

SmartSuite

GRC & Resilience > Operational Resilience & Business Continuity ·
Datasheet

Incident Management

Capture and resolve incidents with structured workflows, real-time visibility, and integrated response across risk, compliance, and operations.

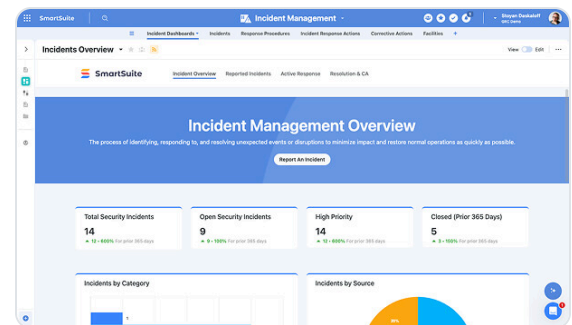
SKU	GRC - RES - INC
Solution area	GRC & Resilience
Works with	Enterprise Risk Management (ERM), Issues Management, Compliance Assessments & Testing, Third Party Risk, Policy Management, Operational Resilience
Updated	Sep 26, 2026
Datasheet	v1.0

What it is

Incident Management is the process of identifying, managing, and resolving operational, security, and compliance-related incidents. It enables organizations to coordinate response activities, minimize impact, and maintain visibility into incident trends and resolution performance.

Incident Management is the process of identifying, managing, and resolving operational, security, and compliance-related incidents. SmartSuite's Incident Management software provides a structured, scalable system to manage incidents across your organization — ensuring timely response, coordination, and resolution.

SmartSuite enables organizations to standardize incident intake, classification, investigation, and resolution workflows across business units. With a centralized system of record, teams can track incident details, assign ownership, and manage response activities in a way that is repeatable, auditable, and defensible.



Incident Management in SmartSuite.

Core capabilities

Incident Intake & Reporting

Capture incidents through forms, integrations, or automated triggers across systems and workflows.

Incident Classification & Severity

Categorize incidents based on type, severity, and impact to prioritize response and escalation.

Incident Response Workflows

Define and manage structured response processes, including investigation, containment, and resolution steps.

Ownership & Escalation Management

Assign owners and escalate incidents based on severity, timelines, and predefined rules.

Root Cause Analysis

Investigate underlying causes of incidents to prevent recurrence and improve controls.

Incident Dashboards & Analytics

Monitor incident trends, response times, and outcomes through real-time dashboards.

Automated Notifications & Alerts

Trigger alerts, reminders, and escalations to ensure timely response and coordination.

Cross-Product Integration

Link incidents to risks, issues, audits, controls, and vendors for full lifecycle visibility.

Role-Based Access Control

Ensure secure access to incident data and workflows across teams and stakeholders.

The Incident Lifecycle

Step 1

Classify & Prioritize

Assess severity, impact, and urgency to determine response actions.

Step 2

Investigate & Respond

Execute response workflows, contain impact, and coordinate resolution efforts.

Step 3

Resolve & Document

Complete remediation activities and document outcomes and lessons learned.

Step 4

Analyze & Improve

Perform root cause analysis and update controls, policies, and risk strategies.

Who it is for

Chief Risk Officer (CRO)

Monitors incident trends and ensures alignment with enterprise risk strategy.

Security / IT Leader

Manages security incidents and operational disruptions across systems and infrastructure.

Incident Response Manager

Coordinates incident response activities and ensures timely resolution.

Compliance Manager

Tracks compliance-related incidents and ensures regulatory requirements are met.

Risk Manager

Aligns incident data with risk assessments and mitigation strategies.

Executive / Board Member

Monitors incident trends, impact, and response performance through dashboards.

Works with

Enterprise Risk Management (ERM)

Incident impacts dynamically update risk exposure and scoring.

Compliance Assessments & Testing

Control failures and compliance gaps identified through incidents inform testing and improvements.

Policy Management

Policy violations identified through incidents drive updates and enforcement.

Issues Management

Incidents generate issues that are tracked and resolved through remediation workflows.

Third Party Risk

Vendor-related incidents impact third-party risk assessments and monitoring.

Operational Resilience

Incidents trigger resilience workflows and inform continuity planning and testing.

Built differently. Incident Management runs on the same relational platform as every other SmartSuite product, so its records link to the risks, controls, issues and evidence they affect, and every report reflects the current state rather than a copy.

See it working with your data

Ask your SmartSuite account team for a demo of Incident Management configured for your organization, or read the full product entry at smartsuite.com/products/incident-management.

[Schedule a demo](#)