ASTUTE
Business Consult
...System, Standard, Strategy

INFORMATION SECURITY READINESS CHECKLIST

A practical guide to assessing how well your business protects its information, systems, devices and digital operations.

Prepared by **Astute Business Consult**

INTRODUCTION

Every business handles information. This may include customer records, employee details, financial information, contracts, business plans, supplier records and internal communications.

Much of this information is stored or shared through computers, mobile devices, email accounts, cloud platforms and business applications. These tools make work easier, but they also introduce risks.

An employee may send confidential information to the wrong person. A weak password may expose a business account. A stolen laptop may contain sensitive customer records. A system failure or cyberattack may interrupt business operations.

These incidents can affect customer trust, business continuity, finances and the ability to meet contractual or legal obligations.

Protecting business information therefore requires more than installing antivirus software or asking employees to use strong passwords. Your business needs clear responsibilities, appropriate controls and procedures for preventing, identifying and responding to information security incidents.

This checklist will help you assess your current information security arrangements, identify weaknesses and determine where improvements are needed.

You can use it during an internal review, before adopting new technology, when preparing for a client security assessment or as part of a wider management system review.

ASTUTE Business Consult
...System, Standard, Strategy

PART ONE: UNDERSTANDING INFORMATION SECURITY

What is information security?

Information security refers to the protection of information against unauthorised access, use, disclosure, alteration, loss or destruction.

It applies to information in digital and physical formats. This includes files stored on computers, records kept in cabinets, information shared through email and data held by external service providers.

A useful way to understand information security is through three basic principles:

Confidentiality: Information should only be accessible to people who are authorised to use it.

Integrity: Information should remain accurate, complete and protected against unauthorised changes.

Availability: Information and systems should be accessible to authorised users when they need them.

For example, a business may have confidential customer records. Confidentiality prevents unauthorised people from viewing them. Integrity helps ensure that customer details are not changed without permission. Availability ensures that authorised employees can access the records when required.

These three principles are often called the CIA triad.

Key terms you should understand

Information asset: Any information or resource that has value to a business and needs protection. Examples include customer databases, financial records, laptops, software and business documents.

Cybersecurity: The protection of computers, networks, applications and digital information against cyber threats and unauthorised activity.

Threat: Anything that could cause harm to an information asset. Examples include phishing attacks, malware, malicious insiders and system failures.

Vulnerability: A weakness that a threat could exploit. Examples include outdated software, weak passwords and poorly configured systems.

Risk: The possibility that a threat will exploit a vulnerability and cause harm to the business.

Access control: Rules and processes that determine who can access information, systems and applications.

Multi-factor authentication (MFA): A security process that requires users to provide more than one form of verification before accessing an account.

Data breach: An incident involving the unauthorised access, disclosure, alteration or loss of personal or other protected information.

Incident response: The procedures a business follows to identify, manage, contain and recover from information security incidents.

Backup: A separate copy of information or systems that can be used to recover data after loss, damage or disruption.

Information Security Management System (ISMS): A structured approach to managing information security risks through policies, responsibilities, processes and controls.

Who should use this checklist?

This checklist is suitable for:

- Small and medium-sized businesses.
- Financial and professional service firms.
- Healthcare and educational organisations.
- Technology companies and digital service providers.
- Retail and e-commerce businesses.
- Organisations that store or process customer information.
- Businesses that use cloud platforms and third-party software.

- Companies preparing for an information security assessment or ISO 27001 implementation.

Business owners, IT managers, information security officers, compliance personnel and operations managers can use it.

You do not need a dedicated IT department to begin reviewing your information security arrangements. However, technical controls should be assessed by people with the necessary competence.

PART TWO: HOW TO USE THE CHECKLIST

Review each question and select the response that best describes your organisation's current arrangements.

Response	Meaning
Yes	The requirement is in place and there is evidence to support it.
Partly	Some arrangements exist, but they are incomplete or inconsistently applied.
No	The requirement is not in place.
N/A	The requirement does not apply to your organisation.

