

Cybersecurity posture brief

Illustrative assessment / priority exposures and treatment

LENS
Business impact

METHOD
Evidence-led

DECISION
Treat or accept

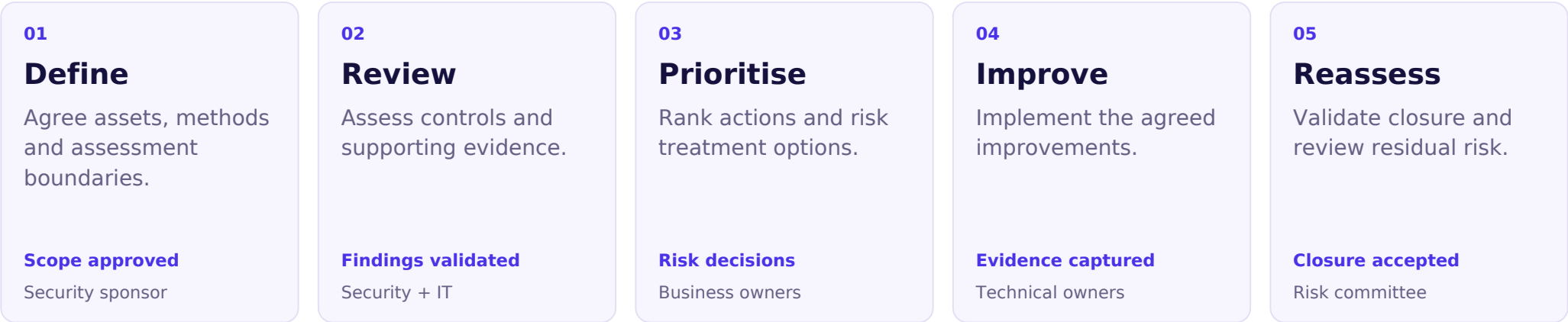
Exposure	Business consequence	Next action	Owner
Privileged access exceptions	Unauthorised change to critical services	Review + restrict access	Identity lead
Unvalidated restore process	Recovery may miss service objectives	Run scoped restore test	Infrastructure lead
Logging coverage gap	Incidents may be harder to investigate	Connect priority sources	Security operations
External access unclear	Third-party exposure is not understood	Review access + contracts	Vendor owner

An assessment is useful when the next action is owned.

Risk priorities in this sample are illustrative. Findings must be validated against the actual environment.

Implementation & governance blueprint

Cybersecurity Assessment / indicative sequence, gates and accountable roles



GOVERNANCE / DECISIONS, OWNERS AND EVIDENCE

Decision	Accountable role	Evidence
Assessment boundaries	Security sponsor	Approved systems and methods
Technical validation	System owner	Finding evidence and reproduction steps
Risk acceptance	Business risk owner	Documented rationale and expiry
Closure	Security lead	Validation results and residual risk

Timing and final roles follow the scope, dependencies and readiness. No delivery result is implied.