

FOR FCA-REGULATED FIRMS

Operational resilience in **Halo**.

How it works, screen by screen.

From important business services and impact tolerances to the FCA's 24-hour incident clock and the material third-party register: how HaloNinjas sets up the Halo Platform so the evidence comes out of everyday work.

**18 Mar
2027**

FCA PS26/2 applies

24 h / 4 h

To report serious incidents

**50+
fields**In the FCA's third-party
register**INSIDE**

- 2 Why now: the rules and the dates
- 3 The model: important business services
- 4 Incidents: two clocks and a decision
- 5 Problems and changes
- 6 Third parties: the register as a report
- 7 Testing and the board view
- 8 What changes for end users and agents
- 9 How we deliver, and the next step

Two sets of rules. One deadline that matters.

The operational resilience rules have been fully in force since 31 March 2025, when the transition ended. The reporting rules that put a clock on every serious incident apply from 18 March 2027.



An incident is reportable when it risks

- **Intolerable harm to consumers** that they cannot easily recover from
- **The safety and soundness** of the firm or other market participants
- **Market stability, integrity or confidence** in the UK financial system

Where firms struggle

Not with the rules, with the evidence. Incident timelines sit in the service desk, change approvals in email, supplier contracts in a shared drive, and the mapping in a spreadsheet nobody has opened since the self-assessment. When the clock starts, assembling that takes longer than 24 hours.

The rest of this document shows how we set Halo up so the evidence is a by-product of the work your teams already do.

Two reporting tiers

Enhanced: banks, insurers and other dual-regulated firms, enhanced-SMCR firms and payment service providers. An initial report within 24 hours (4 for PSPs), intermediate updates on any significant change, and a final report within 30 working days of resolution.

Standard: other solo-regulated firms. One report within 24 hours. In Halo each stage is a task with its own timer, so nothing depends on someone remembering.

What a supervisor will ask to see

- Your important business services and their impact tolerances
- The mapping: people, processes, technology, facilities, information, third parties
- Scenario test results and the actions they produced
- Incident timelines, with the time you decided an incident was reportable
- The register of material third parties and your exit plans

Important business services sit at the top.

Everything else in Halo connects to them. Once incidents, changes, suppliers and tests all link to a service, resilience evidence is a filter, not a project.



Configuration > Services > Make a payment
Edit

Make a payment
Important business service
Within tolerance

Resilience details

Accountable SMF	A. Fictional, SMF24
Impact tolerance, FCA client harm	2 hours
Impact tolerance, FCA market integrity	N/A
Impact tolerance, PRA safety and soundness	4 hours
Harm rationale	Customers unable to pay bills or wages
Data owner	Payments Operations
Last scenario test	12 Aug 2026 · Passed
Next mapping review	12 Nov 2026

Dependencies (from the CMDB)

Technology	Payments gateway	Operational
Technology	Core banking API	Operational
Technology	Fraud screening service	Operational
People	Payments operations team (6)	Staffed
Third party	Acme Payments Ltd · CTR-0217	Material
Third party	CloudHost Ltd · CTR-0190	Material
Facility	Glasgow data centre	Operational
Information	Customer account data	UK, Ireland

Illustrative mock-up of a HaloITSM service record configured for resilience. Not a product screenshot.

Six tolerance fields

One per regulator, in hours or N/A: FCA client harm, FCA market integrity, PRA safety and soundness, PRA financial stability, PRA policyholder protection, Bank of England FMI. They feed the clocks and the register.

Six dependency types

People, processes, technology, facilities, information and third parties, as SYSC 15A asks. Held in the CMDB, so an incident on any one of them finds the service it supports.

Status is computed

Open major incidents on a dependency roll up to the service. The same status shows on the self-service portal, the agent view and the board dashboard.

Two clocks and a recorded decision.

Log an incident against any system and Halo finds the important services it affects. A major incident then runs a tolerance clock, a reporting clock and a regulatory assessment, with every answer timestamped.

