

Documenting Decisions in Cybersecurity



Build a repeatable practice for capturing risk, control, and architecture decisions



Defensibility, audit readiness, and institutional memory drive the urgency



Scope: risk acceptances, exceptions, compensating controls, escalation calls, design changes



Undocumented choices cause repeated debates, inconsistent treatment, and audit findings



Outcomes: classify, write audit-grade records, assign rights, run lifecycle, launch rollout



Why Decision Records Are a Control, Not Paperwork



A decision record captures context, options, chosen path, approver, and review trigger



Records let an outside reviewer reconstruct the choice without interviewing the analyst



Undocumented verbal approvals and scattered emails drive most risk-area audit findings



Documentation as a control objective makes risk treatment reproducible, not ad hoc



Active acceptance is identified, analysed, and signed off — passive neglect is not

STRONGER CONTROLS
GREATER ASSURANCE

DECISION
RECORD



What Qualifies as a Decision Worth Recording

- 1 A decision is a choice between realistic options; tasks and updates are not
- 2 High-value types: risk acceptance, long-lived exceptions, compensating controls, design trade-offs
- 3 Departures from written policy and incident escalation calls qualify
- 4 Tier by impact and reversibility: routine, significant, strategic
- 5 Deferred patch with owner and date qualifies; a closed ticket reading "fixed" does not
- 6 Aim for a handful of well-formed records per quarter, not one per ticket



Minimum Viable Record: The One-Page Template

- Title, date, status, context, options with trade-offs, decision and reason
- Residual risk stated plainly, plus the controls and who runs them
- Named approver with role and authority basis; include the business risk owner
- Review trigger as a date or event — never "revisit periodically"
- Status values: proposed, accepted, superseded, retired

DECISION RECORD		
Title	Date	Status
Context		
Options with trade-offs		
Decision and reason		
Residual risk, controls and who runs them		
Approver (role and authority basis)		
Business risk owner		
Review trigger (date or event)		

● Title, date, status, context, options with trade-offs, decision and reason

● Residual risk stated plainly, plus the controls and who runs them

● Named approver with role and authority basis; include the business risk owner

● Review trigger as a date or event — never "revisit periodically"

● Status values: proposed, accepted, superseded, retired

Annotating the Record: A Worked Example

CLEAR RECORDS
STRONGER
DECISIONS

Risk Acceptance (Draft)

“business need”,
“server has a security issue”



Risk Acceptance (Final)

Assets: _____

Policy ID: _____

Legacy system: vendor patch unavailable:
90-day acceptance

Compensating controls: network segmentation,
enhanced monitoring

Cost: _____

Downtime: _____

Residual risk: _____

APPROVED

Date



Legacy system, vendor patch unavailable:
90-day acceptance



Compensating controls: network segmentation,
enhanced monitoring



Weak draft: “business need”, “server has a security issue”



