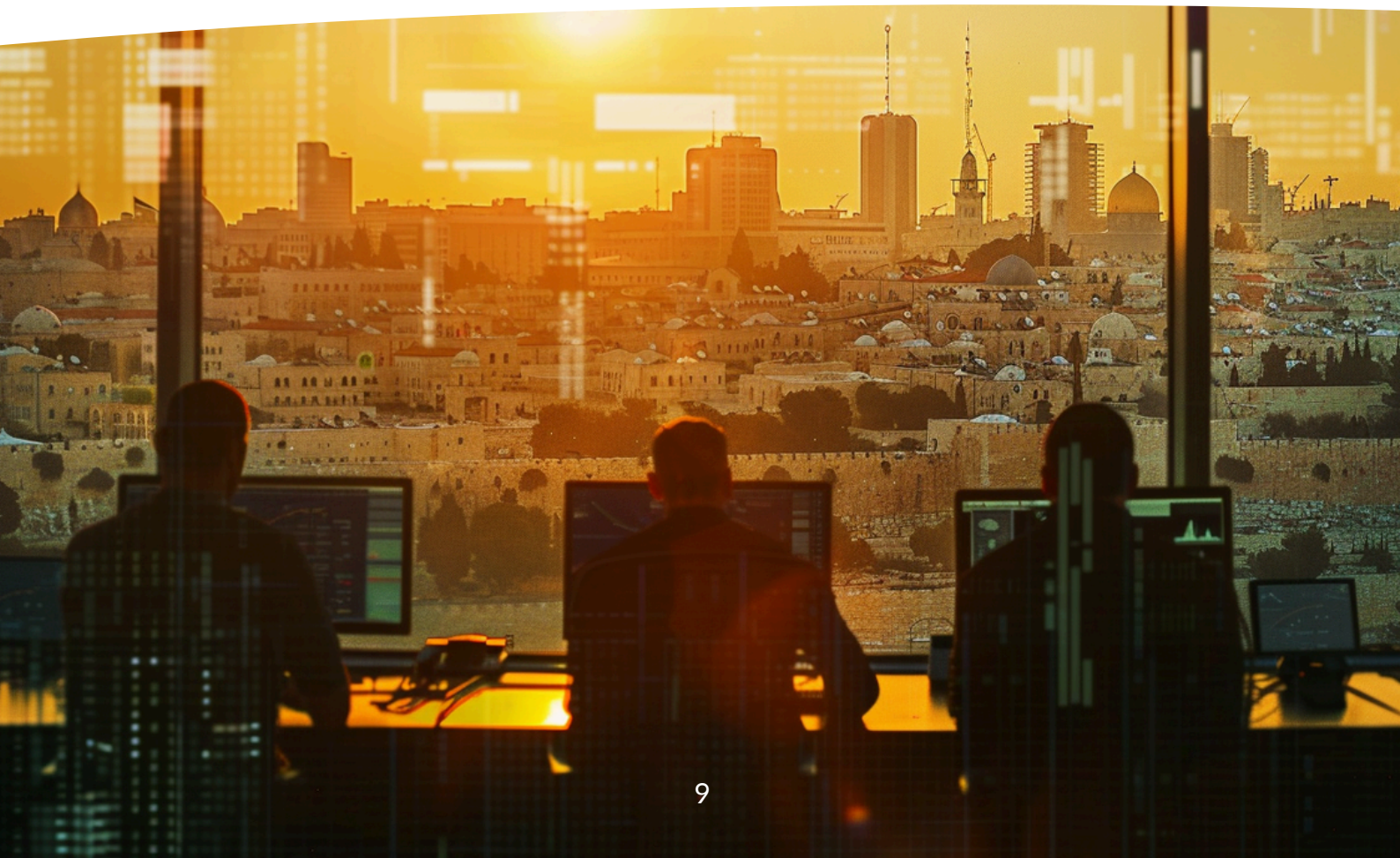
The importance of an internal management team

With the right people, ready at the right time, you transform your playbook from a policy document into an operational weapon—one that meets NIS2's 24 / 72-hour reporting deadlines **and** limits business disruption when real-world attackers come knocking. The table below provides an initial composition of the internal incident management team. Depending on the type of incident, phase of the attack/incident, and possibilities for rapid containment, the composition of this internal team can be adapted. In addition, the source of and technical context surrounding the incident is relevant. For instance, if the incident originates from or occurs within a cloud environment, it could be wise to include Cloud/SaaS expertise in the incident management team. Another example is when the incident evolves into a fraud investigation, or when it is espionage related. Then it could be wise to include digital forensics expertise early on in the investigation.

Team documentation

Role	Name
IT manager (or incident lead)	
Legal / General Counsel (see RACI)	
***If applicable*: External CERT**	
Technical support networking	
Technical support endpoints	
Technical support (other)	

Table 3 - Overview of the incident management process & backup



RACI Matrix

WHO IS INVOLVED?

A RACI matrix defines who is responsible, who is accountable, who should be consulted, and who should be kept informed during an incident, depending on the system, department, or business process that's been impacted. On the next page, a template is provided for filling in such a matrix.

- **R = Responsible:** Executes the task's concrete actions—collect logs, isolate a server, draft the press release, whatever "gets it done." Allow multiple 'R's, but designate a lead. Mind set should be: Task-oriented, detail-obsessed, and deadline-aware; they live in playbooks and ticket queues.

- **A = Accountable (also approver or final approval authority):** Owns the outcome—quality, timing, and impact. They sign off on every major decision and report upward, and delegate the work to those responsible. Only one assignee may be specified for each task or deliverable. Multiple Accountables = no Accountable. With a Big-picture strategist mindset, someone who balances risk, speed, and resources; must stay calm under fire

- **C = Consluted (sometimes consultant or counsel):** Those whose opinions are sought, usually subject matter experts; and with whom there is two-way communication. With a collaborative and responsive mindset. Include 'C's only where their domain truly matters; prune the list mercilessly

- **I = Informed:** Those who are kept informed of progress, often only after task completion or deliverable, and with whom there is only one-way communication. Stay in the loop so they're never surprised—Board members, HR, peripheral IT teams, regulators. Set an update cadence sharing with 'I's and stick to it; surprises breed distrust faster than breaches do.

Incident Management Activity	IT	Management	Legal	HR
Informing employees				
Informing management				
Conducting investigation				
Execute recovery plan				

Table 4 - RACI Matrix

Add additional incident management activities based on the features of your own organisation and the incident at hand

Conclusion

This playbook has outlined a practical approach to handling incidents in a way that supports recovery, minimizes impact, and meets growing legal obligations such as NIS2. But a plan on paper is only as strong as its execution. Regular practice, review, and alignment across teams are essential to keep your response capabilities sharp.

While incident management helps you regain control, some situations will call for a broader, organisation-wide response. That's where the next part of this series comes in—the Crisis Management playbook focuses on navigating high-impact scenarios where business, reputation, and leadership are on the line.

HUNT & HACKETT

Hunt & Hackett was founded in 2020 by Ronald Prins (co-founder Fox-IT) and Jurjen Harskamp (former executive Fox-IT). Hunt & Hackett is a privately-owned Dutch company based in The Hague, the Netherlands, and governed by stringent national and European standards on privacy and security. A fast-growing team of highly experienced security specialists and upcoming talents is protecting customers against their sector- and organisation-specific threat landscape, including the most sophisticated APTs.

Want to know more?

Join one of our CyberConnect roundtables

Questions or want to get in touch?

+31 70 22 0000

info@huntandhackett.com

www.huntandhackett.com