

BUILD THE WHOLE STORY



SITUATION

Describe the business need, assets, consequences, regulatory context, uncertainty and governance problem.



TASK

Explain accountability, wider stakeholders, risk owner, delegated analysis and who could accept residual risk.



ACTION

Show assessment method, limitations, appetite, tolerance, treatment choices, challenge and decision forums.



RESULT

State control implementation, risk movement, assurance, decisions, follow-up and institutional adoption.



PRACTITIONER

Apply the risk process

SHOW: how you established business need; identified assets, threats, vulnerabilities, controls and consequences; used qualitative or quantitative analysis appropriately; and explained limitations. Reference appetite and tolerance.

EXAMPLE: assessed a cloud service with supplier administration. Worked with the owner, technical lead, supplier and privacy specialist; identified persistent privilege and password-only access as outside tolerance; proposed named accounts, MFA, time-limited privilege, supplier assurance and restoration testing.

RESULT: account review verified control operation, recovery testing found and corrected a dependency, and the authorised owner accepted reduced residual risk.

PROVE IT

Control evidence and a recorded risk decision verify the outcome.

PRINCIPAL

Lead risk and governance

SHOW: framework adaptation, business-to-security traceability, competing risks, governance forums, escalation thresholds, formal acceptance, treatment ownership and stakeholder influence.

EXAMPLE: found inconsistent ratings, duplicate records and actions without owners. Delegated register analysis, created a common model linking findings to services, separated risk and action owners, retained specialist evidence and established monthly reviews plus a quarterly committee view above appetite.

RESULT: overlapping risks were consolidated, every high risk gained an owner, and the committee sponsored an organisation-wide response to shared privileged-access weakness.

FOLLOW UP

Later reviews and assurance confirm ownership, authority and treatment.

CHARTERED

Integrate enterprise decisions

SHOW: enterprise or sector leadership; board-approved appetite and tolerances; strategic control choices; independent challenge; proportionate external assurance; and sustained governance across suppliers and investment.

EXAMPLE: integrated risk with corporate decisions, delegated control mapping and supplier analysis, defined control outcomes and accountability, tiered supplier assurance, redesigned board reporting and required investments to state expected risk reduction and verification.

RESULT: risks above appetite received executive decisions, duplicated requests reduced, external testing covered evidence gaps and investment shifted to systemic identity, logging and supplier weaknesses.

SUSTAIN IT

Six-month and annual reviews demonstrate whether treatments reduced exposure.

TURN "IMPROVED" INTO VERIFIABLE EVIDENCE

WEAK

"Supplier oversight and executive reporting improved."



SUBSTANTIATED

Critical suppliers were reviewed against defined evidence and remediation requirements; overdue high-risk actions were escalated to executive owners and independent external assurance was commissioned where internal evidence was insufficient. Later reviews confirmed closure or formal re-acceptance.

THE EVIDENCE TEST

A result is strongest when the change is owned, checked and sustained.

1

WHAT CHANGED?

Control or method

2

WHO OWNED IT?

Test lead + action owner

3

HOW CHECKED?

Retest or peer review

4

WHAT RESULT?

Attack path closed

5

SUSTAINED?

Later QA sample