Tickets > INC-0004120
Update

INC-0004120 · Payments gateway degraded
Major incident
Affects: Make a payment
Stage: Escalated

Timeline

08:34 Monitoring alert: gateway latency > 8s. Disruption start recorded.

08:41 Major incident declared. Service owner and SMF notified.

09:12 Logged to supplier Acme Payments Ltd (ref ACM-55821).

09:46 Regulatory assessment completed: reportable. FCA clock started.

09:52 Customer status page updated: Degraded.

Impact tolerance · Make a payment

2 hours from disruption start at 08:34 · 1 h 24 m used

Escalated at 50% · next at 75% **36 m remaining**

FCA report

24 h from determination at 09:46 · Compliance lead

Enhanced tier · initial report **23 h 48 m remaining**

Tasks

Submit FCA report via FCA Connect **Due 09:46 tomorrow**

Hourly customer update **Recurring**

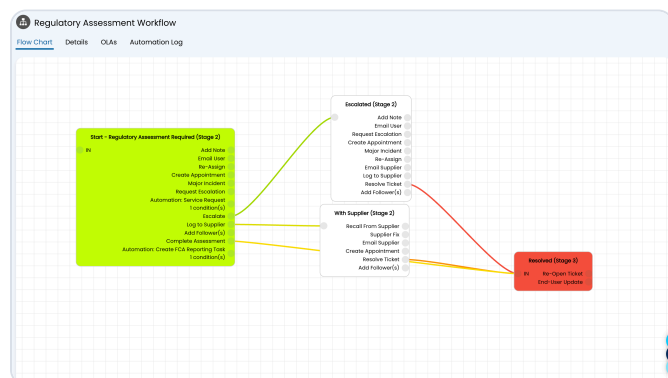
Intermediate update to FCA **On significant change**

Final report to FCA **30 working days after resolution**

Regulatory assessment

Intolerable consumer harm	Met
Safety and soundness	Not met
Market integrity	Not met
Reportable	Yes · 09:46 · Compliance lead
Linked events	None · problem PRB-0310 open

Illustrative mock-up of a major incident in HaloITSM with resilience SLAs and a regulatory assessment. Not a product screenshot.



Screenshot from the HaloNinjas demo instance: the Regulatory Assessment workflow that drives the assessment, escalation and FCA reporting task.

What the clocks are

- **Tolerance:** a 24/7 SLA on a child ticket, set from the service's tolerance, starting at disruption start and never paused.
- **Reporting:** an SLA on the "Submit FCA report" task, 24 hours from determination, or 4 hours from detection for payment firms. Enhanced-tier firms get intermediate and final-report tasks too, the final one 30 working days after resolution.
- **Reassessment:** if the incident escalates or passes 75% of tolerance, the assessment reopens automatically.

Linked events, and change you can defend.

PS26/2 treats a series of linked events as one incident. Problem records group them and carry their own assessment. Any change touching a system behind an important service gets a higher risk rating, the service owner's approval and a blackout check.

Tickets > CHG-0001842

Submit for approval

CHG-0001842 · Patch core banking API to v4.2

Normal change

Affects: Make a payment

Risk: High

Impact analysis

Affected CI	Core banking API
Supports important service	Yes · Make a payment
Risk	Raised to High automatically
Rollback plan	Attached · tested 2 Oct

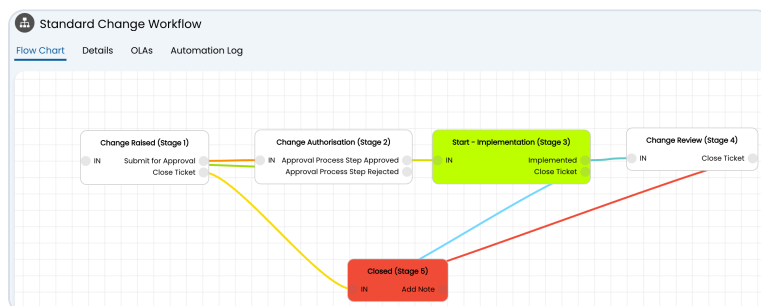
Approvals

CAB	Approved 13 Oct
Service owner (required)	Pending
Accountable SMF	Informed
Supplier (Acme Payments)	Confirmed

Schedule

Requested	29 Oct 02:00
Blackout check	Month-end freeze 28–31 Oct
Proposed	3 Nov 02:00
Audit trail	11 entries · full audit trail

Illustrative mock-up of a change record in HaloITSM with resilience controls. Not a product screenshot.



