



CyberSafe SW

LOCAL KNOWLEDGE. DIGITAL CONFIDENCE.

A CLEAR PICTURE. A PRACTICAL WAY FORWARD.

Cyber Security *Check-Up*

Example assessment report

A fictional small business scenario showing the clear findings, priorities and next steps a report can contain.

SAMPLE REPORT - FOR ILLUSTRATION ONLY

No real customer, account or assessment results are represented. Actual checks and reporting depend on the agreed scope and package.

BUNBURY & SOUTH WEST WA

cybersafesw.com | 0409 224 814



01 / EXECUTIVE SUMMARY

A clearer picture.

This example considers a fictional small business with one reviewed Windows computer, a primary email account, Wi-Fi and existing backup arrangements.

2

Action recommended

2

Worth reviewing

2

Looking good

What matters most

Start with sign-in protection for the primary email account and review the use of administrator access. Then verify that backups can recover files and review guest Wi-Fi arrangements.

ACTION RECOMMENDED

Account access needs attention

Two-factor authentication is not enabled on the primary email account. The everyday Windows account has administrator privileges.

WORTH REVIEWING

Backups and network arrangements

Successful file recovery has not been verified. Guest devices use the same network as business devices.

LOOKING GOOD

Useful protections are already in place

Automatic operating system updates and built-in device protection are enabled in this fictional example.



02 / DEFINED SCOPE

What we checked.

The agreed example scope covers six areas. The list below describes the kind of evidence considered; it does not promise the same checks in every real assessment.

01 Email sign-in

Two-factor authentication and recovery arrangements.

02 Windows account access

Everyday account type and administrator privileges.

03 Backup & recovery

Configured backups and evidence of successful file recovery.

04 Wi-Fi arrangements

Guest access and separation from work devices.

05 Operating system updates

Automatic update setting and visible update status.

06 Device protection

Enabled protection and reported definition status.

Not included in this example

Penetration testing, every device or cloud setting, historical incident analysis, ongoing monitoring and formal compliance certification are outside this example scope.



03 / FINDINGS & PRIORITIES

Where to focus first.

F01 / ACTION RECOMMENDED

Protect the primary email account

Observed: Two-factor authentication is not enabled on the fictional primary email account.

Recommended: Enable a supported sign-in method, preferably a phishing-resistant option where available. Check recovery details and store recovery codes safely.

F02 / ACTION RECOMMENDED

Separate everyday and administrator access

Observed: The fictional everyday Windows account has administrator privileges.

Recommended: Discuss using a standard account for daily work and a separate administrator account for authorised changes. Confirm application needs before changing access.

F03 / WORTH REVIEWING

Verify that files can be recovered

Observed: Backups are configured, but successful file recovery has not been verified.

Recommended: With permission, restore a non-sensitive test file to a separate location. Check the contents, date and backup coverage. Record the result.

F04 / WORTH REVIEWING

Review guest Wi-Fi arrangements

Observed: The fictional guest Wi-Fi network uses the same network as work devices.

Recommended: Review a separate guest network where supported. Confirm business requirements and test connectivity before making changes.



04 / AN ORDER OF ACTION

Your practical next steps.

LOOKING GOOD - F05

Keep automatic updates enabled

Automatic operating system updates are enabled. Periodically review update history, restart requirements and relevant applications.

LOOKING GOOD - F06

Maintain device protection

Built-in protection is enabled and reports current definitions. Review warnings; the reported state does not prove threats are absent.

A sensible action plan

01 Start with account access.

Enable supported two-factor authentication and review administrator use with the account owner.

02 Test recovery safely.

Restore a non-sensitive test file to a separate location and confirm important files are covered.

03 Review the network.

Check guest Wi-Fi options. Agree changes before interrupting connectivity.

04 Maintain what is working.

Keep updates and protection enabled, and review their status regularly.

Agree an owner for each action and a review date that suits the environment. Implementation is separate from this example assessment unless explicitly included in the service.

**05 / SCOPE & LIMITATIONS**

Clear boundaries matter.

Entirely fictional information.

This is a marketing example, not a real assessment. No real customer, device, account, visit or finding is represented.

A point-in-time review.

A Cyber Security Check-Up reviews agreed areas using the information and access available at the time. Settings and threats can change after the review.

No guarantee of complete protection.

The assessment cannot establish that systems are completely secure, detect every threat or guarantee future outcomes. It is not a formal certified audit, penetration test, compliance certification or ongoing monitoring service.

Scope and permission come first.

Available checks depend on the environment, access permissions and agreed service. Changes, recovery tests and additional work require appropriate permission and an agreed scope. Reporting is supplied where the assessment package includes it.

Evidence and information handling.

The handling of assessment evidence and delivery of any report must be agreed before the visit. No proprietary toolkit code, confidential information or internal scoring algorithms are included here.

Not sure where your security stands?

Talk to Josh / 0409 224 814 / cybersafesw.com