Do not select Yes simply because a policy or procedure exists. Check whether employees follow it and whether the relevant security control works.

Where possible, record the evidence you reviewed. This may include access records, policies, training records, system settings, backup reports, supplier agreements and incident logs.

Important: If you identify an active security incident, do not wait until you complete the checklist before taking action. Follow your incident response procedures and involve the appropriate technical or management personnel.

ASTUTE Business Consult
...System, Standard, Strategy

PART THREE: INFORMATION SECURITY READINESS ASSESSMENT

1. Information Security Leadership and Responsibilities

Information security requires management involvement. Someone must be responsible for setting expectations, approving controls and ensuring that security risks receive attention.

Assessment question	Yes	Partly	No	N/A
Has management recognised information security as a business responsibility?	☐	☐	☐	☐
Has a person or team been assigned responsibility for information security?	☐	☐	☐	☐
Are information security responsibilities clearly defined?	☐	☐	☐	☐
Has the organisation established an information security policy?	☐	☐	☐	☐
Has management approved and communicated the policy?	☐	☐	☐	☐
Are information security risks discussed during relevant management meetings?	☐	☐	☐	☐
Are resources provided to manage identified security risks?	☐	☐	☐	☐
Are employees aware of their responsibilities for protecting business information?	☐	☐	☐	☐

Evidence to check: Information security policy, assigned responsibilities, management meeting records, approved budgets and internal communications.

ASTUTE Business Consult
...System, Standard, Strategy

2. Information Assets and Risk Assessment

Your business cannot protect information effectively if it does not know what information it holds, where it is stored and who can access it.

Assessment question	Yes	Partly	No	N/A
Has the organisation identified its important information assets?	☐	☐	☐	☐
Is there an inventory of computers, mobile devices, servers and other relevant equipment?	☐	☐	☐	☐
Are business applications and software platforms documented?	☐	☐	☐	☐
Does the organisation know where important business information is stored?	☐	☐	☐	☐
Has information been classified according to its sensitivity or business importance?	☐	☐	☐	☐
Have information security threats and vulnerabilities been identified?	☐	☐	☐	☐
Are information security risks assessed and prioritised?	☐	☐	☐	☐
Are risk assessments reviewed when business operations or technology change?	☐	☐	☐	☐
Are identified security risks assigned to responsible persons for treatment?	☐	☐	☐	☐

Evidence to check: Asset registers, software inventories, data classification records, risk assessments and risk treatment plans.

3. Access Control and User Accounts

Employees should only have access to the information and systems required for their responsibilities. Access should be reviewed regularly and withdrawn when it is no longer needed.

Assessment question	Yes	Partly	No	N/A
Does the organisation have a process for creating and approving user accounts?	☐	☐	☐	☐
Are access rights based on employees' job responsibilities?	☐	☐	☐	☐
Are unique user accounts provided instead of shared accounts where practicable?	☐	☐	☐	☐
Are strong password requirements established?	☐	☐	☐	☐
Is multi-factor authentication enabled for important accounts and systems where supported?	☐	☐	☐	☐
Are administrator accounts restricted to authorised personnel?	☐	☐	☐	☐
Are access rights reviewed periodically?	☐	☐	☐	☐
Are accounts disabled promptly when employees or contractors leave?	☐	☐	☐	☐
Is access to sensitive information restricted to authorised users?	☐	☐	☐	☐
Are unsuccessful login attempts and unusual access activities monitored where appropriate?	☐	☐	☐	☐

Evidence to check: User access lists, account approval records, access reviews, authentication settings and employee exit procedures.

4. Data Protection and Information Handling

Information should be handled according to its sensitivity. Your business should control how information is collected, stored, shared, transferred and disposed of.