Screenshot from the HaloNinjas demo instance: the Standard Change workflow, raised, authorised, implemented, reviewed, closed.

Why this matters for the self-assessment

- Every approval, vote and status change is in Halo's audit trail, which is the evidence of controlled change supervisors ask for.
- Linked incidents under one problem can be assessed together: several small outages may be reportable as a series even if none is on its own.
- The change calendar per service stops risky work landing on month-end, payroll or a known peak.

Tickets > PRB-0310

Reassess as series

PRB-0310 · Intermittent payment gateway timeouts

Affects: Make a payment

Series: reportable

Linked incidents

INC-0003655 · 2 Sep · 31 min · not reportable alone	Closed
INC-0003902 · 24 Sep · 1 h 37 m · 81% of tolerance	Closed
INC-0004120 · 14 Oct · in progress	Major

Combined assessment

Common root cause	Supplier certificate rotation
Assessed as a series	Yes · 14 Oct 10:20 · Compliance
Supplier RCA requested	Due 21 Oct

Illustrative mock-up of a problem record grouping linked incidents for a combined assessment. Not a product screenshot.

The register as a report, not a project.

The FCA's register runs to more than 50 fields and is filed per contract. We hold them on Halo's supplier contract record, using the FCA's own field names and numbering, so the annual submission is an export.

Suppliers > Acme Payments Ltd > Contracts > CTR-0217
Export register row

CTR-0217 · Payment gateway services
Material third party
Compliant
Supports: Make a payment

Contract FCA 2.xx

2.04 Outsourcing Outsourcing
2.05 Type of service Payment processing
2.06 Cloud model Public cloud
2.08 Supply chain rank 1
2.09 / 2.11 Start / renewal 1 Apr 2024 / 31 Mar 2027
2.12 / 2.13 Notice 90 / 180 days
3.15 Annual value £248,000

Materiality FCA 3.xx

3.01 Reason Supports an IBS
3.02 Assessed 15 Jul 2026
3.05 Service Make a payment
3.06 Core element Yes
3.10 Tolerance, client harm 2 h (from service)
3.13 Data stored in UK, Ireland
5.01 Substitutability Difficult

Assurance FCA 4.xx · from review tickets

4.01–4.02 Risk assessment 12 Aug 2026 · Satisfactory
4.04–4.05 Audit 3 Mar 2026 · Satisfactory
4.06–4.07 Financial DD 3 Mar 2026 · Satisfactory
4.08–4.09 Cyber DD 22 Jun 2026 · Minor findings
4.12 SMF sign-off Yes · 15 Jul 2026
Next review Cyber DD · due 22 Dec 2026

Illustrative mock-up of a supplier contract record in HaloITSM carrying the FCA register fields. Not a product screenshot.

Annual register export

2.01 Ref	2.02 Provider	2.05 Service	3.01 Materiality	3.05 IBS	3.10 Tol. (h)	4.02 Risk outcome	4.12 SMF	5.01 Subst.
CTR-0217	Acme Payments Ltd	Payment processing	Supports an IBS	Make a payment	2	Satisfactory	Yes	Difficult
CTR-0190	CloudHost Ltd	Cloud hosting	Supports an IBS	Make a payment; Log in	2	Satisfactory	Yes	Medium
CTR-0233	Northbridge KYC Ltd	Identity verification	Supports an IBS	Open an account	24	Needs improvement	Yes	Easy

Columns follow the FCA template order (1.02 to 5.03), run for contracts that were active on 31 December, and submitted within the FCA's 90-day window.

How it stays current without a spreadsheet

1 · New supplier request

Every new-supplier request runs a materiality assessment. If the answer is material, Halo raises a "Notify FCA" task and holds approval until it's done, so nobody signs before the regulator has been told.

