

EXAMPLE DELIVERABLE / SECURITY BASELINE REVIEW

Know what needs fixing first.

Illustrative sample report

Sample only. Fictional findings. No client data or systems were assessed for this sample.

Executive summary

In this fictional scenario, the first priority is administrator access. Email authentication and recovery evidence also need attention. Each finding pairs the observation with a next action and a way to check the result.

Agreed scope comes first.

Example scope: one public website and email domain, an account-access discussion, and a review of backup records provided by the business. No exploitation, password guessing, or production changes.

Example domain: workshop.example

Prepared: October 12, 2026

Priority	Example finding	First decision
High	Administrator account lacks MFA	Protect privileged access first.
Medium	DMARC is monitoring only	Verify senders before enforcing a policy.
Medium	Restore capability is unconfirmed	Show that critical data can be recovered.

Priority reflects the example business impact and exposure. It is not a CVSS score. Actual findings and priorities depend on the agreed review and available evidence.

Your handoff: plain-language findings, a prioritized fix list, and a walkthrough.

SB-01 / HIGH PRIORITY / OPEN IN THIS SAMPLE

Administrator account lacks MFA

Example evidence. Fictional evidence: an account-settings export shows one active email administrator with MFA disabled. No sign-in was attempted.

Why it matters. A stolen password could expose email administration and account recovery controls.

Recommended action. Enroll the administrator in phishing-resistant MFA supported by the provider, such as a security key or passkey. Test recovery access before enforcing the policy. Review other privileged accounts and remove unnecessary access.

How to check the result. Confirm the policy applies to every privileged account, test a fresh sign-in and the approved recovery procedure, and retain a dated settings record.

Example owner: Email administrator

Suggested timing: First agreed change window

Guidance: Reference 1 on page 3.

SB-02 / MEDIUM PRIORITY / OPEN IN THIS SAMPLE

DMARC is monitoring only

Example evidence. Fictional evidence: `_dmarc.workshop.example` contains `p=none`. Aggregate reports are available but have no assigned reviewer.

Why it matters. The domain publishes a monitoring policy, without requesting quarantine or rejection of messages that fail DMARC.

Recommended action. Assign an owner for reports, inventory legitimate mail senders, and check SPF/DKIM alignment. Resolve delivery issues before moving to quarantine or reject using a planned rollout.

How to check the result. Recheck the DNS record, review aggregate reports, and confirm delivery from each legitimate sender after the change.

Example owner: Email administrator and business owner

Suggested timing: After sender inventory and delivery checks

Guidance: Reference 2 on page 3.

SB-03 / MEDIUM PRIORITY / OPEN IN THIS SAMPLE

Restore capability is unconfirmed

Example evidence. Fictional evidence: backup jobs report success, but the supplied records contain no recent restore test. This does not prove that backups have failed.

Why it matters. The business does not have evidence of the time or steps needed to recover critical files.

Recommended action. Choose representative critical data and arrange a controlled restore to an isolated location. Protect a backup copy from routine account compromise and document who can recover it.

How to check the result. Record the restored files, integrity checks, elapsed time, and any missing dependencies. Have the business owner compare the result with agreed recovery needs.

Example owner: IT or backup provider

Suggested timing: Next planned recovery exercise

Guidance: Reference 3 on page 3.

Turn findings into an action list.

1. Walk through the findings and confirm business impact, owners, and change windows.
2. Agree the first fixes and record any accepted risks or evidence still needed.
3. Check the changes against the evidence above and update the action list.

A real engagement includes a walkthrough so the priorities and next decisions are understood.

A scoped first pass cannot establish that every system is secure. Findings reflect the agreed scope and available evidence at the time of a review. Penetration testing, remediation work, formal certification, and a full recovery exercise require a separate scope.

Guidance and references

1. NIST SP 800-63B-4: Authentication and Authenticator Management, section 3.2.5
2. Google Workspace: Set up DMARC
3. CISA, MS-ISAC, NSA, and FBI: StopRansomware Guide, page 5

Security Baseline Reviews from \$995 | Final scope and price agreed before work starts.