
CYBER
CONFIDENCE
BUILDING STRONGER, SAFER BUSINESSES
A PROGRAMME BY
BESPOKE
IT SOLUTIONS LTD
CYBER ESSENTIALS
CERTIFIED
BESPOKE
IT SOLUTIONS LTD
QUALITY GUARANTEE
A plain English guide for business owners
Simple steps to protect your people, data and reputation
No scare tactics. No jargon. Just clear advice.

Start with the business, not the technology

Cyber confidence means knowing **what matters**, how it is protected, who is accountable, and what the organisation will do when something goes wrong. The aim is not “zero risk”; it is informed, proportionate and repeatable risk management.

A strong foundation

Cyber Essentials centres on five technical control themes: firewalls, secure configuration, security update management, user access control and malware protection. This guide adds identity, data, email, people, suppliers, backup and incident readiness so that the review reflects day-to-day business risk.

Six principles of cyber confidence

1 Know your estate	Maintain a current view of users, devices, software, cloud services, data and suppliers. You cannot protect what nobody owns or knows about.
2 Protect identities first	Use multi-factor authentication (MFA), least privilege and disciplined joiner-mover-leaver processes. Treat administrator accounts as high risk.
3 Keep technology supportable	Remove or isolate unsupported systems, patch promptly and use secure configuration rather than vendor defaults.
4 Make recovery real	Back up critical information, protect backups from the same compromise, and prove restoration through testing.
5 Prepare people to act	Give staff simple rules for suspicious messages, payments, data sharing and reporting. Make early reporting easy and blame-free.
6 Review and improve	Assign owners, retain evidence, track exceptions and revisit controls after change, incidents and at least annually.

How Bespoke IT Solutions fits

As a Microsoft-focused MSP, Bespoke IT Solutions can help translate business priorities into proportionate controls across Microsoft 365, identity, endpoints and support operations - while keeping the conversation clear, human and practical.

Cyber confidence checklist

For each statement, mark **Yes**, **Partial**, **No** or **Unknown**. Record evidence and an owner. “Unknown” is a finding, not a failure.

Area	Review statement	Alignment	Result
Governance & scope	We have a named senior owner for cyber risk and a clear route for escalating material decisions.	**Hygiene**	☐ Y ☐ P ☐ N ☐ ?
Governance & scope	We maintain inventories of business devices, software/cloud services, user accounts and key suppliers.	**CE: scope**	☐ Y ☐ P ☐ N ☐ ?
Governance & scope	We know which systems and data are critical, where they are held and the impact if unavailable or disclosed.	**Hygiene**	☐ Y ☐ P ☐ N ☐ ?
Firewalls & internet	Internet-facing services and firewall rules are documented, justified and reviewed; unnecessary access is removed.	**CE: firewalls**	☐ Y ☐ P ☐ N ☐ ?
Firewalls & internet	Default administrator credentials have been changed and management interfaces are not unnecessarily exposed.	**CE: firewalls**	☐ Y ☐ P ☐ N ☐ ?
Secure configuration	Devices and cloud services use an approved secure baseline; unused accounts, applications and features are removed or disabled.	**CE: secure config**	☐ Y ☐ P ☐ N ☐ ?
Secure configuration	Only approved software is installed, and users cannot routinely bypass security settings.	**CE: secure config**	☐ Y ☐ P ☐ N ☐ ?

Cyber confidence checklist continued

Area	Review statement	Alignment	Result
Updates & support	Operating systems, applications, browsers, firmware and network devices are supported by their suppliers.	**CE: updates**	☐ Y ☐ P ☐ N ☐ ?
Updates & support	Security updates are deployed through a managed process, with urgent vulnerabilities prioritised and exceptions recorded.	**CE: updates**	☐ Y ☐ P ☐ N ☐ ?
Identity & access	Every person has an individual account; shared accounts are avoided or tightly controlled and attributable.	**CE: access**	☐ Y ☐ P ☐ N ☐ ?
Identity & access	MFA protects cloud services, remote access and privileged accounts; stronger phishing-resistant methods are used where practical.	**CE + hygiene**	☐ Y ☐ P ☐ N ☐ ?
Identity & access	Administrator access is separate from everyday work, restricted to those who need it and reviewed regularly.	**CE: access**	☐ Y ☐ P ☐ N ☐ ?
Identity & access	Joiners, role changes and leavers trigger prompt access changes, including third-party and shared access.	**Hygiene**	☐ Y ☐ P ☐ N ☐ ?

