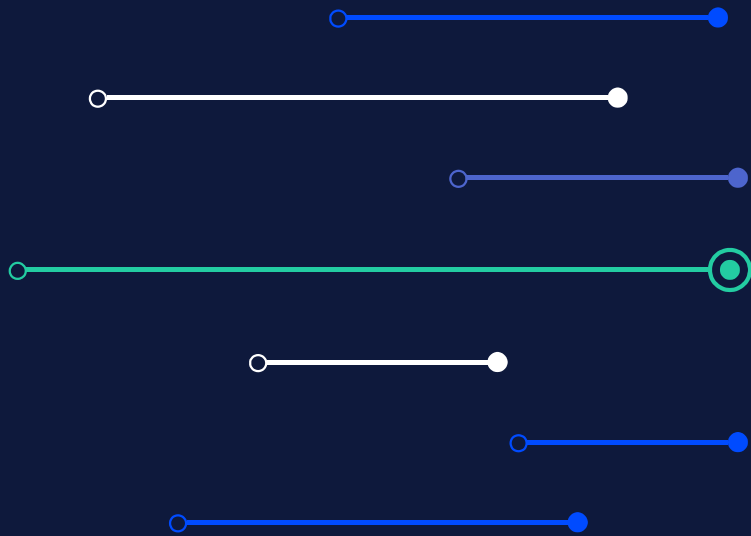




RISK AND GRC TOOLKIT

The Policy Exception Management Kit

Make every exception audit evidence, not an audit finding.

Eight tools for risk, compliance and security teams: a process health check, request form, risk assessment worksheet, approval matrix, compensating controls test, exception register, expiry playbook and audit-ready checklist.

Nick Rafferty, CEO and Co-Founder, SureCloud

Technically reviewed by Gabriel Few-Wiegratz, [job title], SureCloud

Version 1.0 · August 2026

How to use this kit

Who it's for

Risk managers, compliance leads and CISOs who approve, track or defend policy exceptions. And the business units who need a clear, fair way to ask for one.

How it works

Start with the health check. It takes ten minutes and tells you which tools to open first.

Every tool is built to be printed, copied into your own templates, or rebuilt inside your GRC platform. The request form and exception register are also available as a spreadsheet: [\[link to companion template\]](#).

What you'll have at the end

- **One front door.** Every request comes through the same form, with the same information.
- **One set of rules.** Risk-based approval tiers, agreed in advance and applied every time.
- **One register.** Every exception owned, dated, reviewed and closed.

CONTENTS

	Why exceptions become audit findings	3
Tool 01	Process health check	4
Tool 02	Exception request form	5
Tool 03	Risk assessment worksheet	6
Tool 04	Approval authority matrix	7
Tool 05	Compensating controls test	8
Tool 06	Exception register	10
Tool 07	Review and expiry playbook	12
Tool 08	Audit-ready checklist	13
	What frameworks expect, and where to start	14
	Where SureCloud fits	15



An exception with an end date is governance. One without is a policy change nobody approved.

Exceptions aren't the risk. Unmanaged exceptions are.

Every organisation grants exceptions. Legacy systems that can't meet the encryption standard yet. A critical supplier still working towards your security requirements. A migration that needs temporary access. A go-live that lands before the training does.

None of that is a failure. The failure is granting them inconsistently, with no evidence and no plan to resolve them.

● Violation

Unapproved. Undocumented. Open-ended.
Evidence of a governance gap.

✓ Exception

Formally approved. Documented. Time-bound. Conditional on compensating controls or a remediation plan. Evidence of active risk management.

01 ●

Decisions made in email

Approvals happen in a thread. Nobody can say later who agreed, on what basis, or at what level. The auditor has to reconstruct it.

02 ●

Compensating controls nobody checks

"Extra monitoring" gets written down and never verified. The exception is live. The control may not be.

03 ●

End dates that never arrive

No expiry date, or one that passes unnoticed. The temporary deviation quietly becomes the way things are done.

EXPERT VIEW

"The exceptions that cause problems are rarely the risky ones. They're the ones nobody set an expiry date on. A register full of live exceptions with clear owners and dates tells an auditor more about your governance than a register with none."

Matt Davies, Chief Product Officer, SureCloud

Process health check

Find out whether your exceptions would hold up under audit today.