Assessment question	Yes	Partly	No	N/A
Are rules established for handling confidential and sensitive information?	☐	☐	☐	☐
Is access to customer and employee information restricted?	☐	☐	☐	☐
Are sensitive digital files protected against unauthorised access?	☐	☐	☐	☐
Are secure methods used when transferring confidential information?	☐	☐	☐	☐
Are physical records stored in secure locations?	☐	☐	☐	☐
Are information retention periods defined where required?	☐	☐	☐	☐
Are records disposed of securely when no longer needed?	☐	☐	☐	☐
Are employees instructed not to share sensitive information through unauthorised channels?	☐	☐	☐	☐
Are procedures available for correcting or updating important business information?	☐	☐	☐	☐

Evidence to check: Data handling procedures, classification guidelines, retention schedules, secure disposal records and access restrictions.

5. Devices, Software and Endpoint Security

Computers, mobile phones, servers and other connected devices can provide entry points for security threats. Your business should protect these devices and keep the software they use properly maintained.

Assessment question	Yes	Partly	No	N/A
Are business computers and mobile devices identified and documented?	☐	☐	☐	☐
Are devices protected with suitable passwords, PINs or other authentication controls?	☐	☐	☐	☐
Is reputable endpoint protection or antivirus software installed where appropriate?	☐	☐	☐	☐
Are operating systems and applications updated regularly?	☐	☐	☐	☐
Are unsupported or outdated applications identified and addressed?	☐	☐	☐	☐
Are users restricted from installing unauthorised software?	☐	☐	☐	☐
Are devices configured to lock automatically when unattended?	☐	☐	☐	☐
Is sensitive information protected on portable devices?	☐	☐	☐	☐
Are lost or stolen devices reported promptly?	☐	☐	☐	☐
Are devices securely wiped or reset before disposal or reassignment?	☐	☐	☐	☐

Evidence to check: Device inventory, software update records, endpoint protection reports, configuration settings and device disposal records.

6. Network and Internet Security

Business networks connect users, devices, applications and information. Weak network controls can expose business systems to unauthorised access and disruption.

Assessment question	Yes	Partly	No	N/A

Are business networks protected against unauthorised access?	☐	☐	☐	☐
Are firewalls or other suitable network security controls in place?	☐	☐	☐	☐
Are wireless networks protected with appropriate security settings?	☐	☐	☐	☐
Are default passwords changed on network devices?	☐	☐	☐	☐
Is access to network equipment restricted?	☐	☐	☐	☐
Are guest networks separated from internal business networks where appropriate?	☐	☐	☐	☐
Are network devices and software updated regularly?	☐	☐	☐	☐
Are unusual network activities monitored where appropriate?	☐	☐	☐	☐
Are secure remote access arrangements used when employees connect from outside the office?	☐	☐	☐	☐

Evidence to check: Network diagrams, firewall settings, wireless configuration, network access records and technical review reports.

7. Email, Internet and Digital Communication

Email and online communication are common channels for phishing, impersonation, malicious attachments and accidental disclosure of information.

Assessment question	**Yes**	**Partly**	**No**	**N/A**
Are employees trained to identify suspicious emails and messages?	☐	☐	☐	☐
Are there procedures for reporting suspicious emails?	☐	☐	☐	☐

Are employees advised not to open unexpected attachments or suspicious links?	☐	☐	☐	☐
Are business email accounts protected with appropriate authentication controls?	☐	☐	☐	☐
Are email security protections configured where supported?	☐	☐	☐	☐
Are employees trained to verify unusual payment or account-change requests?	☐	☐	☐	☐
Are approved communication platforms identified for business use?	☐	☐	☐	☐
Are employees discouraged from sending confidential information through unauthorised platforms?	☐	☐	☐	☐
Are procedures available for responding to compromised email accounts?	☐	☐	☐	☐

Evidence to check: Email security settings, awareness training records, reporting procedures and approved software lists.

8. Backup, Recovery and Business Continuity

Information may become unavailable because of hardware failure, accidental deletion, cyberattacks or other disruptions. Your business should have reliable ways to recover important information and continue essential operations.