Strong version: assets, policy ID, cost,
downtime, residual risk



Controls earn credit only when tested,
not just described



Same pattern fits a security section in an
architecture decision record

Roles, Decision Rights, and Delegation of Authority



Delegation matrix



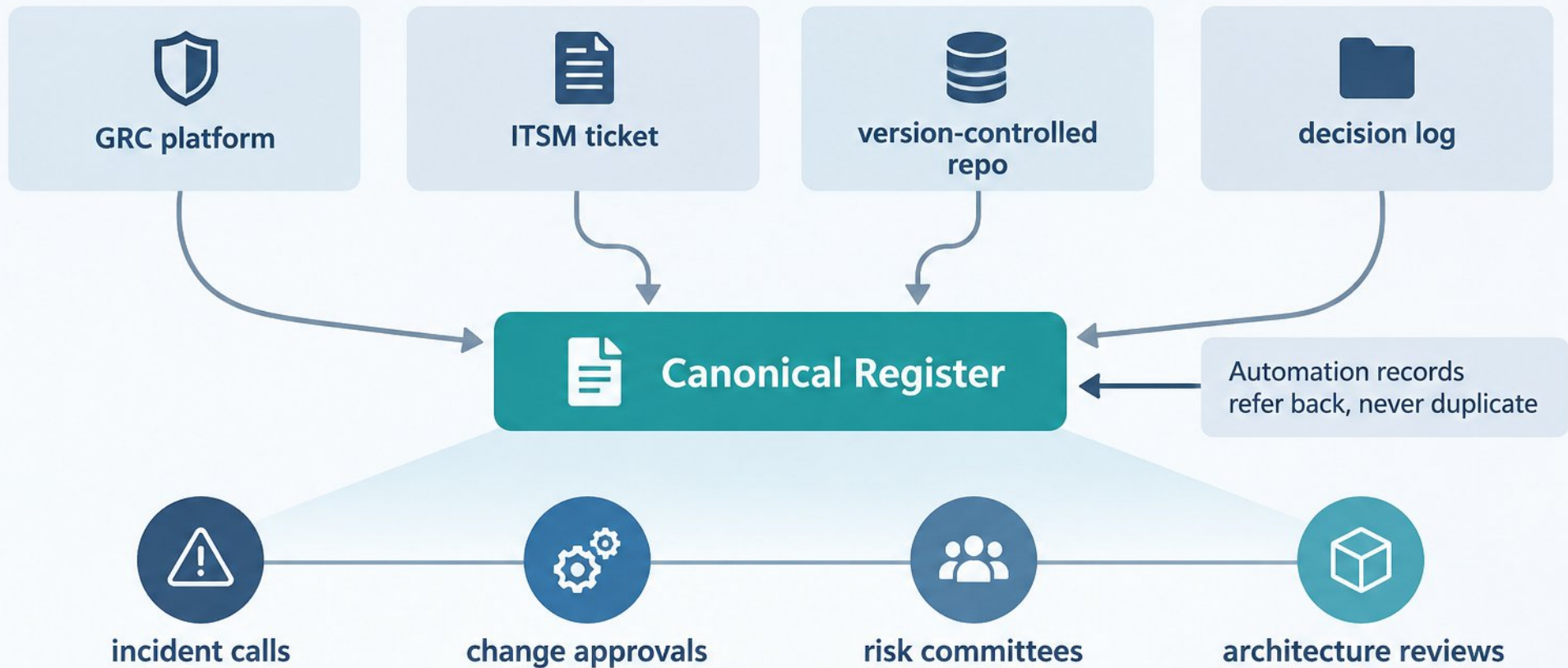
- Four roles: decision owner, recorder, approver, independent reviewer
- Requesters never approve their own exceptions
- Accountability is not delegable; authority is the missing piece
- Delegation matrix: risk band, approver role, duration, escalation path
- Break-glass paths governed, logged, and reviewed after activation
- Absent from the rights table means automatic escalation

Mapping Records to Audit and Regulatory Expectations



- ISO 27001 Clauses 6.1.3 and A.5.36: documented risk treatment and acceptance review
- SOC 2 CC3 and CC4: risk assessment and continuous monitoring evidence
- NIST CSF 2.0 GV.RR-02, GV.RM-04, GV.OV-03: decision rights and review as expected practice
- Auditors ask: who decided, when, on what evidence, within what authority, how closure verified
- One control library mapped across frameworks beats separate evidence packs

Where and How to Capture Decisions Without Friction



- Tooling options: GRC platform, ITSM ticket, version-controlled repo, decision log
- Choose one canonical register; automation records refer back, never duplicate
- Capture at incident calls, change approvals, risk committees, architecture reviews
- Lightweight forms and ticket fields beat after-the-fact reconstruction
- Records in private folders nobody visits will never be read or reviewed

Writing Rationale That Survives Challenge



- 1 Separate facts, implications, and decisions into three distinct layers
- 2 State residual risk precisely: concrete scenario or number, not vague phrases
- 3 Name options considered and why each was declined, including unchosen paths
- 4 Five-sentence summary: what, why not fixed, who's exposed, limits, end date
- 5 Record dissent and low-confidence judgements; avoid after-the-fact justification tone



