everbridge
xmatters

Incident response integration planning checklist

Build a connected, automated incident response ecosystem

Modern incident response depends on more than alerts. As environments become increasingly distributed across cloud infrastructure, observability platforms, collaboration tools, ITSM systems, AI workflows, and security operations, organizations need a connected operational ecosystem that helps teams detect, decide, and act faster.

This checklist helps operational leaders evaluate integration gaps, prioritize modernization efforts, and improve incident response coordination across teams and systems. Before prioritizing new integration implementation, it's important to understand where operational friction exists today.

For each area below, assess whether workflows are:

Manual

Tasks are completed primarily by people, with little to no system-driven support. Processes may rely on individual judgment, spreadsheets, emails, or one-off actions to move work forward.

Partially automated

Some steps are supported by technology or predefined workflows, but human intervention is still required to review, trigger, coordinate, or complete key parts of the process.

Fully orchestrated

The process is connected end-to-end across systems, teams, and workflows. Actions, notifications, escalations, and handoffs are automatically coordinated based on defined rules, data, and real-time conditions.

Connect your incident response ecosystem with xMatters - start free today: xmatters.com/signup

Section 1

Evaluate your current incident response environment

01 Detection and observability

Questions to evaluate	Manual	Partially automated	Fully orchestrated
Are monitoring and observability platforms integrated into incident response workflows?	☐	☐	☐
Are alerts enriched with operational context before responders are engaged?	☐	☐	☐
Can teams correlate signals across infrastructure, applications, and services?	☐	☐	☐
Are high-priority incidents automatically identified and escalated?	☐	☐	☐
Is alert noise creating responder fatigue?	☐	☐	☐

Operational gaps to look for

- Excessive false positives
- Manual triage
- Lack of service ownership visibility
- Siloed monitoring tools
- Slow escalation paths

Common integration priorities

- Datadog
- New Relic
- Grafana
- Splunk
- Dynatrace

02 Incident management and ITSM

Questions to evaluate	Manual	Partially automated	Fully orchestrated
Are incidents synchronized across operational systems?	☐	☐	☐
Are responder engagement workflows automated?	☐	☐	☐
Can teams escalate incidents intelligently based on severity, ownership, or service impact?	☐	☐	☐
Are major incident workflows standardized?	☐	☐	☐
Can operational updates flow bi-directionally between systems?	☐	☐	☐

Operational gaps to look for

- Manual paging
- Ticket-centric response delays
- Poor coordination across teams
- Disconnected ITSM workflows
- Inconsistent escalation management

Common integration priorities

- ServiceNow
- Jira Service Management
- Freshservice
- BMC

03 Collaboration and ChatOps

Questions to evaluate	Manual	Partially automated	Fully orchestrated
Can responders coordinate directly within collaboration platforms?	☐	☐	☐
Are incident channels created automatically?	☐	☐	☐
Can teams execute workflows directly from Slack or Teams?	☐	☐	☐
Are bridge coordination workflows automated?	☐	☐	☐
Do executives and stakeholders receive consistent updates?	☐	☐	☐

Operational gaps to look for

- Ad hoc collaboration
- Excessive context switching
- Manual bridge coordination
- Communication bottlenecks
- Fragmented incident updates

Common integration priorities

- Slack
- Microsoft Teams
- Zoom
- Cisco

04 DevOps and CI/CD Coordination

Questions to evaluate	Manual	Partially automated	Fully orchestrated
Can deployment failures automatically trigger operational workflows?	☐	☐	☐
Are rollback and approval workflows coordinated consistently?	☐	☐	☐
Are engineering and operations teams aligned during release incidents?	☐	☐	☐
Can incidents be connected directly to deployments and changes?	☐	☐	☐
Are CI/CD pipelines integrated into incident response workflows?	☐	☐	☐

Operational gaps to look for

- Slow rollback coordination
- Poor release visibility
- Manual deployment escalations
- DevOps silos
- Reactive incident management

