



01 / EXECUTIVE OVERVIEW

What a useful report can show.

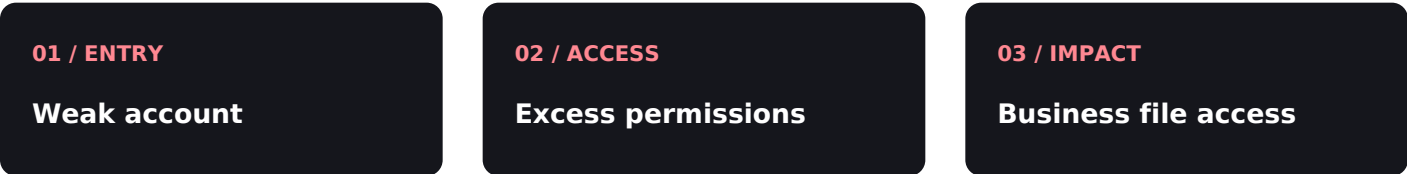
An example of how an assessment connects technical evidence to business decisions. This document contains fictional findings and proposed actions only. It is not an assessment of Summit, Veritex, or any customer.

FICTIONAL ENVIRONMENT

Example organization: A business with office devices, an identity directory, shared files, and cloud accounts. **Example scope:** Selected internal network and identity controls. Actual scope, access, timing, and deliverables are agreed before testing.

Illustrative risk story

In this scenario, a weak account credential and broad permissions combine to create a route to business files. The value of the finding is understanding that route and deciding where to break it.



Illustrative finding summary

F-01 / HIGH	Overprivileged account Credential and access review
F-02 / HIGH	Broad file-share access Restrict group permissions
F-03 / MEDIUM	Incomplete logging Confirm alert coverage

Severity and priorities above are illustrative judgments, not CVSS scores. Real ratings depend on validated access, business impact, and the agreed scope.



ILLUSTRATIVE SAMPLE

No customer data. No test performed.

02 / TECHNICAL FINDING EXAMPLE

From finding to a clear action.

F-01 / EXAMPLE HIGH PRIORITY

Overprivileged account creates a route to files

Business impact: If this fictional account were compromised, its permissions could expose shared business documents beyond the normal responsibilities of its owner.

Evidence a real report would include

The authorized asset or account reference, observed access, relevant timestamps, and a concise explanation of the validated path. Sensitive evidence would be handled through the agreed delivery process. This sample contains no real evidence.

Recommended remediation

Review the account owner and purpose; remove unnecessary group memberships; replace weak or reused credentials; check related privileged access; and confirm affected file permissions. Assign the work to an accountable owner.

Example retest criteria

After changes, repeat the agreed checks and confirm that the original access path is no longer reproducible. Record the date, tested scope, evidence, and any residual exposure.

Limits of the conclusion

A retest addresses the checks actually repeated. It is not a guarantee that all vulnerabilities have been removed or that future compromise is impossible.

Real engagement deliverables: Executive context, technical findings, prioritized remediation guidance, and retest records as agreed in the proposal.



ILLUSTRATIVE SAMPLE

No customer data. No test performed.

03 / REMEDIATION AND RETEST EXAMPLE

Make progress visible.

An example work plan that helps the business, IT team, and assessment team coordinate. These are proposed actions for a fictional scenario; none has been performed.

Proposed remediation sequence

- 1 Contain the access path**
PROPOSED OWNER: IT / IDENTITY OWNER
Review and reduce the account privileges and exposed file permissions. Prioritize based on business impact.
- 2 Strengthen related controls**
PROPOSED OWNER: IT / SECURITY OWNER
Review credential hygiene, related accounts, and logging. Document approved changes and their owners.
- 3 Verify the change**
PROPOSED OWNER: ASSESSMENT TEAM + IT
Agree on the retest scope and timing. Repeat the relevant checks and record what remains open.

Example status language

Open: Action not yet verified. **Ready for retest:** The owner reports that changes are complete.

Verified resolved: The agreed checks no longer reproduce the original path. **Residual risk:** Remaining exposure is documented for a business decision.

Want to discuss your environment? Request an assessment at summit-mi.com/penetration-testing/. Coverage and deliverables are confirmed during scoping.