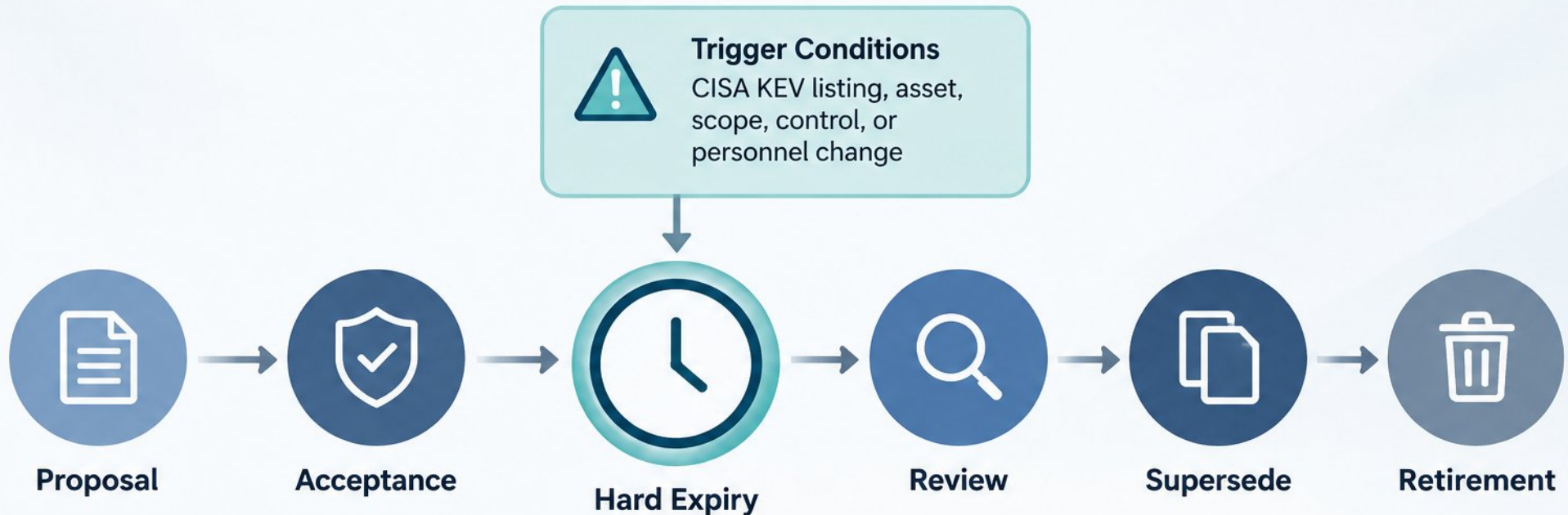
Five-Sentence Summary



Dissent

Record dissent and low-confidence judgements; avoid after-the-fact justification tone.

Lifecycle: From Recording to Review and Retirement



- Every exception and acceptance carries a hard expiry; permanent exceptions are control gaps
- Default expiry ladders by risk tier, with alerts before lapse and no silent auto-renewal
- Trigger conditions invalidate records: CISA KEV listing, asset, scope, control, or personnel change
- Link decisions to risks, controls, incidents, and changes; supersede rather than edit
- If expired and the gap remains: report non-compliance, keep controls running, then fix, renew, or escalate

Quality Checks, Metrics, and Common Pitfalls

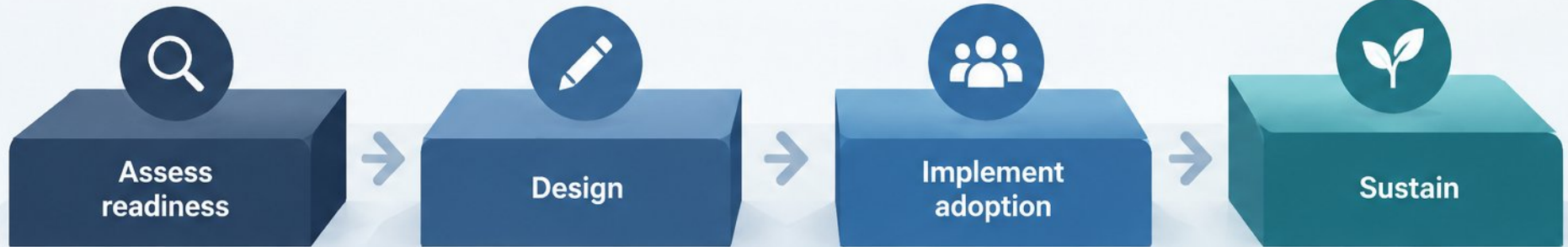
- Peer review against the one-page template before a record is final
- Common pitfalls: missing assumptions, unclear owners, verbal approvals, inconsistent terms, no expiry
- Metrics: on-time resolution against the cohort due that period, zero exceptions past review, traceability coverage, completeness
- Document sampling population, method, and rationale so reviewers can reproduce the test
- Feed post-incident and audit findings back into templates and thresholds



Building the Habit: Adoption, Culture, and Leadership Signal



A clear signal from leadership drives adoption across teams



Reduce friction:
templates and approval
routing in tools people
already use



**Train first, then
enforce;** teams that
understand the why
follow it



Four change phases:
assess readiness,
design, implement
adoption, sustain



Reinforce via
onboarding, quarterly
log reviews, and
named practice owners

Pilot Rollout: 30/60/90-Day Action Plan



-  Define exit criteria per phase so progress is evidenced, not asserted
-  Role-specific first steps: security ops, IT, risk, and compliance
-  Train first, then enforce; pilot to surface gaps before full rollout



Key Takeaways and Next Steps

CLEAR DECISIONS
STRONGER OUTCOMES

From principles to practice, with a clear path forward.



Audit-grade test:
an outsider can
defend the choice
and the closure



One system of
record; options
written fairly;
residual risk
stated plainly



Always set a hard
expiry or explicit
review trigger



Decision rights
and delegated
authority make
the practice
enforceable



Next 30 days:
adopt the template,
register open
exceptions, set one
review cadence

DOCUMENT
DECIDE
MOVE FORWARD



PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/499ab951/public