Common integration priorities

- GitHub
- GitLab
- Jenkins

05 Security operations and cyber resilience

Questions to evaluate	Manual	Partially automated	Fully orchestrated
Can security detections automatically trigger coordinated response workflows?	☐	☐	☐
Are SecOps and ITOps teams aligned during incidents?	☐	☐	☐
Are cyber response workflows standardized?	☐	☐	☐
Can stakeholder communications be coordinated automatically?	☐	☐	☐
Are containment and escalation workflows automated?	☐	☐	☐

Operational gaps to look for

- Delayed cyber coordination
- Disconnected response workflows
- Manual stakeholder communications
- Security escalation bottlenecks
- Limited cross-functional visibility

Common integration priorities

- CrowdStrike
- Palo Alto Networks
- Splunk
- Okta

06 AI and operational intelligence

Questions to evaluate	Manual	Partially automated	Fully orchestrated
Are teams using AI to reduce operational overhead?	☐	☐	☐
Can AI assist with incident summarization and context gathering?	☐	☐	☐
Are operational workflows enriched with intelligent recommendations?	☐	☐	☐
Can AI-generated insights integrate directly into response workflows?	☐	☐	☐
Are humans still maintaining oversight and control?	☐	☐	☐

Operational gaps to look for

- Manual incident coordination
- Information overload
- Slow knowledge retrieval
- Inconsistent operational context
- Excessive cognitive load on responders

Common integration priorities

- OpenAI
- Google Gemini

Section 2

Prioritize your integration strategy

Not all integrations create equal operational value.

The highest-impact integrations typically:

- Reduce decision latency
- Eliminate manual coordination
- Improve cross-team visibility
- Accelerate escalation workflows
- Automate repetitive operational tasks

High-impact integration categories

Integration area	Business impact	Operational complexity	Typical priority
Observability	High	Medium	High
ITSM and incident management	High	Medium	High
ChatOps and collaboration	High	Low	High
Cloud infrastructure	High	High	Medium
Security operations	High	Medium	High
DevOps & CI/CD	Medium	Medium	Medium
AI and operational intelligence	Emerging High	Medium	Strategic

Section 3

Incident response maturity assessment

Level 1 — Reactive

Characteristics:

- Manual paging
- Siloed operational tools
- Limited automation
- Slow escalations
- Heavy reliance on tribal knowledge

Level 2 — Coordinated

Characteristics:

- Integrated ITSM workflows
- Standardized escalation paths
- Cross-team collaboration
- Automated notifications
- Centralized incident visibility

Level 3 — Orchestrated

Characteristics:

- Automated operational workflows
- Integrated observability and ChatOps
- Auto-remediation capabilities
- AI-assisted coordination
- Cross-platform orchestration

Level 4 — Dynamically Adaptive

Characteristics:

- AI-assisted operational intelligence
- Dynamic workflow orchestration
- Predictive operational response
- Continuous operational learning
- Reduced decision latency across systems

Section 4

Building a more resilient operational ecosystem

The most effective incident response teams are no longer relying on disconnected operational tooling and manual coordination.

They are building integrated ecosystems where observability, ITSM, collaboration, automation, cloud infrastructure, security operations, and AI-assisted workflows work together in real time.

The result:

- Faster response
- Better coordination
- Reduced operational friction
- Lower incident impact
- More resilient operations

Ready to modernize incident response?

See how xMatters helps organizations connect monitoring, collaboration, automation, ITSM, cloud operations, security workflows, and AI-driven operational intelligence into a coordinated incident response ecosystem.

Book a demo

Connect your incident response ecosystem with xMatters - start free today: **xmatters.com/signup**

Everbridge delivers a business resilience advantage with High Velocity CEM™, powered by Purpose-built AI and decision-ready intelligence to accelerate response, reduce downtime, and protect what matters most.
Request a demo at everbridge.com/demo or call +1 (888) 366-4911.

everbridge™