The Operational Resilience process

Powered by Smart Assessment Engine
Speed Learning

Risk Business Unit – Outbound Product Management

Product Adoption Architect

servicenow

The Operational Resilience process

Powered by Smart Assessment Engine Speed Learning

Operational Resilience has four interconnected capabilities — Importance and Impact Tolerance (IIA) Assessments, Scenario Analysis, Self-Attestation, and Operational Vulnerability Management — forming a continuous resilience cycle. The Smart Assessment Engine (SAE) powers three of the four. Each capability is the what; SAE is the how — a recurring theme throughout.

servicenow

Table of contents

servicenow

01

The foundation

Operational Resilience context, the resilience cycle & getting started

01.

What is ServiceNow Operational Resilience ?

Operational Resilience context, the closed loop & getting started

Operational resilience involves the capacity to foresee, prevent, respond to, and adjust to disruptive operational incidents. The ServiceNow GRC: Operational Resilience solution enables organizations to maintain business service continuity during challenges like pandemic, severe weather, or cyber threats. As part of the GRC product suite, it offers a unified platform spanning IT, HR, Finance, Security, and Facilities.

Four interconnected capabilities — one continuous cycle

Importance and Impact Tolerance Assessments

Measure service importance & impact tolerance. The scoring foundation. SAE-powered.

Scenario Analysis

Test IIA tolerance baselines against simulated disruptions. Detect breaches. Event-driven.

Self-Attestation

Formally certify resilience status. Generate signed PDF reports. SAE-powered.

Operational Vulnerability Mgmt.

Capture gaps from all three. Perform impact assessment and drive remediation via action tasks. SAE-powered[1].

servicenow

[1] SAE template for Operational Vulnerability is not provided out of box

01.

What Operational Resilience on ServiceNow delivers

The value story

Establish resilience baselines

1

Data-driven importance ratings and four-dimensional tolerance thresholds via SAE — replacing subjective guesswork with configurable, auditable methodology

Test with structured tabletop exercises

2

Scenario analysis simulates adverse events against services, comparing disruption to IIA tolerance thresholds to detect breaches before they happen in reality

Certify for regulators and auditors

3

SAE-powered self-attestation generates signed PDF reports combining IIA results, scenario analysis approaches, and formal compliance certification with e-signature

Close the remediation loop

4

Operational vulnerabilities from all capabilities funnel into structured remediation with treatment decisions, action tasks, and root cause analysis — ensuring gaps get resolved

Unify on one assessment engine

5

SAE powers IIA, self-attestation, and operational vulnerability impact assessment with consistent UX, collaboration, scoring, and automation — learn once, apply everywhere

Scale across the data model

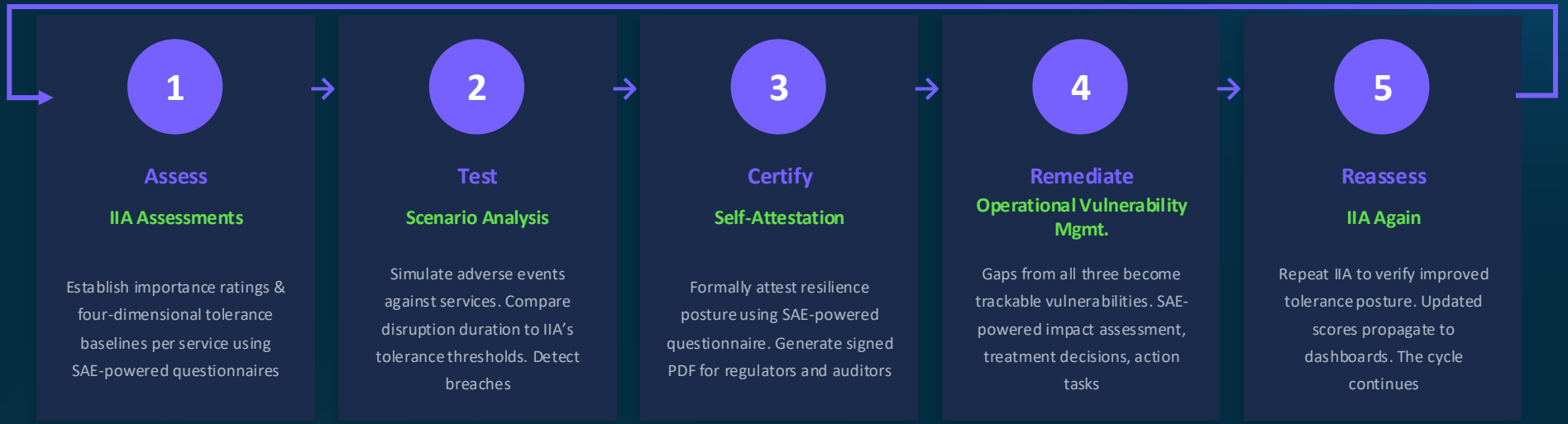
6

Flexible data model and configurable top-class property let you assess and report at any CSDM level: business services, offerings, processes, or applications

01.

The Operational Resilience process on ServiceNow

Four capabilities forming a continuous improvement cycle — SAE powering three of four



Continuous loop — vulnerabilities can be raised from IIA, scenario analysis, self-attestation, services, and manually reported by anyone using the Employee Center

IIA baselines inform the thresholds tested by scenario analysis

Self-attestations is substantiated by testing

Operational vulnerability helps address gaps from IIA, scenario analysis, & self-attestation

servicenow

01.

Prerequisites

Foundation topics recommended for this speed learning

While none of these are mandatory, prior familiarity with the topics below will make the session land more cleanly. They cover the broader GRC and platform context that Operational Resilience builds on:

- ❑ ServiceNow GRC Fundamentals in context of Organizational Entities
- ❑ Configuration Management Database and its significance
- ❑ Common Service Data Model (CSDM) - service hierarchy and dependency pillars
- ❑ Operational Resilience application fundamentals and the four-stage resilience lifecycle
- ❑ Smart Assessment Engine fundamentals – templates, scoring, and automation

For deeper coverage of Operational Resilience and the Smart Assessment Engine, refer to the ServiceNow documentation site — both products have dedicated documentation.