Cyber confidence checklist continued

Area	Review statement	Alignment	Result
Malware & endpoints	Anti-malware or equivalent endpoint protection is active, centrally monitored and cannot be casually disabled.	**CE: malware**	☐ Y ☐ P ☐ N ☐ ?
Malware & endpoints	Applications are obtained from trusted sources; risky scripts, macros and untrusted code are controlled.	**CE: malware**	☐ Y ☐ P ☐ N ☐ ?
Devices & mobility	Business devices are encrypted, screen-lock automatically and can be managed or wiped if lost.	**Hygiene**	☐ Y ☐ P ☐ N ☐ ?
Email & collaboration	Anti-phishing, anti-malware and impersonation protections are configured for email and collaboration tools.	**Hygiene**	☐ Y ☐ P ☐ N ☐ ?
Email & collaboration	External sharing in SharePoint, OneDrive and Teams is governed, time-limited where appropriate and reviewed.	**Hygiene**	☐ Y ☐ P ☐ N ☐ ?
Email & collaboration	Payment or bank-detail changes require an independent verification step outside the original message.	**Hygiene**	☐ Y ☐ P ☐ N ☐ ?
Data protection	Sensitive information has an owner, classification and clear rules for access, sharing, retention and disposal.	**Hygiene**	☐ Y ☐ P ☐ N ☐ ?

Cyber confidence checklist continued

Area	Review statement	Alignment	Result
Data protection	Critical business data is stored in approved locations rather than unmanaged devices or personal services.	Hygiene	☐ Y ☐ P ☐ N ☐ ?
Backup & recovery	Critical data and configurations are backed up to meet defined recovery needs, with protected/offline or logically isolated copies.	Hygiene	☐ Y ☐ P ☐ N ☐ ?
Backup & recovery	Restore tests are performed and results show that priority services can be recovered within business expectations.	Hygiene	☐ Y ☐ P ☐ N ☐ ?
People & awareness	Staff receive role-relevant cyber awareness training and know how to report suspicious activity quickly.	Hygiene	☐ Y ☐ P ☐ N ☐ ?
Incident readiness	We have a short, accessible incident plan with contacts, decision owners, containment priorities and communication routes.	Hygiene	☐ Y ☐ P ☐ N ☐ ?
Incident readiness	We know when and how to involve our IT provider, insurer, legal advisers, the ICO, law enforcement or the NCSC.	Hygiene	☐ Y ☐ P ☐ N ☐ ?
Suppliers	Security expectations are included in supplier selection, contracts, access reviews and offboarding.	Hygiene	☐ Y ☐ P ☐ N ☐ ?

Interpret your results

CONTROLLED	EXPOSED	UNCERTAIN
Mostly Yes, with current evidence and named owners. Keep testing and improving.	Any No or Partial on identity, internet exposure, updates, backup or incident readiness. Prioritise action.	Unknown answers, missing inventories or no evidence. Establish the facts before assuming protection.

Priority rule

Do not rely only on a total score. One serious weakness - such as no MFA for administrators, unsupported internet-facing systems, or untested recovery - can outweigh many “Yes” answers.

Common weaknesses - and what to do next

MFA gaps and excessive privilege

Warning signs: MFA applies to some users but not all cloud/admin access; shared admin accounts; dormant privileged users.

Action: Close coverage gaps, separate admin and daily accounts, review roles and use Conditional Access where licensed and appropriate.

Unknown or unsupported assets

Warning signs: No reliable inventory; old operating systems, appliances or line-of-business software; unclear owners.

Action: Discover and assign assets, remove what is unnecessary, upgrade supported systems and isolate unavoidable legacy technology.

Patching without assurance

Warning signs: Updates are “automatic” but nobody checks failures; remote or rarely used devices drift; firmware is overlooked.

Action: Set update responsibility and service levels, monitor compliance, prioritise exploited/high-impact flaws and record exceptions.

Email and payment fraud exposure

Warning signs: Unexpected forwarding rules; lookalike domains; urgent payment requests; bank-detail changes accepted by email alone.

Action: Harden email protection, disable legacy authentication, train staff and independently verify sensitive financial changes.

Uncontrolled cloud sharing

Warning signs: “Anyone” links, old guest accounts, public Teams or SharePoint spaces, sensitive files without clear owners.

Action: Set sharing defaults, use named access and expiry, review guests and apply information protection where proportionate.

