CYBERSECURITY & ACCESS

Cybersecurity risk & control management

Turn identified exposure into prioritised work, documented ownership and reviewable control decisions.

DOCUMENT	PREPARED	STATUS
MSP-07	1 October 2026	Draft for adoption

Scope & application

Risk assessments and security improvement plans for managed client environments. Regulatory requirements, threat context and any desired maturity target are established for the engagement.

Who does what

NovaSoft engagement lead

Scopes the work, assigns authorised personnel and maintains implementation and exception records.

Client service and risk owners

Approve access, business decisions, priorities, notices and residual risks; provide accurate scope and timely lifecycle requests.

Users and suppliers

Follow the approved arrangements, report issues and perform responsibilities assigned in the service schedule.

Draft for adoption. Confirm applicable requirements, implementation, owners and approval in the written client service schedule before operational use. Effective date is assigned on adoption.

THE POLICY IN PRACTICE

Control requirements.

01 Define the assessment

Identify important services, information, users and business consequences. Agree the assessment boundary and evidence required, including systems NovaSoft cannot inspect or change.

02 Maintain a risk register

Record each finding, affected asset, consequence, likelihood rationale, owner and next action. Distinguish observed facts from assumptions and prioritise according to the client's operation.

03 Plan a security baseline

Use the Essential Eight as one reference where suitable, alongside additional controls required by the environment. Agree a target and implementation plan; do not infer a maturity level from this document.

04 Validate controls

Inspect configuration and perform authorised tests proportionate to the risk. Record coverage, evidence date and limitations. A purchased tool or enabled feature is not sufficient proof of effectiveness.

05 Manage exceptions

Require a named client risk owner, rationale, compensating measures and a review or expiry date. Escalate unacceptable exposure through the engagement and agree a safe path for affected services.

06 Report proportionately

Provide an understandable improvement plan and progress record. Keep detailed weaknesses and exploit information restricted; public policy publication is not a security certification or an assurance report.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Agree important assets, risk criteria and assessment scope.

02 Gather evidence and prioritise the findings.

03 Approve treatment, owners, funding and exceptions.

04 Validate changes and reassess residual exposure.

Agree with the client

- Risk owner and business priorities
- Assessment scope and maturity objective
- Treatment budgets and decision dates
- Accepted exceptions and review dates

Evidence to retain

- Risk register and assessment boundary
- Control evidence and remediation plan
- Risk decisions and review outcomes

Exceptions & review

Record the requirement, reason, affected scope, risk owner, compensating measures and expiry or review date. Seek approval before deviating, or use documented emergency authority and arrange prompt review. Exceptions cannot waive applicable legal duties.

Review trigger: At the agreed risk review, after significant incidents and after material environment changes.

Proposed owner: NovaSoft engagement lead with the client service/risk owner. Review at least annually, and earlier when the trigger above applies. Version changes require an approval and client-impact record.

References & related information

ASD/ACSC - Essential Eight maturity model

ASD/ACSC - Managed service provider guidance

NovaSoft public policy library and application notes