02

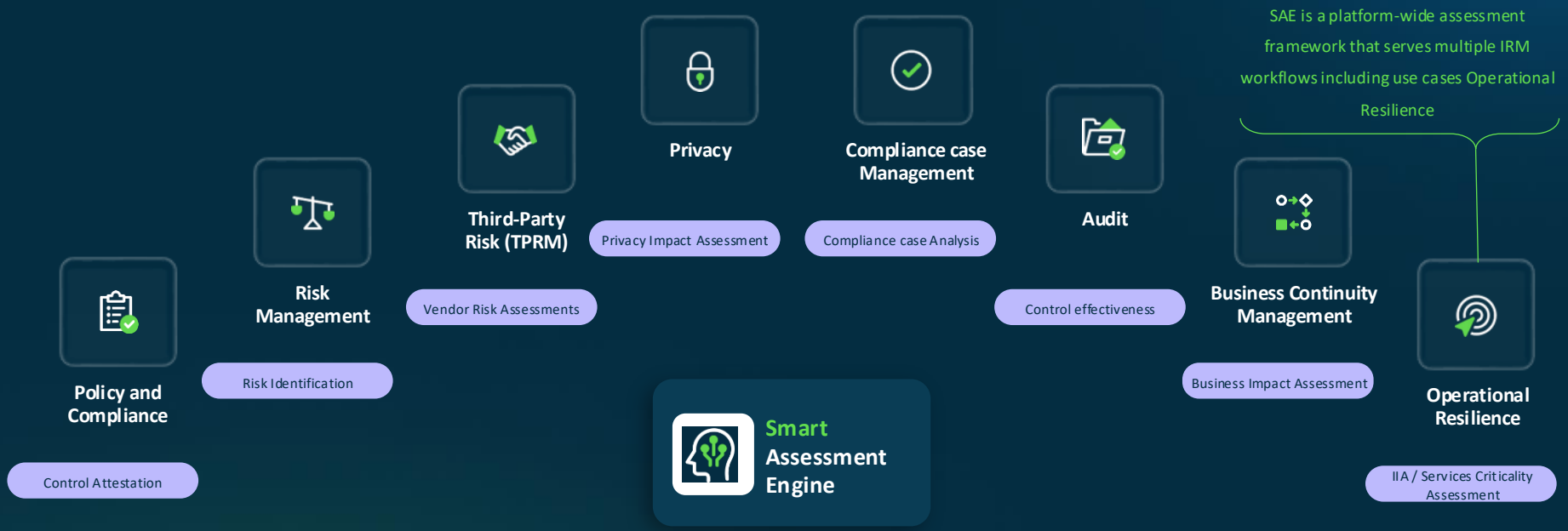
Smart Assessment Engine

One framework for every assessment across IRM

02.

Smart Assessment Engine (SAE) in IRM

One framework for every risk assessment



SAE provides a single, consistent design and execution framework reused across all IRM assessment workflows reducing training overhead and enabling unified governance.

02.

SAE — Assess smarter, not harder.

“Smart Assessment Engine provides One unified framework for every assessment across IRM—designed for business users, powered by AI”

Design

Unified Template Designer
Build assessments in a single intuitive interface with sections, dependencies, and configuration pills

Flexible Question Types
Radio, checkbox, dropdown, number, multi-select reference, and barcode/QR code scanning

Scoring & Normalization
Business users configure scoring –with cross scale normalization at question, section, and assessment levels without coding

Template Copy & Quick Edit
Duplicate published templates; make minor edits without full republish cycle

Multi-Role Categories
Assign multiple roles to a single template category for flexible access control

Assess

Modern Assessor UX
Auto-save, progress tracking, inline justifications, attachments, and streamlined navigation

Combined Assessments
Respond to multiple assessments in one view with bulk submit, cross-template combine, and auto-copy

Real-Time Collaboration
Multiple stakeholders co-author simultaneously with live presence and change tracking

Granular Delegation
Primary Owners, Assessment Contributors, and Sectional Contributors with scoped permissions

Domain Separation
Multi-tenant support with process-segregated templates available across child domains

Automate

Response Automation
Auto-prefill answers from prior assessments or external systems with editable or read-only controls

Post Assessment Actions
Trigger notifications, record updates, and subflows automatically based on assessment responses

Combined Assessment Auto-Copy
Answers replicate across related assessments automatically—including justifications and attachments

Migration Utility
Seamlessly migrate legacy Metric-type assessments into SAE templates with full tracking

Flow Action Integration
Trigger assessments from any workflow using platform Flow Designer for end-to-end automation

Serving multiple IRM workflows: Compliance | Risk | TPRM | Privacy | Audit | BCM | OpRes | ESG • Xanadu through Australia

servicenow

02.

How SAE powers each Ops Res capability

Three of four capabilities are directly SAE-powered; the fourth feeds into SAE-powered assessments

IIA Assessments

Drives importance & tolerance questionnaires. Auto-calculates scores across four dimensions. Supports retake, override governance, and SAE collaboration

SAE Templates: Importance / Impact Tolerance / Combined assessment templates (default ships OOB)

Scenario Analysis

Uses its own event/participant/response task model — not SAE directly. But breach results and gap findings feed into SAE-powered vulnerability assessments

SAE Templates: Not Applicable — uses scenario events, participant roles, and response tasks

Self-Attestation

Powers the attestation questionnaire. Creates assessment instances automatically. Supports contributors. Combines SAE results with PDF export and e-signature

SAE Templates: Self attestation assessment template (default ships OOB)

Operational Vulnerability Mgmt.

Drives vulnerability impact assessment during the Assessment state. Template configured in the vulnerability type setup. Evaluates severity, scope, and impact

SAE Templates: Template must be configured per vulnerability type in Assessment Workspace, no default out of the box

03.

Plugin dependencies

What must be installed for Ops Res to function

Required plugins (hard dependencies)

Plugin	App ID
GRC: Operational Resilience	com.sn_grc_oper_res
GRC: Common Workspace Elements	com.sn_grc_workspace
GRC: Profiles	com.sn_grc
GRC: Core Case Management	com.sn_grc_case_mgmt
Data Relationships Framework	com.sn_app_grc_relationship_config
Data Registry	com.sn_app_grc_data_registry
GRC: Risk Shared Components	com.irm-shared-common-components
Document Templates	com.snc.app-document-templates

Plugin	App ID
GRC: Assessment Designer	sn_smart_asmt_desg
GRC: Post Assessment Actions	sn_smart_imp_auto
Smart Assessment Collaboration	sn_smart_collab

Optional plugins (maximize the value)

- Policy & Compliance Management (recommended)
- Advanced Risk (recommended)
- Risk Management (recommended)
- Business Continuity Planning
- Business Impact Analysis
- Crisis Management
- Vulnerability Response

Smart Assessment Collaboration (sn_smart_collab) enables the Contributors feature in SAE-based IIA assessments — not a formal Ops Res dependency but required for full collaboration capabilities in the IIA workflow.

servicenow

04.