Use it when
before your next audit or risk committee

Time needed
10 minutes

Owner
risk or compliance lead

Score each statement honestly. **0** = no. **1** = partly, or true but not evidenced. **2** = yes, and we could show an auditor today.

#	Statement	0	1	2	Fix with
1	We have a written policy defining how exceptions are requested, assessed, approved and reviewed.	☐	☐	☐	Tool 08
2	Every exception request comes through one standard form or workflow.	☐	☐	☐	Tool 02
3	Every request names the specific policy, control or clause affected.	☐	☐	☐	Tool 02
4	Every request is assessed against our risk appetite before it is approved.	☐	☐	☐	Tool 03
5	We check whether the control is a legal or regulatory baseline before treating it as an internal exception.	☐	☐	☐	Tool 03
6	Approval authority is tiered by risk level, with criteria agreed in advance.	☐	☐	☐	Tool 04
7	Every approval in the last 12 months was made at the right tier.	☐	☐	☐	Tool 04
8	Every compensating control is specific, measurable and has a named owner.	☐	☐	☐	Tool 05
9	Compensating controls are verified as operating before the exception starts.	☐	☐	☐	Tool 05
10	Every exception has an expiry date.	☐	☐	☐	Tool 06
11	Every exception sits in one register, linked to the risk register.	☐	☐	☐	Tool 06
12	We review every exception before it expires, and extensions need a fresh assessment.	☐	☐	☐	Tool 07

Your score:

/ 24

0 to 8

● Exceptions by email

Decisions are happening, but the evidence isn't. Start with Tool 02 and Tool 06. Get every live exception into one register before you change anything else.

9 to 16

A process on paper

The rules exist but aren't applied consistently. Start with Tool 04 and Tool 05. Consistent tiers and verified controls fix most audit findings.

17 to 24

✓ Audit-ready

Keep it that way. Start with Tool 07 and Tool 08, and check that expiry reviews are happening on time, every time.

Exception request form

One front door. Complete information, every time, so approvers aren't negotiating.

Use it when
any time a policy or control can't be met

Time needed
15 minutes to complete

Owner
requester, with the risk owner

A. Request details

Exception ID (assigned by risk team)

Date submitted

Requester name and role

Business unit

B. The deviation

Policy or control affected (name and clause or reference)

Framework references affected, if known (for example ISO/IEC 27001 Annex A control, PCI DSS requirement)

What is the deviation, in plain language?

Why can't the requirement be met today? Attach supporting evidence.

Scope: which systems, processes, people or business units are affected?

C. Duration and exit

Proposed start date

Proposed end date

What has to happen for this exception to close? Include the remediation plan and target date.

D. Proposed compensating controls

Control	How it will be measured	Owner (named individual)	Verified operating (date and evidence)

E. Accountability

Risk owner (named individual accountable for this exception)

Risk owner signature

Date

F. For risk team use only

Residual risk rating ☐ Low ☐ Medium ☐ High ☐ Critical

Within risk appetite ☐ Yes ☐ No

Regulatory baseline control ☐ Yes ☐ No

Approval tier required

Decision ☐ Approved ☐ Approved with conditions

☐ Rejected

Approver name and role

Approval date

Expiry date

First review date

Risk assessment worksheet

Decide on residual risk and appetite, not on how persuasive the request is.

Use it when
before any exception is approved

Time needed
20 to 30 minutes

Owner
risk manager

1 Exposure without the control

Likelihood (1 to 5) _____ Impact (1 to 5) _____ Score _____

2 Effect of compensating controls

Which controls reduce likelihood?

Which controls reduce impact?

3 Residual risk

Likelihood after controls (1 to 5) _____

Impact after controls (1 to 5) _____

Residual score _____ Rating: ☐ Low ☐ Medium ☐ High

☐ Critical

4 Risk appetite check

Is the residual risk within our risk appetite for this category?

☐ Yes ☐ No

Appetite statement referenced

5 Regulatory baseline check

Is this control a legal or regulatory obligation in its own right, whatever our internal policy says?

☐ Yes ☐ No

Examples: the ten risk-management measures in NIS2 Article 21(2), the ICT risk management requirements of DORA, security of processing under UK GDPR Article 32, a PCI DSS requirement.