2 · Scheduled reviews

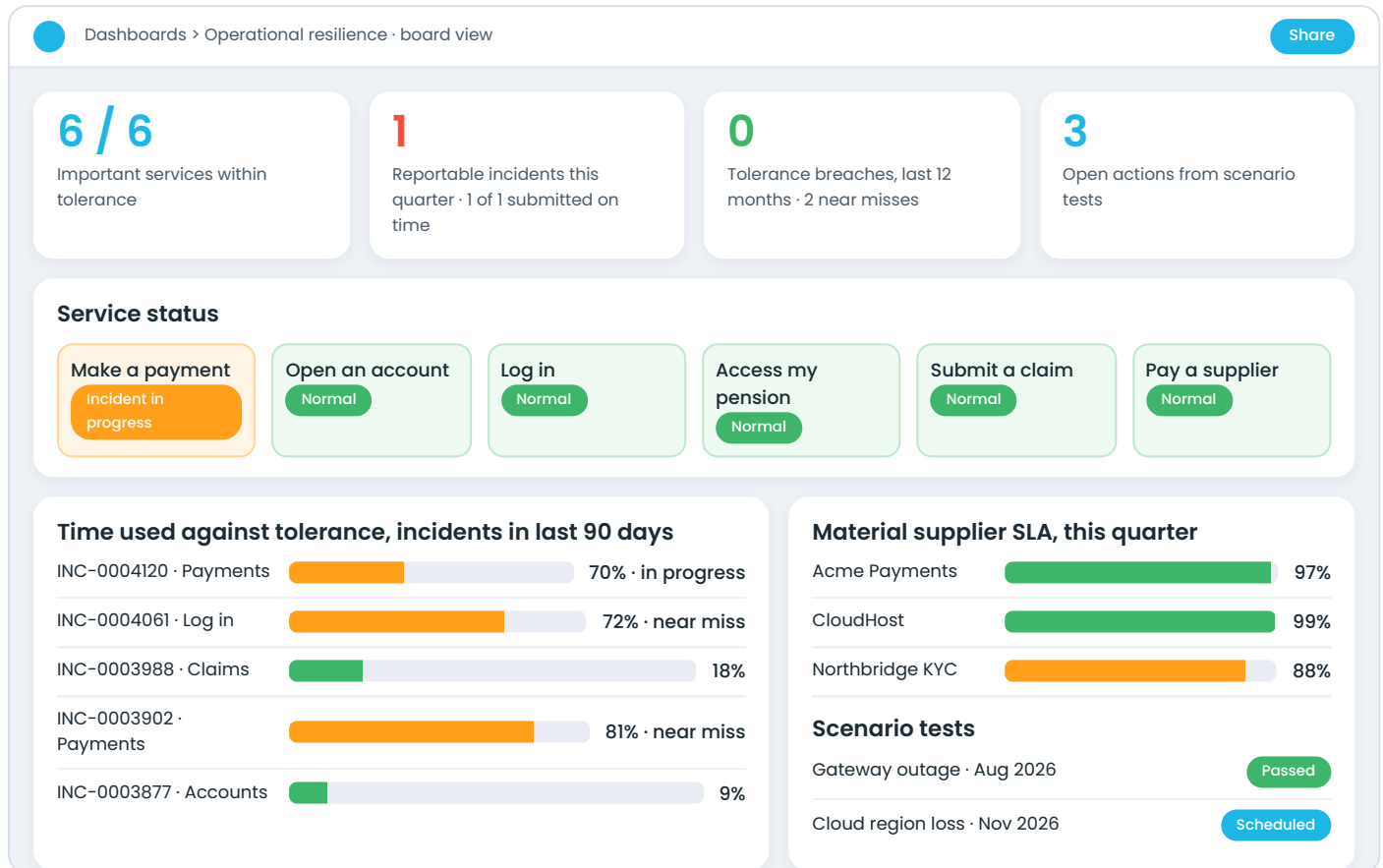
Risk, audit, financial and cyber reviews are recurring tickets. Closing one writes its date and outcome (fields 4.01 to 4.09) back to the contract. SMF sign-off is the approval step, which sets 4.12 and 4.14.