Roles & permissions

Key personas that interact with all four Ops Res capabilities

Administrator

sn_oper_res.admin

- Configure importance & impact tolerance rating scales and choices
- Create scenarios, event groups, and events for scenario analysis
- Configure operational vulnerability types, state models, action task models
- Create and maintain SAE templates (IIA, self-attestation, operational vulnerability (OVs)
- Delete assessments in any state; customize Ops Res dashboard reports
- Configure OpRes record view and task page configurations for tailoring workspace pages
- Contains sn_oper_res.manager

Manager

sn_oper_res.manager

- IIA: Create, scope, assign, review IIA assessment, override results, capture OVs., approve/ reject, close
- Scenario: Create analyses, add scope/dependencies/events/participants, request approvals, capture OVs
- Self-Attestation: Create, respond to questionnaire, generate PDF, close
- Operational Vulnerability: Report, assess impact, determine treatment, manage action tasks, request approval
- Contains sn_oper_res.user role

User

sn_oper_res.user

- IIA: Respond to SAE questionnaires as assessor or contributor
- Scenario: Participate in events; complete response tasks with observations, gaps, recommendations
- Operational Vulnerability: Complete assigned action tasks for remediation
- Self-Attestation: Respond to questions; act as contributor (22.0.x+ — cannot submit, only assessor can)
- View reports and dashboard; contains sn_grc.reader role

Business User sn_oper_res.operational_resilience_business_user — Report operational vulnerabilities from Employee Center only (Self-Service > Risk & Compliance)

⚠ **Approver must differ from owner & assessor (IIA + scenario analysis)**

SAE roles: assign sn_smart_asmt.template_manager for admin profiles; sn_smart_asmt.assessment_reader + sn_smart_asmt.actor for all user profiles

servicenow

05

IIA Assessments

Importance & Impact Tolerance — the scoring foundation

05.

IIA: Metrics that matter in the resilience decisions

Importance

How critical is this service?

- Number of customers using the service
- Revenue the service generates
- Impact on company brand
- Regulatory significance

Impact tolerance

How long can the service be down?

- Unacceptable harm to customers
- Financial loss exceeds threshold
- Transaction volume loss is critical
- Regulatory breach occurs

Built on UK PRA / Bank of England regulations and optimized for global needs — three impact areas: Customers, Firm, Market

servicenow

05.

IIA: Assessment dimensions that feed the metrics

Impact tolerance (four dimensions)

Duration

How many days can the service be non-operational? Tied directly to the importance rating scale.

Customer Impact

Maximum acceptable impact on customers — affected users, SLA breaches, customer satisfaction.

Financial Impact

Maximum acceptable financial loss — revenue impact, penalties, contractual obligations.

Transaction Volume

Maximum tolerable throughput loss — payment processing, order volumes, batch jobs.

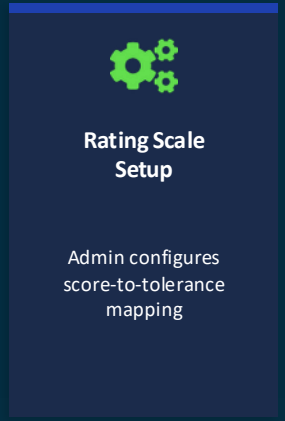
These four measures provide a fuller view of risk by showing how long a service can be down, who is impacted, the financial cost, and the disruption to business. For instance, a payment service might handle 2 days of downtime but not a $10M loss in 4 hours. Duration alone isn't sufficient.

servicenow

05.

IIA: OOTB Rating Scale

Ability to configure: importance, tolerance, score range



Importance	Tolerance	Score Range	Icon	Order
1 — Most Critical	1 Day	76–100	flag-fill	10
2 — Somewhat Critical	2 Days	51–75	triangle-excl-fill	20
3 — Less Critical	3 Days	26–50	binoculars-fill	30
4 — Not Critical	4 Days	0–25	circle-check-fill	40

Key admin notes

- Admins with Ops Res admin (sn_oper_res.admin) role can configure scales as per the SAE template
- Manage Choices via GRC Choice table (choice_category = Assessment Rating, set = Operational Resilience)
- When a new IIA questionnaire template is created, the application clones the default rating scale to it
- Rating scale includes: importance label, color, icon, min/max score, impact tolerance duration, and display order

05.

IIA: Assessment workflow (SAE-powered)

Seven states from Draft to Closed — with retake capability unique to SAE

Draft	Owner	Create IIA assessment, select Smart/Legacy, choose SAE templates, assign owner/assessor/approver
Scope defined	Owner	Add one or more Business Services to the Scope tab — mandatory before proceeding
Pending response	Owner → Assessor	Owner selects Assess. SAE generates instance. Assessor receives email notification
Assessment received	Assessor → Owner	Assessor submits. SAE auto-calculates importance + 4 tolerance dimensions. Owner can override results with justification
Pending approval	Owner → Approver	Owner requests approval. Approver gets email. If no approver specified, auto-approves
Approved	Approver	Verifies and approves. Can reject → reverts to Pending response for retake (SAE advantage)
Closed	Owner	Owner closes the assessment. Closed assessments are considered inactive

NOTE: Operational vulnerabilities can be raised directly from IIA records via the Operational vulnerabilities related list in the IIA assessment before assessment(s) are closed

servicenow

05.

IIA: Intake form & service-level output

What goes in and what comes out

Create IIA form (key fields)

Number	Auto-assigned (IIA0010018)	Auto
Name / Description	Assessment name and context	Req
Assessment type	Smart Assessment or Legacy	Req
SAE templates	1+ templates: Importance / Tolerance / Combined	Smart
Owner / Assessor / Approver	Approver must differ from owner & assessor	Req
Scope (tab)	Add 1+ business services — mandatory	Req

Service-level output (auto-calculated by SAE)

Importance (1–4 rating)	Overridden Importance
Impact Tolerance — Duration	Justification* — Duration
Impact Tolerance — Customer Impact	Justification* — Customer
Impact Tolerance — Financial	Justification* — Financial
Impact Tolerance — Transaction Vol.	Justification* — Trans. Vol.