If yes, route to compliance or legal before approval.

Likelihood × impact

		1	2	3	4	5
5	5	10	15	20	25	
4	4	8	12	16	20	
3	3	6	9	12	15	
2	2	4	6	8	10	
1	1	2	3	4	5	
		1	2	3	4	5

Likelihood

Impact

Example calibration

- ☐ 1 to 4: Low
- ☐ 5 to 9: Medium
- ☐ 10 to 15: High
- ☐ 16 to 25: Critical

Example scoring only. Use your organisation's own risk methodology and appetite statements.

Outside appetite means no.

If residual risk sits outside appetite, the request is declined, however strong the business case.

Borderline goes up, never down.

If the rating is borderline, escalate to the next approval tier.

Approval authority matrix

Authority that scales with risk. Agreed in advance, applied every time.

Use it when
setting up the process, then at every approval

Time needed
1 hour to agree

Owner
Head of Risk, ratified by risk committee

Residual risk	Approval authority	Maximum duration	Extensions approved by	Reported to
 Critical	Board or executive sign-off	_____ days	_____	Board
 High	Risk committee or equivalent governance body	_____ days	_____	Risk committee
 Medium	Head of Risk or CISO	_____ days	_____	_____
 Low	Risk or Compliance Manager	_____ days	_____	_____

90 days is a reasonable starting point for operational exceptions. Set the shortest period that is genuinely necessary.

Rules that apply at every tier

1

Criteria first.

Define what makes an exception Low, Medium, High or Critical before the first request arrives.

2

No self-approval.

The requester and the risk owner never approve their own exception.

3

Borderline goes up.

When in doubt, the higher tier decides.

4

Extensions are new decisions.

Every extension needs a fresh risk assessment and re-approval at the tier that assessment points to.

5

Bypassing the tier is a finding.

Even when the deviation itself was reasonable.

6

Repeat exceptions are a signal.

Three or more exceptions against the same control means the policy owner should review the policy.

Our tier criteria

Low

Medium

High

Critical

Ratified by

Date

Compensating controls test

Vague commitments don't satisfy auditors. Three tests every compensating control must pass.

Use it when

before approval, and again before the exception starts

Time needed

5 minutes per control

Owner

risk owner, checked by risk team

1

Test 1
Specific and measurable

It names exactly what will happen, to what, and how often. Someone else could check whether it's working.

2

Test 2
Named owner

One named individual is responsible for operating it. Not a team. Not "IT".

3

Test 3
Verified before start

Evidence shows it is operating before the exception begins, wherever that's possible. No verified control, no start date.

Control check

Control: _____

- ☐ Says what, where and how often
- ☐ Has a measure someone else could check
- ☐ Has one named owner: _____
- ☐ Verified operating on _____ with evidence: _____
- ☐ Evidence saved to the exception record

Worked pair: legacy system can't meet the encryption standard

Weak

"Extra monitoring on the legacy server until the upgrade."

Strong

"Server moved to an isolated network segment. Access restricted to [two] named administrator accounts with MFA. File integrity monitoring alerts reviewed daily by [role]. Sensitive data not needed on the server removed by [date]. Verified [date] with firewall rule export and alert log."

Weak vs strong: three more common exceptions

Supplier not yet meeting your vendor security requirements

● Weak

"The supplier has confirmed they're working on it."

✔ Strong

"Supplier access limited to [system] through [privileged access tool] with session recording. No customer personal data shared until remediation is complete. Signed remediation plan with milestones received [date]. Progress checked fortnightly by [vendor risk manager]."

Temporary access during a system migration

● Weak

"We'll keep a close eye on access during the migration."

✔ Strong

"Elevated access granted to [five] named migration engineers only, logged in [monitoring tool]. Privileged activity reviewed daily by [role]. Access removed automatically on [date], confirmed by [role] the same day."

Mandatory training not complete before go-live

● Weak

"The team will complete the training shortly after launch."

✔ Strong

"Team briefed on [key risks] before go-live, with attendance recorded. Production access limited to [supervised or read-only] until training is complete. Completion by [date], tracked weekly by [role]."

Handling card data? PCI DSS sets its own bar. Compensating controls are only permitted where there is a legitimate technical or documented business constraint, and they must meet the intent and rigour of the original requirement. Document them the way your assessor expects, and expect them to be evaluated at every annual assessment.

