

SmartSuite

GRC & Resilience > Operational Resilience & Business Continuity · Datasheet

Operational Resilience

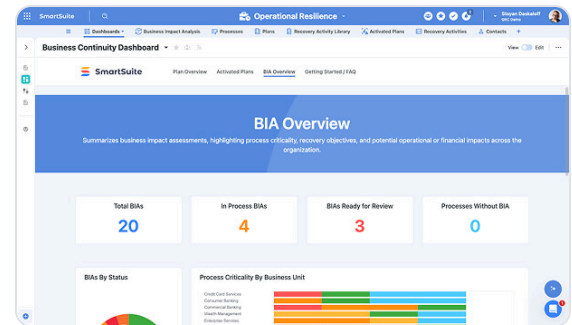
Define critical services, map dependencies, and validate recovery strategies to ensure business continuity, regulatory alignment, and organizational resilience.

SKU	GRC - RES - OPR
Solution area	GRC & Resilience
Works with	Enterprise Risk Management (ERM), Third Party Risk, Incident Management, Control Framework & Regulatory Libraries, Policy Management, Issues Management
Updated	Sep 26, 2026
Datasheet	v1.0

What it is

Operational Resilience is the ability of an organization to anticipate, withstand, and recover from disruptions while maintaining critical business services. It enables organizations to identify dependencies, plan for disruptions, and ensure continuity across operations and systems.

Operational Resilience is the ability of an organization to anticipate, withstand, adapt to, and recover from disruptions while maintaining critical business services. SmartSuite's Operational Resilience software provides a structured, scalable system to manage resilience across your enterprise — ensuring continuity of operations under adverse conditions.



Operational Resilience in SmartSuite.

Core capabilities

Critical Service Mapping

Identify and map critical business services along with supporting systems, processes, and third-party dependencies across the organization.

Business Impact Analysis (BIA)

Assess the impact of disruptions on critical services, including financial, operational, and regulatory consequences.

Dependency Mapping

Visualize relationships between people, processes, systems, and vendors to understand potential points of failure.

Scenario Testing & Simulation

Model disruption scenarios and evaluate organizational readiness through structured testing and simulation exercises.

Recovery Planning & Playbooks

Define and manage response plans, recovery strategies, and escalation procedures for different disruption scenarios.

Impact Tolerance Definition

Establish thresholds for acceptable disruption levels and measure resilience against defined tolerances.

Resilience Dashboards & Analytics

Monitor resilience posture, testing outcomes, and recovery readiness through real-time dashboards and reporting.

Workflow Automation

Automate testing cycles, review processes, and response coordination using configurable no-code workflows.

Role-Based Access Control

Ensure secure access to resilience plans, testing results, and critical service data across teams and stakeholders.

The Resilience Lifecycle

Step 1 Identify Critical Services Define critical business services and map dependencies across systems, processes, and third parties.	Step 2 Assess Impact & Risk Conduct business impact analysis and evaluate disruption scenarios and vulnerabilities.	Step 3 Plan & Prepare Develop recovery strategies, response plans, and resilience playbooks aligned with impact tolerances.	Step 4 Test & Validate Execute scenario testing and simulations to validate readiness and identify gaps.	Step 5 Respond & Improve Coordinate response during disruptions and continuously improve resilience based on insights and outcomes.
--	---	---	--	---

Who it is for

Chief Risk Officer (CRO) Oversees resilience posture and ensures alignment between risk exposure and business continuity strategies.	Business Continuity Manager Develops and manages continuity plans, testing programs, and resilience strategies.	Risk Manager Aligns operational risks with resilience planning and monitors exposure across critical services.
IT Operations Lead Ensure system availability, recovery readiness, and operational continuity across infrastructure and services.	Compliance Manager Ensures alignment with regulatory resilience requirements such as DORA and ISO 22301.	Executive / Board Member Monitors resilience readiness, disruption impact, and recovery performance through dashboards.

Works with

Enterprise Risk Management (ERM) Operational risks and residual exposures inform resilience planning and prioritization.	Third Party Risk Vendor dependencies and risks are incorporated into resilience and continuity strategies.
Incident Management Vendor dependencies and risks are incorporated into resilience and continuity strategies.	Control Framework & Regulatory Libraries Real-time incidents trigger response workflows and update resilience readiness insights.
Policy Management Resilience policies and standards guide planning, testing, and response activities.	Issues Management Track and resolve resilience gaps identified during testing and disruption events.

Built differently. Operational Resilience 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 Operational Resilience configured for your organization, or read the full product entry at smartsuite.com/products/operational-resilience.

Schedule a demo