* Owner can override (with justification)

IIA output informs:

Dashboards: Business services by importance, by impact tolerance, by red flags

Scenario analysis: Compares impact tolerance vs disruption duration to determine breach status

Self-attestation: Attestation questionnaire asks about IIA results and tolerance assessment approach

Operational Vulnerability mgmt: Tolerance gaps can be raised as operational vulnerabilities directly from IIA records

servicenow

06

Scenario Analysis

Conduct tabletop scenario exercises

06.

Scenario analysis: building blocks & event model brief

If IIA asks “how critical?”, scenario analysis asks “what happens when it goes wrong?”

Scenario analysis is a structured tabletop exercise — simulate adverse events against business services and measure whether the disruption would breach IIA’s tolerance thresholds. It uses its own event-driven model (not SAE) with a dual-approval workflow and multi-departmental participant responses.

Four admin building blocks

Scenarios	Event groups	Events	Participant roles
Business risks (e.g., Flooding, Cyber Attack). Linked to pillars. Created via Admin > Scenarios	Categorize events (e.g., Weather, Energy Issues). Configured as GRC Choices	Specific occurrences (e.g., Flooding, Power Outage). Linked to scenarios and event groups	HR, Legal, Finance, Technology, Security, Supplier Tier1/2/3, Data, People

Key data captured per scenario event

Each scenario event records: potential start/end time, duration, observations, gaps, and recommendations from each participant. Multiple events can overlap — the system calculates both “duration with overlaps” and “duration without overlaps” separately. Participant response tasks are auto-created when participants are added to events.

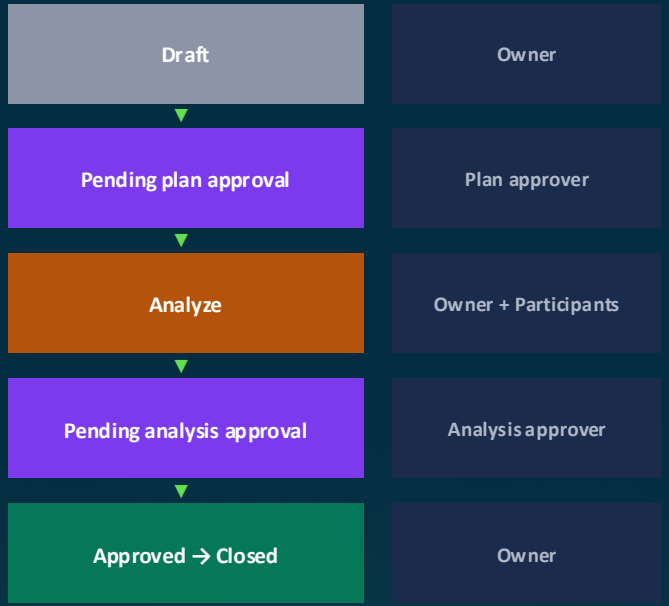
Operational vulnerabilities can be raised directly from scenario analysis records via the Operational vulnerabilities related list

servicenow

06.

Scenario analysis workflow

Dual-approval structure: plan approval + analysis approval



Create analysis, add scope (services), dependencies (assets from pillars), assign plan approver and analysis approver

Reviews scope, services, dependencies, events, participants. Approves → Analyze. Rejects → Draft

Add scenario events and participants. System auto-creates response tasks. Participants provide observations, gaps, recommendations, and impact duration from their departmental perspective

Reviews full scope and progress. Approves or rejects (→ back to Analyze)

Analysis finalized and closed. Breach data feeds dashboard and operational vulnerability management

servicenow

06.

Breach detection — where IIA meets scenario analysis

The system compares IIA tolerance baselines against scenario disruption durations

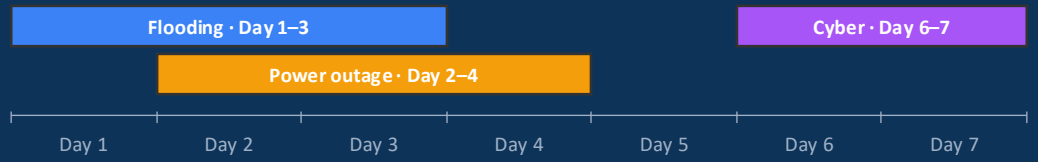
Per-service data in a scenario analysis

- Importance (from IIA)
- Impact Tolerance (from IIA)
- Disruption Duration (from scenario events)
- **Breach Status (auto-calculated)**
- **Deviation % (auto-calculated)**

Summary panel aggregates

- Services under impact tolerance
- Services above impact tolerance
- Total disruption duration
- Duration with event overlaps
- Duration without event overlaps

Example — three events in one scenario



Flood + power outage overlap on Days 2–3, merging into one Day 1–4 window. Cyber attack adds 2 separate days.

With event overlaps
3 + 3 + 2 = **8 days**

Without event overlaps
4 (Day 1–4) + 2 (Day 6–7) = **6 days**

When disruption duration exceeds impact tolerance → service flagged as breached. Deviation % shows the overshoot magnitude. OOTB breach detection focuses on duration alongside the four tolerance dimensions (duration, customer, financial, transaction volume). Breaches feed operational vulnerabilities for remediation.

07

Self-attestation

Formal “sign-off” that certifies services meet resilience

07.

Self-attestation: SAE-powered certification

The formal “sign-off” that certifies services meet resilience requirements

Self-attestation is the formal certification step. After measuring tolerance (IIA) and testing it (scenario analysis), a resilience manager formally attests that services meet requirements, generates a signed PDF report, and stores it as a compliance record. The SA E attestation questionnaire explicitly asks about IIA results and scenario analysis approaches — making it a synthesis document, not a standalone exercise.

Self-attestation workflow (SAE-powered)

1. **Draft**
   Create attestation, select Smart Assessment type, choose Self attestation assessment template, select PDF template (Default Self Attestation HTML Template), optionally attach e-signature (JPEG/PNG/SVG)
2. **Awaiting attestation**
   After adding services to Scope tab and selecting Attest, SAE creates an assessment instance automatically. Owner/assessor responds to questions about importance, scenario analysis approach, and resilience posture
3. **Attestation received**
   After submission, Export to PDF button appears. PDF combines assessment form data with SAE results and e-signature. Downloaded from Activity section. Can share offline with auditors and stakeholders
4. **Closed**
   Owner closes the attestation. Can also be Cancelled if erroneous. Operational vulnerabilities can be raised from the self-attestation record

Note: Contributors can answer questions but only the assessor can submit the self-attestation assessment.