Exception register

The central record of every live and past exception. A living document, not an archive.

Use it when
every exception, from request to closure

Time needed
set up in an hour

Owner
risk team

Field	What it captures	Worked example
Exception ID	Unique reference for tracking and audit	EX-2026-014
Policy or control reference	Specific policy, control or framework clause	Cryptography policy s.4.2 · ISO/IEC 27001 A.8.24
Requesting business unit	Team or department that submitted it	Finance systems
Risk owner	Named individual accountable	[Name], Head of Finance Systems
Description of deviation	Plain-language summary and rationale	Legacy ledger server can't support current encryption standard until the platform upgrade
Risk assessment summary	Residual risk rating and key findings	Medium. Exposure limited by network isolation and restricted access
Compensating controls	Specific controls with named owners	Network isolation, MFA for two admin accounts, daily integrity alert review ([name])
Approval authority	Who approved it, and in what role	[Name], CISO
Approval date	Date of formal approval	[Date]
Expiry date	Date it lapses and must be reviewed or closed	[Date + 90 days]
Status	Active, Under review, Closed or Escalated	Active
Review notes	Interim reviews, extensions, control changes	Day 45 review: controls operating, upgrade on track
Resolution	Remediated, escalated or converted to a policy change	[Pending]



Link each exception to the risk it represents in your risk register. Exceptions are open risk decisions and belong alongside your other open items, not in a separate silo.

Keeping the register honest

Status definitions

Active

approved, within its dates, compensating controls verified.

Under review

approaching expiry or triggered for review. Decision pending.

Escalated

controls failing, root cause unresolved, or outside appetite. Awaiting a higher-tier decision.

Closed

resolved, with the resolution method and evidence recorded.

Three ways an exception ends

Remediated

the underlying issue is fixed and the original control is operating.

Escalated

the root cause remains. It is recorded as a risk in the risk register and decided at a higher tier.

Converted to a policy change

the deviation is the right answer long term, so the policy changes through the normal policy change process.

Five monthly register checks

- ☐ Any exception past its expiry date still marked Active
- ☐ Any exception without a named risk owner or compensating control owner
- ☐ Any exception extended more than once
- ☐ Any control with three or more exceptions against it
- ☐ Any exception approved below the tier its risk rating requires

Run these five checks before every risk committee. Each one is a question an auditor is likely to ask.

Review and expiry playbook

Every exception gets a decision before its end date. Never after.

