BIGBand
Digital Made Easy

Cyber Security Risk Review Checklist

2026 Edition

You do not need to be an IT expert to complete this checklist.

Every question is written in plain business language. Simply answer Yes (tick) or No (leave blank) based on what you know about your business. Each section also includes a short technical note on the shaded line below the question, so that your IT team or security provider can understand the exact standard being assessed.

One tick = 1 point. Total all sections for your final score out of 35.

Company Name:		Date Completed:	
Completed By:		Job Title:	

SECTION 01

Internet and Network Protection

Think of your network as the front door to your business. This section checks whether that door has a proper lock, who is allowed in, and whether anyone is watching who comes and goes.

- [ ] Do you have a proper business firewall protecting your internet connection?
  Technical: A dedicated hardware firewall (not a consumer router) managed by IT or a service provider, with current firmware.

- [ ] Is someone reviewing and updating your firewall settings at least every few months?
  Technical: Firewall rules and firmware are audited and patched quarterly. Outdated rules create exploitable gaps.

- [ ] Does your system control what goes out of your network, not just what comes in?
  Technical: Outbound traffic filtering is configured. This catches malware that is already inside and attempting to communicate externally.

- [ ] Are old or unused network connections switched off?
  Technical: Unused network ports and services are disabled. Open ports are open doors for attackers to exploit.

- [ ] Does anyone check your network activity logs for unusual behaviour?
  Technical: Network traffic is centrally logged and reviewed. Automated alerts are configured for anomalous patterns.

Section Score (max 5):	

SECTION 02

Staff Computers and Devices

Every laptop, desktop and work phone your staff use is a potential entry point. This section checks whether those devices are protected and kept up to date.

- [ ] Does every staff computer have security software installed and running?
  Technical: All endpoints have up-to-date EDR or next-generation antivirus software deployed and actively monitored.

- [ ] Can someone in your company see the security status of all staff devices from one place?
  Technical: Endpoint protection is centrally managed. Unmanaged devices create blind spots that attackers exploit.

- [ ] Are all computers and devices kept up to date with the latest software updates?
  Technical: Operating system and application patches are applied promptly. Most ransomware exploits known, unpatched vulnerabilities.

- [ ] Is the use of USB thumb drives and external storage devices controlled?
  Technical: Removable media access is restricted or monitored. Physical devices bypass network security controls entirely.

- [ ] If staff use their personal phones or laptops for work, are there rules for how they do so?
  Technical: A documented BYOD (Bring Your Own Device) policy is in place with minimum security requirements enforced.

Section Score (max 5):	

SECTION 03

Working Remotely and Accessing the Office From Outside

Many attacks happen when staff connect to company systems from home, hotels or outside the office. This section checks whether that remote access is secure.

- [ ] When staff work from home or outside the office, do they connect through a secure, encrypted channel?

  Technical: Remote access is conducted through a VPN or zero-trust network access (ZTNA) solution. Direct internet-facing access is not permitted.

- [ ] Do staff need more than just a password to log in when accessing the system remotely?

  Technical: Multi-factor authentication (MFA) is enforced for all remote access. MFA blocks credential-based attacks even when passwords are stolen.

- [ ] Is your company's remote desktop access hidden from the public internet?

  Technical: Remote Desktop Protocol (RDP) is not directly exposed to the internet. Exposed RDP is one of the top ransomware entry vectors globally.

- [ ] Do staff only have access to the systems and files they actually need for their job?

  Technical: Access is granted on a least-privilege basis. Excessive permissions allow attackers to move freely once inside.

- [ ] Do remote sessions automatically close or log out after a period of inactivity?

  Technical: Session timeout policies are enforced. Persistent open sessions provide attackers extended access windows.

Section Score (max 5):	

SECTION 04

Backup and Recovery: What Happens If You Get Attacked

If your files are encrypted by ransomware, your backup is the only thing standing between you and paying the ransom. This section checks whether your backup plan would actually work.

- [ ] Is your important business data backed up every day?
  Technical: Critical data is backed up daily at minimum. Backup frequency should match the organisation's acceptable data loss tolerance.

- [ ] Are your backups stored in more than one place, including somewhere that is not connected to your main system?
  Technical: The 3-2-1 rule is followed: 3 copies of data, on 2 different media types, with 1 stored offsite or offline.

- [ ] Has your team actually tried restoring from a backup to make sure it works?
  Technical: Backup restoration has been tested within the past 6 months. Untested backups frequently fail when most needed.

- [ ] Are your backups stored separately so that a ransomware attack cannot encrypt them too?
  Technical: Backup systems are network-isolated or air-gapped. Backups accessible from the main network can be encrypted alongside live data.

- [ ] Does your business know how long it can afford to be down, and how much data loss is acceptable?
  Technical: Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are documented and communicated to key stakeholders.

Section Score (max 5):	

SECTION 05

Email Safety and Avoiding Scam Emails

More than 9 out of 10 successful cyber attacks start with an email. This section checks whether your email system and your staff are prepared to spot and stop them.