08

Operational vulnerability

Close the resiliency loop with gap identification and remediation

08.

Operational Vulnerability

Capture gaps from all capabilities and drive structured remediation

"Operational vulnerability" terminology originates in the UK PRA/FCA regulatory — covering non-IT process weaknesses that scanning tools can't detect. This capability closes the resilience loop: gaps identified through IIA, scenario analysis, and self-attestation become trackable operational vulnerabilities with full remediation workflows.

Several sources for reporting vulnerabilities

From IIA
Operational vulnerabilities related list on the IIA assessment record. Source auto-set to "Importance and impact assessment"

From scenario analysis
From the scenario analysis record. Breach discoveries and gap findings become trackable operational vulnerabilities

From self-attestation
From the self-attestation record. Gaps identified during the formal certification process become trackable operational vulnerabilities

From services / entities
Directly from service, service offering, business process, or application records in the workspace reported by owners

Employee Center
Any employee can report via Self-Service > Risk & Compliance

Manual
Operational Resilience Managers expected to create directly in workspace

State constraints

You cannot add operational vulnerabilities to: an IIA in Assessment Received state, a scenario analysis in Pending Analysis Approval state, or a self-attestation in Attestation Received state. They must be created before those terminal assessment states.

08.

Operational Vulnerability workflow & action tasks

Several states from New to Closed, with SAE-powered assessment and structured remediation

Operational vulnerability reported. Assigned to requester and analyst. Notifications sent

SAE-powered impact evaluation via template in vulnerability type. Analyst evaluates impact, severity, scope. Note – Build your own template in Assessment workspace, no default

Active investigation. Treatment: Accept, Avoid, Mitigate, Transfer, or None. Root cause analysis conducted

Action tasks must be completed. Approvers receive notifications

Resolution verified. Operational vulnerability closed. Can also be Cancelled

Action tasks are the hands-on remediation work items with their own 7-state workflow:

Draft → Assigned → Work in Progress → Review → Closed Complete / Closed Incomplete / Cancelled

Multiple action tasks can be created without limitation and assigned to different users — enabling parallel remediation across teams.

All action tasks must be closed before the vulnerability can move to approval. This enforces that remediation is complete before resolution.

Key form attributes to note

Severity (Low/Medium/High/Critical) • Priority (1-Critical to 5-Planning) • Vulnerability type & sub-type • Primary entity & entity owner • Personal information flags • Impacted business unit & department • Date of occurrence vs discovery • Treatment decision • Root cause analysis • PDF export capability

servicenow

09.

The interconnection map

Every capability feeds Operational Vulnerability Management — vulnerability sources across the system

Source	How vulnerability is raised	Source field auto-set to
IIA Assessment	Ops Res. vuln related list on IIA record	Importance and impact assessment
Scenario Analysis	Ops Res. vuln related list on scenario record	Scenario analysis
Self-Attestation	Ops Res. vuln related list on attestation record	Self-attestation
Service Records	From service, offering, process, application records	Service
Employee Center	Any employee via Self-Service > Risk & Compliance	Employee Center
Manual	Manager creates directly in workspace	Manual

SAE as the common thread

- **IIA:** SAE templates for importance, tolerance, and combined assessments. Auto-scoring, retake, collaboration
- **Scenario Analysis:** Own event model. But outputs (breaches) feed into SAE-powered operational vulnerability assessments
- **Self-Attestation:** SAE template for attestation questionnaire. Combined with PDF export and e-signature
- **Operational vulnerability:** SAE template in vulnerability type config. Drives impact evaluation during Assessment state

10.

CSDM Framework for Overseeing Operational Resilience

Common Service Data Model — the unified reference for services and their dependencies

Service hierarchy

Business Services / Services → Service Offerings → Business Processes → Application Services

Dependency pillars

Technology | People | Suppliers | Facilities | Data | Others *

Characteristics of the adaptable data model

- **Main node configurations:** Start tracking resilience from any level in the hierarchy — not just business services
- **Top-class property:** sn_oper_res.top_class_name lets admins switch dashboard view between BS, SO, BP, or AS
- **Vertical layout:** User-friendly navigation— four quadrants: Services & Dependencies, Ongoing Events, Red Flags, Program Activities

Key tables & relationships

- **sn_oper_res_profile:** CSDM objects table — stores BS, SO, BP, AS references with class and parent nodes
- **sn_grc_m2m_profile_profile:** Entity hierarchy — saves upstream/downstream parent-child relationships
- **Data Relationships Framework:** Main node configurations define dependency roll-up chains from CMDB into Ops Res

Two jobs drive the flexible data model

- **Weekly: Update CSDM and other dependencies :** Updates hierarchy chain, class assignments, parent nodes. Only relevant objects stored
- **Daily: Calculate red flags for CSDM and dependencies:** Populates dashboard metrics: red flags, importance, impact tolerance values

Critical: Operational Resilience enriches its own tables — it never writes back to CMDB

