ILLUSTRATIVE REPORT / VERSION 1.0

A security review, from findings to action.

See how we explain a finding, set priorities and define the next step. This example shows the structure of a focused security review.

An illustrative example

The organisation, observations and proposed actions in this sample are fictional. An actual report reflects the agreed review scope and the evidence available.

A clear summary for management.

A business with an external IT provider wants to understand three areas: administrator access, security log reviews and incident responsibilities. The sample identifies a gap in each area and sets out a proposed action, an owner and a way to verify the result.

The scope of this example

Account access	The authentication settings for an administrator role in a service that supports multi-factor authentication (MFA).
Log review	The documented process for reviewing security records and escalating findings.
Incident contacts	The coordinator, backup contact and communication arrangements in an incident plan.

The example is based on a review of settings and procedures. Configuration changes, penetration testing and ongoing monitoring require their own agreed scope.

Illustrative findings

SR-01 / ACCOUNT ACCESS

An administrator account without MFA

High priority	Proposed action

What was observed	The sample configuration allows an administrator to sign in with a password alone, although the service supports multi-factor authentication.
Supporting information in this sample	Sample access policy: the MFA requirement is disabled for the administrator role.
Why it matters	A stolen password could be sufficient to access administrative functions.
Recommended action	Agree the change with IT, enforce MFA for administrator accounts in the reviewed service and check account recovery arrangements before rollout.
Proposed owner	The IT provider implements the change; the business owner approves it.
How to verify the improvement	Use an authorised test account to check that MFA is required and that the agreed access recovery process works.

Related guidance

CIS Control 6: Access Control Management

Illustrative findings

SR-02 / SECURITY RECORDS

Log reviews have no assigned owner

Medium priority	Proposed action

What was observed	Security records are collected in the sample environment, but the procedure does not assign responsibility for reviewing them.
Supporting information in this sample	Sample monitoring procedure: no named reviewer, review schedule or escalation contact.
Why it matters	Relevant activity could remain unreviewed, and the team may not know who should decide what happens next.
Recommended action	Assign a reviewer, define which records and alerts are included, and agree review intervals and escalation contacts.
Proposed owner	The business owner agrees responsibilities with the IT provider and security partner.
How to verify the improvement	Generate a harmless, agreed test event and confirm that it is recorded, reviewed and escalated through the agreed process.

Related guidance

CIS Control 8: Audit Log Management

Illustrative findings

SR-03 / INCIDENT READINESS

The incident plan relies on one contact

Medium priority	Proposed action

What was observed	The sample incident plan lists the usual IT contact, but no backup contact or alternative communication route.
Supporting information in this sample	Sample contact list: one IT contact and no documented cover when that person is unavailable.
Why it matters	An unavailable contact could delay decisions and the containment of a suspected incident.
Recommended action	Appoint a coordinator and backup, agree an alternative communication channel and clarify who can approve response actions.
Proposed owner	Management and the IT provider agree the roles, contacts and decision-making authority.
How to verify the improvement	Walk through a short scenario in which the usual contact is unavailable. Record unanswered questions and assign follow-up work.

Related guidance

CIS Control 17: Incident Response Management

Next steps and references

Turn the findings into agreed work.

Confirm priorities	Review the findings with management and IT, including business impact and dependencies.
Agree the changes	Define the work, permissions, responsibilities and fees before implementation.
Verify and record	Check completed changes and record the outcome, remaining risks and follow-up work.

You can use the findings with your existing IT provider. Implementation support and ongoing monitoring are agreed separately.

Guidance behind the example

The recommendations refer to the following CIS Controls. This sample illustrates selected topics rather than a complete controls assessment.

CIS Control 6: Access Control Management
https://cas.docs.cisecurity.org/en/latest/source/Controls6/

CIS Control 8: Audit Log Management
https://cas.docs.cisecurity.org/en/latest/source/Controls8/

CIS Control 17: Incident Response Management
https://cas.docs.cisecurity.org/en/latest/source/Controls17/

Priorities here reflect the fictional scenario. Actual priorities depend on verified evidence and business impact.

Discuss your review