ONTIC

CHECKLIST

Incident Management Program Assessment for Enterprise Physical Security Teams

If you're part of a global enterprise, you know incident management is rarely simple. One day, it's severe weather or a workplace altercation; the next, it's a protest outside a facility, a suspicious package, or even something as simple as an unlocked door. With teams spread across regions, achieving consistency in capturing, investigating, and resolving these incidents is a constant challenge.

Too often, key details are buried in siloed systems or lost in email threads. Responses slow down, risks persist, and repeat issues aren't prevented. The result: You struggle to show security's impact on business outcomes.

When done strategically, incident management becomes more than just reacting quickly. You reduce costs, minimize disruption, and protect your people and brand. You also transform data into a powerful advantage — preventing repeat issues and demonstrating measurable business value.

Incident management maturity

Before evaluating whether your program is truly operating at a strategic level, it's important first to understand the key phases of incident management program maturity:

- **Ad hoc:** Incidents are tracked in spreadsheets or emails, intake is inconsistent, and response times are slow.
- **Tactical:** Formal processes and playbooks exist, but visibility is partial. It's hard to identify patterns or prevent recurrence.
- **Strategic:** An integrated, data-driven program that not only responds to incidents quickly, but also learns from incidents, prevents recurrence, and demonstrates value.

As you work through the checklist, your responses indicate your level of maturity: mostly 'no' answers suggest an *ad hoc* stage, a mix of 'yes' and 'no' reflects a *tactical* stage, and predominantly 'yes' answers indicate a *strategic* stage.

Assessment Checklist: Are you operating at a strategic level?

The following questions and maturity markers will help you pinpoint the current state of your incident management response process and build a clear plan for moving toward strategic maturity.

1. Capture and triage

How incidents are captured, classified, and prioritized

Can incidents be submitted from multiple channels (intake forms, GSOC, field, HR, external alerts) into one system?	□
Do you apply a common taxonomy and severity matrix across regions and business units?	□
Is triage automated, with routing based on severity, location, or type?	□
Are false positives or routine incidents that require no action resolved quickly through automation, with little to no human intervention?	□
How easily can incidents be enriched with context (HR records, access logs, prior cases, external intel) without manual digging?	□

Maturity markers

Ad hoc: Reports arrive via email or spreadsheets and are often incomplete. Every incident is manually triaged.

Tactical: You have a central intake form and a basic severity matrix, but limited multi-language support. Data enrichment and context is manual.

Strategic: You enable real-time intake from multiple multi-language sources with automated triage, predictive alerts, and instant context from integrated data.

2. Response coordination

How the right teams and actions are activated

Are playbooks automatically triggered by incident type or severity?	□
Do HR, Legal, Facilities, and other partners collaborate in the same case management environment?	□
Can notifications be sent through the tools your teams already use (Slack, Teams, ServiceNow)?	□
Do you track guard dispatch, vendor actions, and external partner engagement in one system?	□

Maturity markers

Ad hoc: Responses are delayed by hours, ownership is unclear, notifications are often missed, and handling varies across shifts, sites, and regions.

Tactical: Playbooks exist but depend on manual call trees, with 80–90% notification coverage and escalations that can still take hours.

Strategic: Priority incidents are escalated in under 10 minutes with 95%+ notification coverage and seamless cross-functional collaboration in one system.

3. Resolution

How incidents are contained, documented, and formally closed

Do all incidents have formal closure with required fields and defensible audit trails?	□
Can you link incidents to prior cases, subjects, or risk indicators?	□
Can field teams capture updates (photos, timestamps, video) in real time and automatically link them to an existing incident record without manual data transfer?	□
Are corrective actions assigned to owners with deadlines?	□
Do you track recurrence rates and use them to measure effectiveness?	□

Maturity markers

Ad hoc: Notes are scattered, recurrence is untracked, and closures lack consistency.

Tactical: Incidents include formal closure fields and a basic audit trail, but recurrence is anecdotal, and time-to-resolution is only tracked weekly.

Strategic: Median priority resolution is achieved within 24–48 hours, over 90% of corrective actions are closed on time, and recurrence drops below 10% for addressed root causes.

4. Analysis

How insights are gathered and improvements are identified

Do you conduct structured reviews after significant incidents?	□
Can you analyze trends by site, region, or incident type?	□
Are playbooks, staffing, or controls updated automatically from insights?	□
Do you track precursors to workplace violence, insider threats, or protests?	□
Do you measure repeat incident reduction as a prevention outcome?	□

Maturity markers

Ad hoc: Lessons are captured only after major events, with little focus on smaller or recurring issues.

Tactical: Trend reviews are conducted quarterly, supported by heat maps and post-incident reviews for severe cases.

Strategic: Analytics run continuously with predictive modeling in place, and the prevention-to-incident ratio steadily improves.

5. Measuring impact

How results are measured and communicated to stakeholders

Can you generate analyst, executive, and compliance reports without manual effort?	□
Can reporting be segmented by site, region, or business unit?	□
Do you provide data-driven incident impact reporting to executives or the board?	□
Do your metrics show outcomes such as reduced recurrence, faster resolution, or cost savings?	□
Can other business functions say that your insights help them make better decisions?	□

Maturity markers

Ad hoc: Reporting is limited to raw activity metrics with no clear ROI connection.

Tactical: Standard dashboards track TTA/TTR, with SLA attainment at 70–80%.

Strategic: SLA attainment exceeds 95%, cost avoidance is quantified, and metrics are tied directly to enterprise risk appetite.

Not there yet? Start taking steps to mature your program today

If your program isn't fully strategic yet, these steps you can take today will help close the gap without overwhelming your team.

- **Audit intake processes:** Map all current reporting channels with the ultimate goal of moving toward centralization.
- **Evaluate triage processes:** Assess how different teams and locations handle triage by incident type and begin defining global rules to ensure consistency.
- **Engage stakeholders:** Gather input on bottlenecks that delay response.
- **Start linking data:** Track connections by people, locations, or assets — even if you don't yet have a dedicated system for this — to build a foundation for pattern recognition.
- **Elevate metrics:** Translate activity counts into business outcomes: cost avoided, recurrence reduced, resilience gained.

Incident management all in one place with Ontic

When security incidents occur, fragmented systems slow you down. Ontic connects response operations, so you can move faster, mitigate impact, and stop incidents from recurring.

Learn More