*** Define your own pillars**

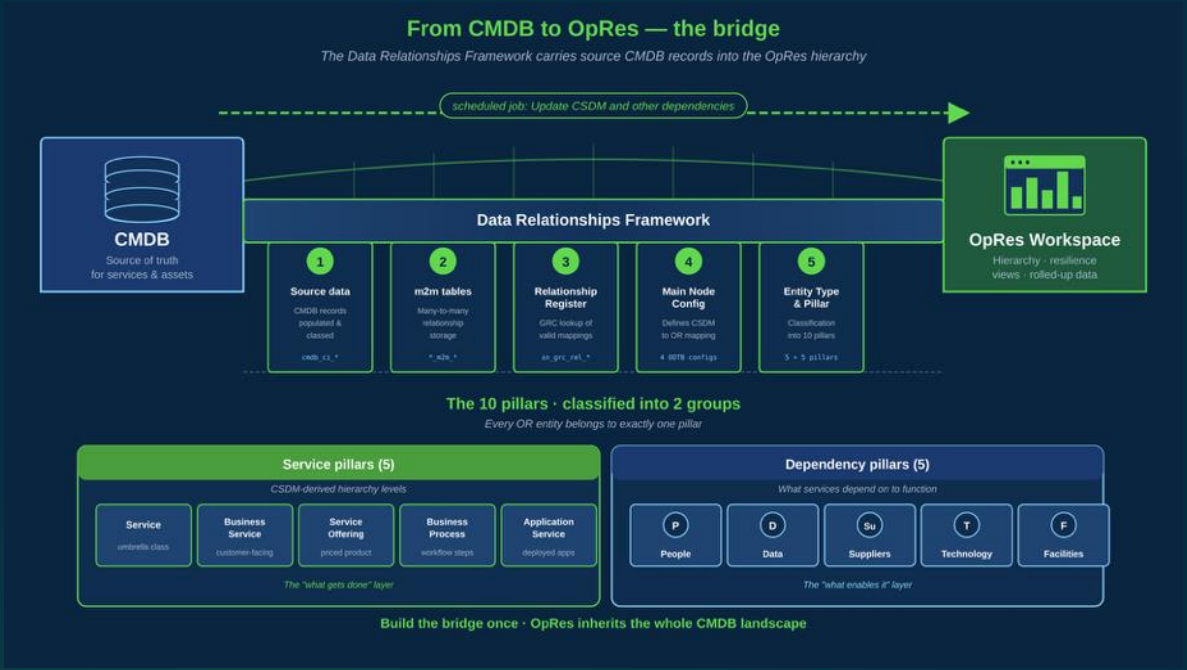
servicenow

11.

Populating Ops Res from CMDB

The single most impactful customer prep activity for scaling adoption

Ops Res can run manually *— but a mature CMDB, wired through Main node configurations, is the* ***single biggest accelerator for adoption at scale****.*



1. **Source data exists**
   Service / dependency record populated in source (target) table.
2. **Set up the m2m table (if needed)**
   Create & populate for many-to-many; else populate target table directly.
3. **Create the relationship register**
   Registers the source relationship with the GRC DRF.
4. **Create the Main node configuration**
   Includes the new OR dependency in the roll-up chain.
5. **Set up the entity type**
   Defines how OR generates entities — and assigns the pillar (service or dependency category).
6. **Run the scheduled job**
   Update CSDM and other dependencies → entity hierarchy & CSDM objects updated.
7. **Dependency surfaces in workspace**
   Appears on the relevant Service / Service Offering / App Service record.

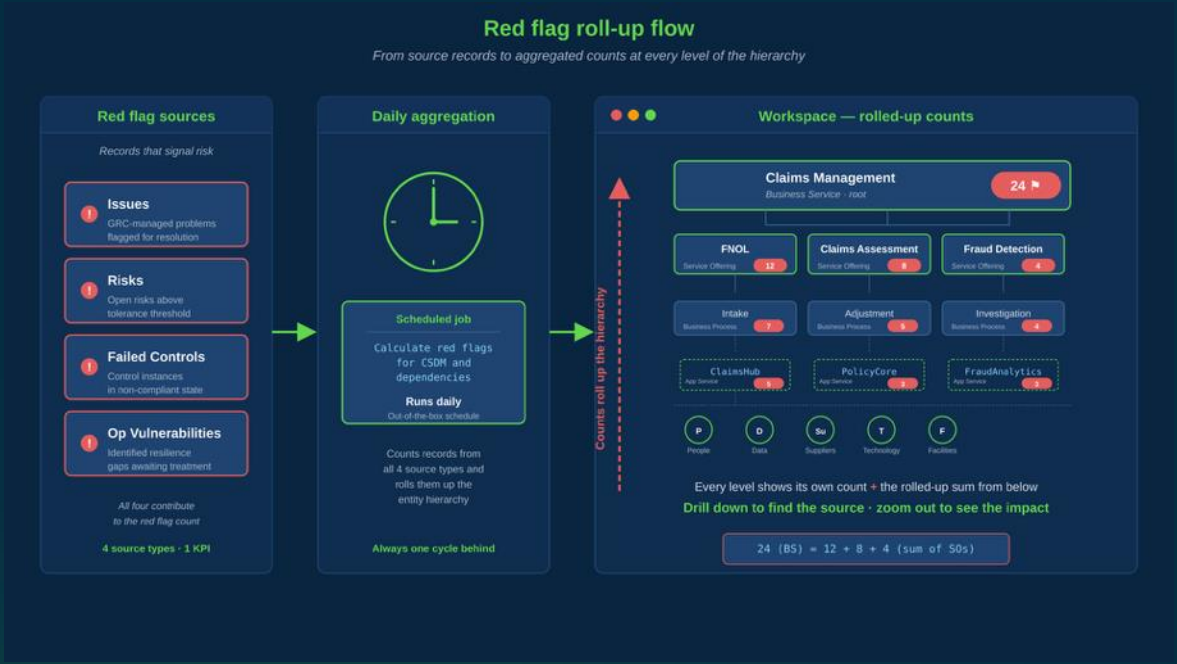
From this point on, every new CMDB record flowing into the source table enters the Ops Res data model automatically — ***compounding value across IIA, scenario analysis, self-attestation, and operational vulnerability.***

12.

How red flags roll up — and where they surface

The actionable KPI that emerges from everything else

*All of OpRes ultimately reduces to one question — **how many red flags does this service have, and how fast can we close them**?*



1. **Issues**
   GRC issues — non-compliance, risk-driven, audit findings.
2. **Risks**
   Open or high-severity risks from Risk Management.
3. **Failed Controls**
   Control attestations that failed in Policy & Compliance.
4. **Operational Vulnerabilities**
   Gaps identified through IIA, scenarios, attestations, or reported via Employee Center.
5. **Outages**
   Active service downtime from cmdb_ci_outage records.
6. **Incidents**
   Active major incidents impacting business or application services.
7. **Change Requests**
   In-flight or high-risk changes touching critical services.

*Identify · prioritize · address · reassess — **the red flag count falls as resilience improves.***

13.

Backend: Main Node Configuration

For technical architects · developers

The data-layer configuration that bridges CMDB to OpRes

*What runs under the bridge — the configuration records that **drive every dependency you see in OpRes**. Configure once at the data layer, and the workspace, dashboards, and red flags inherit the structure.*

Configuration components

Main Node Configuration
Parent record. One per CSDM class. 5 OOTB: Service (CMDB), Opres with CSDM header, plus Service Offering, Business Process, Application Service

Node Relationship Configurations
Child records. Map source CMDB relationships to target OR entities. Reference the GRC Relationship Register.