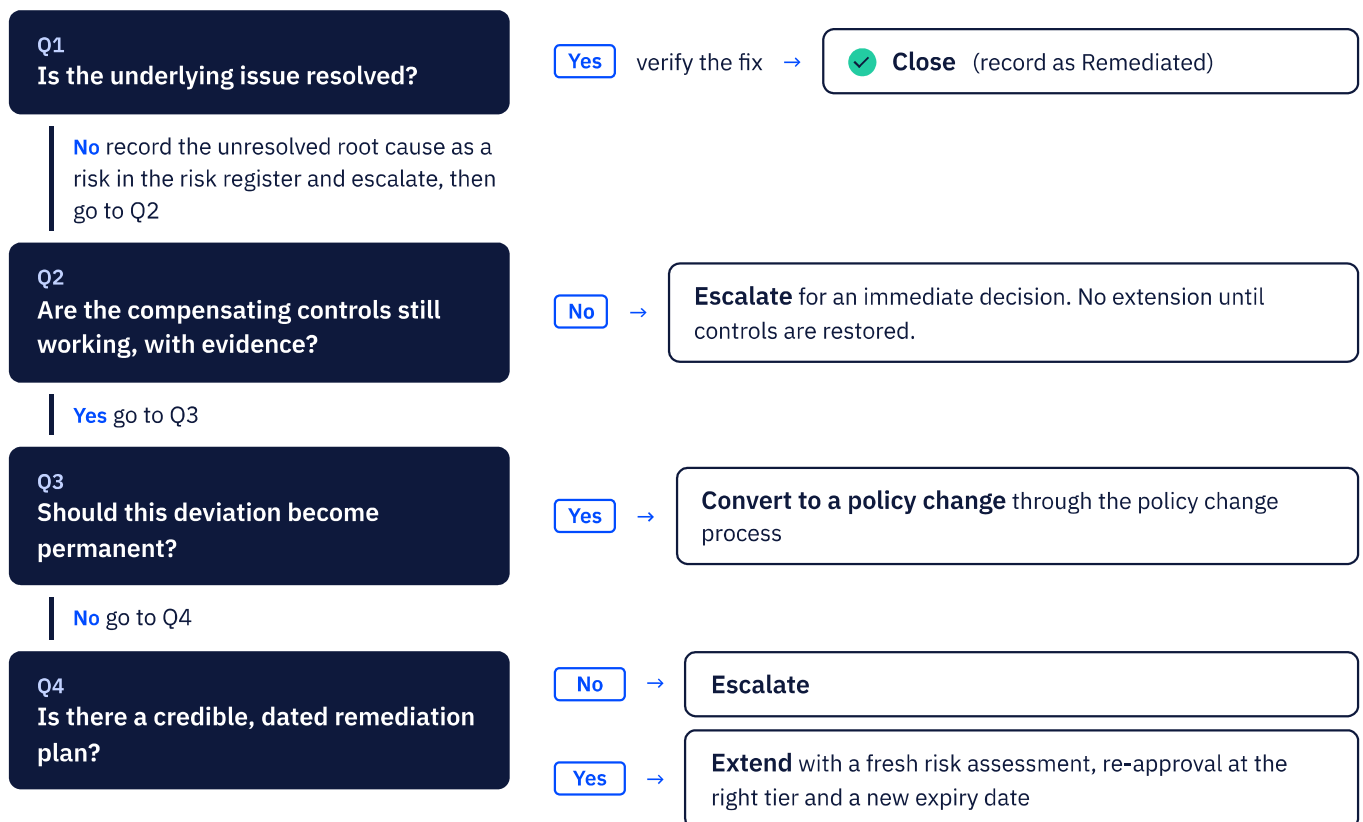
Use it when
from approval to closure

Time needed
15 minutes per review

Owner
risk owner, with risk team



Pre-expiry decision tree



An exception that reaches its expiry date without a decision is no longer an exception. It's a violation.

Audit-ready checklist

What an auditor looks for, and the evidence that answers it.

Use it when
before any internal or external audit

Time needed
1 hour

Owner
compliance lead

☐ What the auditor looks for	Evidence that answers it	Evidence we hold
☐ 1. A defined policy for requesting, assessing, approving and reviewing exceptions	Approved exception policy, with version and date	
☐ 2. Approval at the authority appropriate to the risk level	Approval records with name, role, date and tier criteria applied	
☐ 3. Compensating controls documented and implemented	Control descriptions, named owners, verification evidence dated before start	
☐ 4. Active monitoring during the exception period	Interim and pre-expiry review records, control checks	
☐ 5. Closure records showing how each exception was resolved	Resolution method, date, remediation evidence	

What auditors read as red flags

- Exceptions with no expiry date
- Extensions with no fresh risk assessment
- Compensating controls with no verification evidence
- An empty register in an organisation of any size
- Exceptions past expiry still marked Active
- Approvals made below the required tier
- Exceptions that only exist in email threads