3 · Renewals and exits

The renewal workflow asks whether anything significant changed (1.07) and re-notifies if so. Substitutability, reintegration and discontinuation (5.01 to 5.03) are reviewed with the exit plan each year.

One dashboard for the Senior Manager.

Scenario tests are tickets. Their findings become actions with owners. Together with incident, change and supplier history, they feed a live view that replaces the quarterly slide deck.



Illustrative mock-up of a resilience dashboard built from HaloITSM widgets. Not a product screenshot. All figures are example data.

Scenario tests as tickets

Plan
 A test ticket names the service, the scenario (severe but plausible), the tolerance being tested and who takes part.

Run
 Timings are recorded against the tolerance as the test runs, the same way a real incident would be.

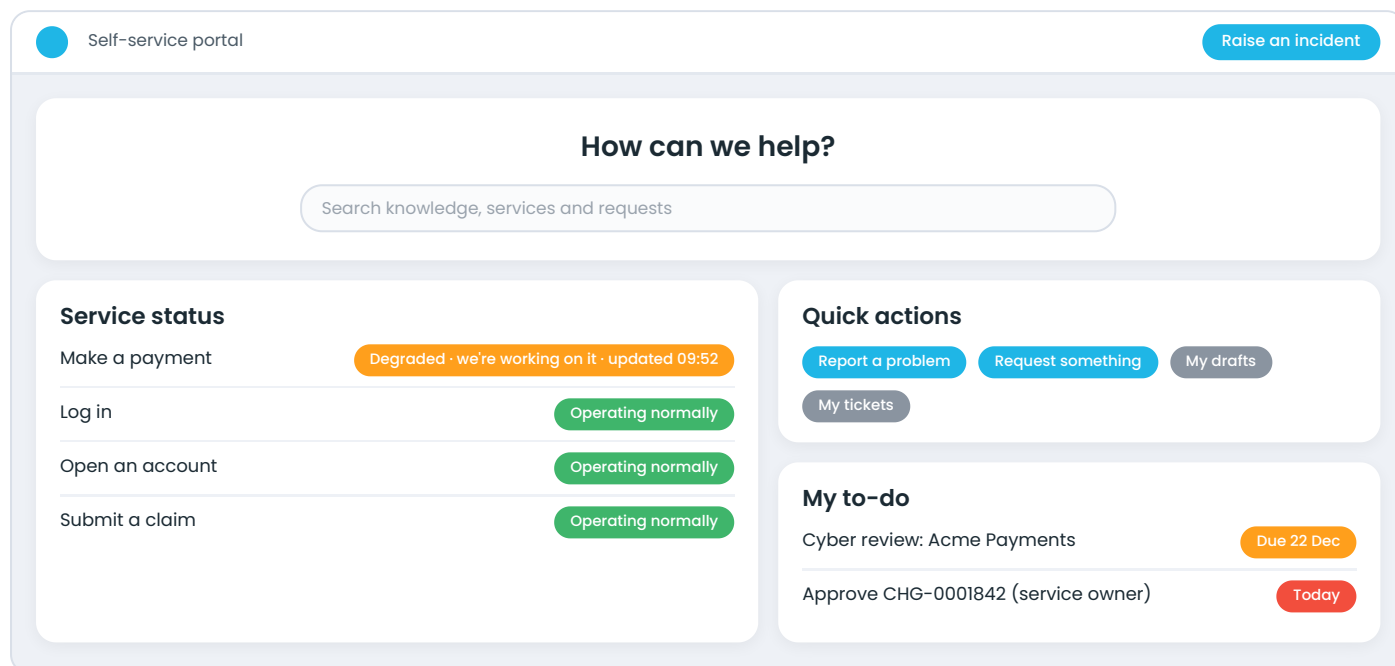
Act
 Each finding becomes an action with an owner and a due date. Open actions appear on the dashboard until closed.