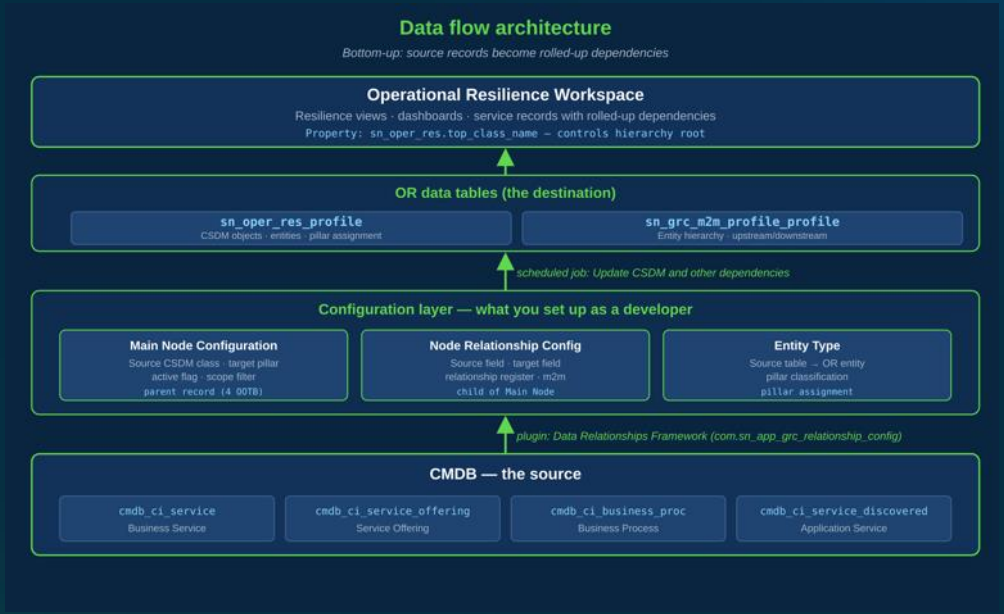
Entity Type
Defines how source records become OR entities — and assigns the pillar (service or dependency category).

Target tables & plugin

sn_oper_res_profile — CSDM objects + entities + pillar assignment
sn_grc_m2m_profile_profile — entity hierarchy, upstream/downstream parent-child
Plugin: Data Relationships Framework — com.sn_app_grc_relationship_config

Scheduled jobs

Weekly — *Update CSDM and other dependencies*
builds entity hierarchy & updates CSDM objects
Daily — *Calculate red flags for CSDM and dependencies*
aggregates counts & populates dashboard metrics



*Configuration path: All > Operational Resilience > Administration > Main Node Configurations · Test changes with the scheduled job's **Execute Now** action before relying on the next cycle.*

13.

Backend: Nexus Map Configuration

For technical architects · developers

The UI-layer configuration powering the Resilience Map

*Where Main Node ends and the visual experience begins — the configuration that turns rolled-up dependencies into **the Resilience Map's interactive view**. Same underlying data, different lenses depending on the audience.*

What Nexus Map governs

The Resilience Map — a configurable, reusable visualization component for entities, dependencies, and impact pathways across the GRC domain.

Hierarchical and interactive — users explore upstream and downstream relationships, trace risk impact, and drill into resilience posture by node.

Typical configuration parameters

- **Root / anchor entity** — The CSDM object the map renders around
- **Hierarchy depth & scope** — How far up/down the tree expands by default
- **Node visual treatment** — Colors · icons · labels · grouping by pillar
- **Edge / pathway styling** — Connection style — dependency vs containment
- **Filter & legend behavior** — Which entity types render, legend visibility

Where it sits in the stack

Main Node Config → OR data tables → **Nexus Map Config** → Resilience Map UI

Data flows in via Main Node; visual rendering is governed by Nexus Map.

Configuration path: All > Operational Resilience > Administration > Nexus Map Configurations · ***Configure once per audience or use case — no code required.***

servicenow

14.

Practical implementation insights

Tips, sequencing guidance, and common gotchas from the product documentation

Sequence matters

1

Complete IIA assessments before running scenario analysis — scenario analysis needs tolerance baselines to detect breaches. Complete tiering/assessment before self-attestation — the attestation questionnaire asks about IIA and scenario results

Operational vulnerability state constraints

4

You cannot add vulnerabilities to records in terminal assessment states (Assessment Received for IIA, Pending Analysis Approval for scenarios, Attestation Received for attestations). Create vulnerabilities before hitting those terminal states

Configure rating scales first

2

The default rating scale is cloned to each new template. Customize it before creating IIA assessments — otherwise you'll need to reconfigure per template. Rating scales live at: Admin > Importance and Impact Tolerance Rating Scale

Ops Res enriches, never overwrites

5

All Operational Resilience data is stored in its own tables (sn_oper_res_profile, etc.) — it never writes back to CMDB. This is critical implementation insight since it is most common source of confusion

Publish SAE templates before use

3

SAE templates must be published in Assessment Workspace with correct category, target, and reader role. Unpublished or miscategorized templates won't appear in the IIA, self-attestation, or operational vulnerability type dropdown

Flexible data model setup

6

Configure Main node configurations before expecting dashboard data. The weekly hierarchy job and daily red flags job must run successfully. Use sn_oper_res.top_class_name property to control which level the dashboard visualizes

Install Smart Assessment Collaboration plugin (sn_smart_collab) for contributor features in respective assessments. Install Document Templates plugin for PDF export in self-attestation and operational vulnerability management.

servicenow

15.

Meet Meridian Insurance Group

The demo customer — what you're about to see in action

*A textbook operational resilience customer — **concentrated channels, shared infrastructure, key-person risk, and a regulator watching closely**.*

Company snapshot

Market: Lloyd's of London (UK specialty insurer)

Regulators: PRA & FCA

Premium: £3.2B gross written premium

Workforce: ~2,000 employees

Lines: Commercial property · Marine cargo · Professional liability · Financial

Distribution: Broker-only (no direct-to-consumer)

Resilience tension points

Single distribution channel
Broker portal is the only path to market — outage = zero new business intake.