- [ ] Does your email system automatically filter out suspicious, fake or dangerous emails before staff see them?
  Technical: Advanced email threat protection is in place, filtering phishing, malware attachments and malicious URLs before delivery.

- [ ] Is it technically difficult for someone to send an email pretending to be from your company?
  Technical: Email authentication records (SPF, DKIM, DMARC) are configured to prevent domain spoofing and impersonation attacks.

- [ ] Have your staff been trained in the past year on how to spot a fake or suspicious email?
  Technical: Security awareness training including phishing simulations has been conducted within the last 12 months.

- [ ] Is it easy and quick for a staff member to report a suspicious email to the right person?
  Technical: A one-click phishing reporting mechanism is available. Simple reporting increases early detection rates significantly.

- [ ] Are website links inside emails checked for safety before staff click on them?
  Technical: URL rewriting and real-time link scanning is active. This blocks access to malicious sites even if a link is clicked.

Section Score (max 5):	

SECTION 06

Monitoring: Do You Know What Is Happening in Your Systems?

In Malaysia, the average business takes 187 days to discover a breach. During that time, attackers are already inside. This section checks whether your business would notice something wrong before it is too late.

- [ ] Are activity records from your key business systems collected and stored in one place?
  Technical: Security event logs from endpoints, servers and network devices are centralised using a SIEM or log aggregation platform.

- [ ] Does someone actually look at those records regularly, either your own staff or an outside service?
  Technical: Logs are reviewed on a scheduled basis by qualified personnel or a managed detection service. Logs without review provide no protection.

- [ ] Will your system automatically alert someone if unusual activity occurs, such as repeated failed login attempts?
  Technical: Alert rules are configured for critical events including failed logins, privilege escalation and unusual account activity.

- [ ] Would you know if a large amount of your company data was being copied or sent outside the business?
  Technical: Data loss prevention (DLP) or network monitoring tools detect unusual outbound data transfers. Exfiltration often precedes ransomware.

- [ ] Is there a team or service that actively watches your systems for threats around the clock?
  Technical: A Security Operations Centre (SOC) or managed detection and response (MDR) service provides continuous threat monitoring.

Section Score (max 5):	

SECTION 07

What Would You Do If You Got Attacked Today?

When an attack happens, every minute matters. Businesses with a clear, tested plan recover faster and with far less damage. This section checks whether your business is ready to respond.

- [ ] Does your business have a written plan for what to do if you are hit by a cyber attack?
  Technical: A documented incident response plan (IRP) exists, is accessible to key staff and is reviewed at least annually.

- [ ] Does everyone know who to call and who makes decisions if a cyber incident happens?
  Technical: An escalation matrix identifies key contacts across IT, management, legal and communications for incident response.

- [ ] Do all staff know how to report if they think something suspicious has happened?
  Technical: An internal incident reporting process is communicated to all staff. Early reporting reduces dwell time and limits damage.

- [ ] Has your team ever practised what they would do in a cyber attack, even just as a discussion exercise?
  Technical: Tabletop exercises or incident response drills have been conducted within the past 12 months to test plan effectiveness.

- [ ] After any security incident, does your team review what happened and make improvements?
  Technical: A post-incident review process captures lessons learned and feeds back into updated controls and response procedures.

Section Score (max 5):	

BIGBand
Digital Made Easy

Total Score Summary

Section	Area Reviewed	Max	Your Score
01	Your Internet and Network Protection	5	
02	Staff Computers and Devices	5	
03	Working Remotely and Accessing the Office From Outside	5	
04	Backup and Recovery: What Happens If You Get Attacked	5	
05	Email Safety and Avoiding Scam Emails	5	
06	Monitoring: Do You Know What Is Happening in Your Systems?	5	
07	What Would You Do If You Got Attacked Today?	5	
	TOTAL SCORE	35	

What Your Score Means

Find your total score in the table below to understand your organisation's current risk level and the recommended next step.

Score	Risk Level	What This Means for Your Business
30 - 35	**Low Exposure**	Your foundation is strong. Focus on continuous improvement, stay current with new threats and review your monitoring capability.
20 - 29	**Moderate Risk**	Some controls are in place but important gaps exist. Review the areas where you scored lowest and engage a specialist for a targeted review.
10 - 19	**High Risk**	Significant vulnerabilities are present in your business. Seek a professional security assessment and begin remediation without delay.
0 - 9	**Critical Exposure**	Your business is highly exposed. Attackers could exploit these gaps today. Contact BigBand immediately for an urgent security review.

Recommended Next Steps

Score 20 or below: Contact BigBand immediately. Your business has identifiable gaps that represent active risk. A professional assessment will pinpoint the most urgent areas.

Score 21 to 29: Schedule a consultation with BigBand to review the specific sections where you could not tick all items. A focused improvement plan can significantly reduce your exposure.

Score 30 to 35: Your foundation is strong. BigBand can help you stay ahead of new threats, review your monitoring capability and ensure your protection keeps pace with the evolving landscape.

Speak with a BigBand Cyber Security Specialist

Request a free consultation to discuss your results and the protection options available for your organisation @ https://bigband.net.my/index.php/bigband-cyber-security-specialist/