What the self-assessment pulls from Halo

- Services, tolerances and dependency maps, with review dates
- Every incident that touched an important service, with time used against tolerance
- Reportable incidents, with the decision, the decision-maker and the submission time
- Scenario tests, results and the actions they produced
- Changes to systems behind important services and who approved them

What changes for the people using it.

Resilience shouldn't add work. End users see honest service status and can report problems in one place. Agents see business impact and the clocks on the ticket they're already working.



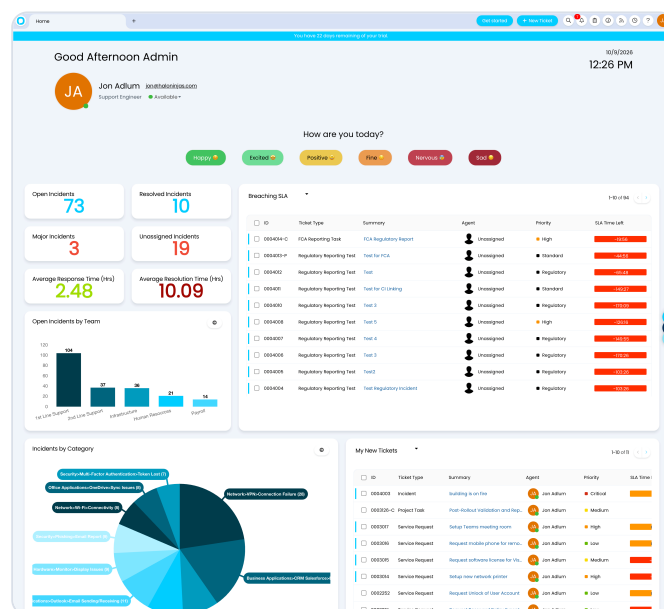
Illustrative mock-up of the HaloTSM self-service portal with the service status widget and to-do items. Not a product screenshot.

For end users and customers

- Service status by important business service, in plain words, on the portal and on ticket dashboards.
- One place to report a problem; the CMDB works out which service it affects.
- Service owners and supplier managers get their resilience tasks as to-do items they can complete from the portal.

For agents and the resilience team

- Business impact, the tolerance clock and the reporting clock appear on the incident itself, not in a separate tool.
- The regulatory assessment is a required step on major incidents; the ticket can't move on without it.
- Review tickets write assurance dates and outcomes back to the supplier contract, so the register stays current without anyone maintaining it.



Screenshot from the HaloNinjas demo instance: the agent home screen, with open and major incidents, breaching SLAs and the team's queue. The board view on page 7 is built from the same widgets. Figures are test data.

Four phases. Two before March 2027.

We start from your existing Halo instance, or plan the move from another platform around these phases.

PHASE 1 · PRIORITY

Discovery workshop

Confirm your important business services, tolerances, reporting tier, firm type and whether the third-party rules apply to you.

PHASE 2

Service model and CMDB

Build the service records, map dependencies across people, technology, facilities, information and third parties; add discovery where the estate needs it.

PHASE 3 · PRIORITY

Incident, problem and change

Configure the clocks, the regulatory assessment, reporting tasks and change controls, then run a practice major incident end to end.

PHASE 4

Suppliers, testing, dashboards

The register fields and export, supplier onboarding checks, scenario test records and the board view.

See it on your own services.

Book a 30-minute resilience session. We'll take two of your important business services and show what the evidence would look like in Halo.

haloninjas.com/resilience · jon@haloninjas.com

Book 30 minutes

Why HaloNinjas

Scotland's pure-play Halo partner, a HaloITSM Certified Partner, delivering in the UK, EMEA and North America. We only work on Halo, and the senior people who design your setup are the ones who build it.

Please note

Halo is the record and the workflow. Your firm owns its regulatory judgement and submits its own reports. Screens marked as mock-ups show configurations we build in HaloITSM and are illustrative; they are not product screenshots, and the data in them is invented. This document is general information, not legal advice.

Sources: FCA PS26/2, FG26/3 and FG26/4 (March 2026); FCA SYSC 15A. HaloITSM is a product of Halo Service Solutions.