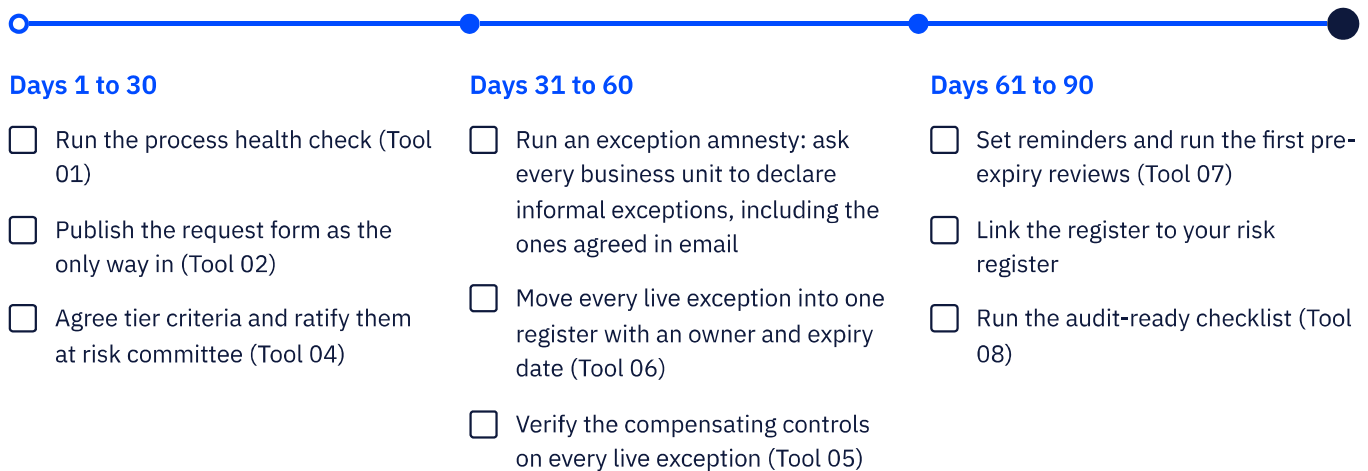
A populated register is evidence of mature governance. The absence of a process is the finding.

What frameworks expect

Regulators and auditors expect departures from policy to be governed with the same rigour as the policy itself. Some obligations can't be excepted internally at all.

Framework	What it means for exceptions
ISO/IEC 27001:2022	Clause 6.1.3 requires risk treatment decisions to be justified, including any Annex A control you exclude in your Statement of Applicability, and residual risks to be accepted by risk owners. Record exceptions as risk treatment decisions with the risk owner's acceptance.
PCI DSS	Compensating controls are permitted only for legitimate technical or documented business constraints, must meet the intent and rigour of the original requirement, and are evaluated at each annual assessment.
DORA	For in-scope EU financial entities, ICT risk management requirements apply in their own right, and the management body bears ultimate responsibility for ICT risk. An internal exception doesn't remove the obligation.
NIS2	Article 21(2) sets ten minimum risk-management measures, proportionate to size and risk but never optional. Article 20 requires management bodies to approve those measures and oversee them.

Where to start: a 90-day plan



Expiry dates only work if someone's watching them.

This kit works in a spreadsheet. At volume, reminders get missed, owners move on and compensating controls drift between reviews. That's where most exception processes fail: not in the design, in the follow-through.



One register. Every risk connected.

SureCloud Risk Management brings IT, cyber, operational and enterprise risk into one register, linking each exception to the controls and incidents it affects.



Nothing expires unnoticed.

Gracie AI Agents with Personas and Skills surface exceptions approaching expiry and compensating controls that have drifted, exactly where manual review cycles lose track.



Evidence built as you go.

Every request, assessment, approval and review is recorded in one place, so the audit trail exists before the auditor asks for it.

40%

faster decision-making with real-time, unified risk data.

[Book a demo · \[demo URL\]](#)

[QR code]

Scan to see SureCloud Risk Management

ABOUT THE AUTHORS

Nick Rafferty, CEO and Co-Founder, SureCloud

[40-word bio: background, years in GRC, why he co-founded SureCloud, areas of focus.]

Gabriel Few-Wiegratz, [job title], SureCloud

[40-word bio: GRC practice experience, frameworks worked with, relevant certifications if held.]

About SureCloud

SureCloud is the GRC platform that does more, better, with less. Founded in London in 2006, SureCloud brings risk, compliance, audit, third-party risk, business continuity and privacy into one platform.

Sources ISO/IEC 27001:2022, Clause 6.1.3 · PCI DSS, Appendix B (Compensating Controls) · Regulation (EU) 2022/2554 (DORA), Chapter II · Directive (EU) 2022/2555 (NIS2), Articles 20 and 21 · UK GDPR, Article 32

Disclaimer This kit is practical guidance, not legal advice. The risk scoring on page 6 is an example; use your organisation's own methodology and appetite statements.

Every exception owned, dated and closed.

See how SureCloud keeps your exceptions, compensating controls and review dates in one register, so nothing expires unnoticed and every decision is ready for audit.

[Book a demo · \[demo URL\]](#)

Read the full guide: How to handle an exception request
surecloud.com/blog-hub/how-to-handle-exception-request

Your Business Assured.