Shared Oracle RAC layer
ClaimsHub · PolicyCore · UnderwriteIQ share one DB — failure cascades across three business services.

Key-person concentration
CUO is sole approver for binding above £5M — no designated deputy.

Facility concentration
80% of claims handlers co-located at Glasgow Claims Centre — single facility disruption halves capacity.

The 5 business services in scope

Ranked by importance from the IIA assessment results

1 **Claims Management** *Most Critical*
FNOL · Loss adjustment · Settlement · Fraud detection

1 **Underwriting & Pricing** *Most Critical*
Risk evaluation · Quote · Bind · Renewal

1 **Broker Distribution** *Most Critical*
Sole market access channel — override demonstrated

2 **Policy Administration** *Somewhat Critical*
Issuance · Endorsements · Renewals

3 **Reinsurance Operations** *Less Critical*
Quarterly treaty placement and cession settlement

*Across IIA · Scenario Analysis · Self-Attestation · Operational Vulnerabilities — **15 operational vulnerabilities surface across the full resilience cycle.***

servicenow

15.

Demo

Six chapters · One bonus

Meridian Insurance Group walks the full operational resilience cycle

1 **SYNTHESIZE** · *The full picture*

Resilience Workspace. Services by importance, red flag rollups, interconnection map.

2 **MAP** · *The data foundation*

CMDB hierarchy — business services, offerings, processes, applications, dependencies. Dependency Map, Resilience Map, 360° view, Go to Entity.

3 **ASSESS** · *The resilience baseline*

IIA on Meridian's 5 services. SAE auto-scores across four tolerance dimensions. Override Claims Management with mandatory justification.

4 **TEST** · *Stress-testing the services*

Ransomware Attack on Slough Data Centre — Retake. Dual approval, multi-departmental input, breach detection with duration overlaps.

5 **CERTIFY** · *The auditor-ready artifact*

Self-attestation referencing earlier chapters. Signed PDF with e-signature.

6 **REMEDIATE** · *Closing the gaps*

Operational vulnerabilities surfaced. SAE-powered impact assessment, treatment decision, action tasks for parallel remediation.

BONUS **Configure** · *How it's wired together* *(For architects & developers)*

Backend tour. SAE Template Designer. Main Node & Nexus Map Configurations. Scheduled jobs. Data Relationships Framework.

Based on Australia release and app version 22.x.x

The contents of this demo are intended to remain relevant for future version releases.

servicenow

16.

Key takeaways

The architectural mental model from the entire session — six points to take with you

The mental model — WHAT vs HOW

IIA, Scenario Analysis, Self-Attestation, and Operational Vulnerability are the four capabilities — the what. SAE is the engine — the how. Three of four are SAE-powered; scenario analysis is the exception with its own event model.

Resilience is a closed loop, not a checklist

Assess → Test → Certify → Remediate → Reassess. Five stages, continuously cycling. A discipline you maintain, not a project you finish.

IIA is the scoring foundation

Importance plus four tolerance dimensions feed everything downstream — scenario breach detection, self-attestation, OV impact assessment, dashboards. Get IIA right and the rest gets easier.

Breach detection is the critical intersection

Scenario analysis compares disruption duration to IIA tolerance thresholds. Where Test meets Assess — the moment the cycle proves itself.

Operational Resilience is distinct from BCM

OR measures and tests resilience. BCM plans for recovery. Complementary disciplines, not interchangeable products.

OR enriches CSDM, never overwrites it

All Operational Resilience data lives in its own tables. The CMDB stays the source of truth; OR is the resilience lens layered on top.

16.

FAQs

The questions that come up most often when teams start with Operational Resilience

Setup & Foundation

Do I need CSDM v4 or v5 to use Operational Resilience?

Recommended for new deployments. Legacy cmdb_ci_service installations are still supported via the Service (CMDB) Main Node Configuration, but modern CSDM (v4 or v5) unlocks resilience views and roll-ups.

Does OR require BCM?

No. BCM is optional but complementary — OR measures and tests, BCM plans recovery.

Scenario Analysis

Why doesn't scenario analysis use SAE?

It has its own event/participant model. But its outputs feed SAE-powered OV impact assessment downstream.

How does breach detection work?

Compares total disruption duration against IIA tolerance thresholds. Deviation % shows the overshoot.

IIA & Smart Assessment

What are the four tolerance dimensions?

Duration, customer impact, financial impact, and transactional volume. Each can be scored independently within a single assessment.

Can I customize the rating scale?

Yes — but customize it before creating templates. The default rating scale clones to each new template at creation; changes after don't propagate.

What happens if an IIA is rejected?

SAE reverts the assessment to Pending Response for retake. Legacy assessments don't support retake.

Data & Architecture

Does Operational Resilience write back to CMDB?

No. OR data lives in its own tables; CMDB remains the source of truth.

When can I add operational vulnerabilities to an assessment?

Before the assessment hits a terminal state — Assessment Received for IIA, Pending Analysis Approval for scenarios, Attestation Received for attestations.

Where can operational vulnerabilities be raised from?

Six sources: IIA, scenario, self-attestation, service records, Employee Center, and manually in the workspace.

16.

Resources

Curated learning paths to deepen your Operational Resilience expertise

Product Documentation

Start here for authoritative product info

- **Operational Resilience docs**
  servicenow.com/docs/r/governance-risk-compliance/operational-resilience-dashboard
- **OR product overview & solution brief**
  servicenow.com/products/operational-resilience.html
- **CSDM framework (v5)**
  servicenow.com/platform/common-services-data-model.html

Practical Guides

Step-by-step from the field & community

- **Smart Assessment Simplified Guide**
  community.servicenow.com (Hemanth M, ServiceNow MVP)
- **Smart Assessment Engine Blog Series**
  community.servicenow.com — GRC articles
- **SAE Webinar Recording**
  community.servicenow.com — GRC blog

Stay Connected

Ongoing learning, releases, and peers

- **ServiceNow GRC Community**
  community.servicenow.com/governance-risk-and-compliance
- **ServiceNow Store — Operational Resilience**
  store.servicenow.com (com.sn_grc_oper_res)
- **Latest GRC release highlights**
  servicenow.com/docs/r/store-release-notes/store-grc-rn-operational-resilience

Keep building. Keep learning. Keep the resilience cycle going.

servicenow

servicenow

Thank you