Backups that have never been restored

Warning signs: Backups report success but recovery is untested; credentials are shared with production; recovery objectives are undefined.

Action: Protect backup administration, retain isolated copies and test restoration of priority services and data.

No rehearsed incident plan

Warning signs: Staff do not know who to call; key contacts exist only in affected systems; no authority to contain or communicate.

Action: Create a one-page plan, retain offline contacts, define decision rights and run a short tabletop exercise.

Making Microsoft 365 work harder for security

Microsoft 365 can provide a strong control plane, but capability depends on licensing, configuration and operational ownership. The practical goal is to use the controls you have consistently, then close justified gaps.

Control goal	Microsoft capability	Practical use
Identity	**Microsoft Entra ID**	Use MFA and Conditional Access to protect sign-ins; review privileged roles, risky access and legacy authentication. Prefer stronger authentication methods for high-risk roles.
Devices	**Microsoft Intune**	Enrol business devices, set compliance and configuration baselines, control applications, enforce encryption and support remote actions for lost devices.
Endpoint protection	**Microsoft Defender**	Use centrally managed anti-malware and endpoint detection capabilities, monitor alerts and ensure incidents have an owner and response route.
Email & collaboration	**Exchange Online Protection / Defender for Office 365**	Configure anti-phishing, impersonation, malicious link and attachment protections appropriate to the licence and risk.
Information protection	**Microsoft Purview**	Use sensitivity labels, retention and data loss prevention where there is a clear data-handling need; keep the user experience simple.
Collaboration	**Teams, SharePoint and OneDrive**	Set safe sharing defaults, manage guests and site owners, and review external access rather than allowing it to accumulate.
Visibility	**Microsoft Secure Score and security portals**	Use recommendations as a prioritisation input, not as a substitute for risk assessment, testing or Cyber Essentials evidence.

Where a Microsoft-focused MSP adds value

- Baseline assessment: map business risks and Cyber Essentials controls to the tenant, devices and operating processes.
- Remediation: sequence changes, test user impact and document controlled exceptions rather than switching on features blindly.
- Ongoing assurance: monitor control health, access, endpoints and security alerts; review changes as the business evolves.
- Human support: give users a clear place to report concerns and leaders a straightforward view of priority, ownership and progress.

Bespoke by name, bespoke by nature

Bespoke IT Solutions can help you use Microsoft security capabilities in a way that fits your organisation, risk appetite and working practices - without turning the guide into a product shopping list.

A practical 30-day improvement plan

DAYS 1-5 • ESTABLISH THE FACTS	☐ Name the senior owner and the operational lead. ☐ Complete the checklist with evidence, not assumptions. ☐ Confirm critical systems, data, suppliers and business recovery priorities. ☐ Escalate any suspected active compromise immediately.
DAYS 6-15 • REDUCE IMMEDIATE EXPOSURE	☐ Close MFA gaps and review privileged access. ☐ Remove unnecessary internet exposure and default credentials. ☐ Address unsupported or critically vulnerable systems. ☐ Confirm endpoint protection is active and monitored.
DAYS 16-23 • PROTECT DATA AND RECOVERY	☐ Review external sharing, guest access and sensitive data locations. ☐ Verify backup coverage, isolation and administrative access. ☐ Run at least one meaningful restore test and record the result. ☐ Agree independent verification for payment and bank-detail changes.
DAYS 24-30 • MAKE IT REPEATABLE	☐ Publish a short incident and reporting process. ☐ Brief staff and rehearse a realistic scenario. ☐ Assign owners and dates to remaining findings. ☐ Agree a review cadence and Cyber Essentials readiness plan.

Move from uncertainty to a clear plan

If this review has surfaced gaps, that is useful progress. The next step is to validate the findings, prioritise the highest business risks and turn them into an achievable improvement plan.

A cyber confidence review with Bespoke IT Solutions can help you

- Validate your checklist and Microsoft 365 security baseline
- Identify quick wins, material risks and evidence gaps
- Build a prioritised remediation roadmap
- Prepare for Cyber Essentials without treating certification as a tick-box exercise
- Put monitoring, review, training and incident readiness on a sustainable footing

START A PRACTICAL CONVERSATION

Contact Bespoke IT Solutions for an initial cyber confidence discussion and a clearer view of your next best steps.

hello@bespokeitsolutions.com - 01252 984 430

Fleet, Hampshire | bespokeitsolutions.com