Assessment question	**Yes**	**Partly**	**No**	**N/A**
Are important business information and systems backed up regularly?	☐	☐	☐	☐
Are backup schedules defined and followed?	☐	☐	☐	☐

Are backups protected against unauthorised access and alteration?	☐	☐	☐	☐
Are backup copies stored separately from the original systems where appropriate?	☐	☐	☐	☐
Are backups tested to confirm that information can be restored?	☐	☐	☐	☐
Are recovery responsibilities assigned to relevant personnel?	☐	☐	☐	☐
Has the organisation identified systems and information that are essential to its operations?	☐	☐	☐	☐
Are procedures available for restoring systems after a disruption?	☐	☐	☐	☐
Are business continuity arrangements documented and reviewed?	☐	☐	☐	☐

Evidence to check: Backup logs, recovery test reports, business continuity plans, recovery procedures and assigned responsibilities.

9. Incident Detection and Response

A security incident may involve a compromised account, malware infection, stolen device, data leak or unauthorised system access. Your business should know how to report and manage these events.

Assessment question	**Yes**	**Partly**	**No**	**N/A**
Is there a documented process for reporting information security incidents?	☐	☐	☐	☐
Do employees know who to contact when they suspect an incident?	☐	☐	☐	☐

Are incidents recorded and investigated?	☐	☐	☐	☐
Are procedures available for containing security incidents?	☐	☐	☐	☐
Are responsibilities for incident response clearly assigned?	☐	☐	☐	☐
Are appropriate technical personnel or external specialists available to support investigations?	☐	☐	☐	☐
Are data breaches assessed to determine whether notification obligations apply?	☐	☐	☐	☐
Are relevant customers, regulators or other parties informed when required?	☐	☐	☐	☐
Are lessons from incidents used to improve security controls?	☐	☐	☐	☐

Evidence to check: Incident response plans, incident registers, investigation reports, escalation procedures and records of corrective actions.

10. Employee Awareness and Information Security Training

Employees can help protect business information, but they can also introduce risks through mistakes, weak security practices or misuse of access privileges.

Assessment question	Yes	Partly	No	N/A
Are employees informed about the organisation's information security policies?	☐	☐	☐	☐
Do employees receive information security awareness training?	☐	☐	☐	☐
Are employees trained to recognise phishing and social engineering attempts?	☐	☐	☐	☐

Do employees understand how to handle confidential information?	☐	☐	☐	☐
Are employees informed about the risks of using unauthorised software and devices?	☐	☐	☐	☐
Are information security responsibilities included in relevant employee agreements or policies?	☐	☐	☐	☐
Are employees aware of the consequences of violating security requirements?	☐	☐	☐	☐
Is information security training repeated or updated when risks change?	☐	☐	☐	☐

Evidence to check: Training materials, attendance records, employee policies, awareness communications and training assessments.

11. Third-Party and Supplier Security

Businesses often rely on external providers for hosting, payroll, accounting, payment processing, cloud storage, software and technical support. These relationships can introduce information security risks.

Assessment question	**Yes**	**Partly**	**No**	**N/A**
Has the organisation identified third parties that access or process its information?	☐	☐	☐	☐
Are relevant suppliers assessed for information security risks?	☐	☐	☐	☐
Are security responsibilities included in relevant supplier agreements?	☐	☐	☐	☐
Are third-party access rights restricted to what is necessary?	☐	☐	☐	☐

Are supplier security arrangements reviewed periodically?	☐	☐	☐	☐
Are suppliers required to report relevant security incidents?	☐	☐	☐	☐
Are arrangements in place to withdraw supplier access when services end?	☐	☐	☐	☐
Are cloud service providers assessed before important business information is stored with them?	☐	☐	☐	☐

Evidence to check: Supplier registers, contracts, service agreements, supplier assessments and access records.

12. Physical Security and Office Access

Information security also applies to physical locations. Unauthorised people may gain access to documents, computers, network equipment and other information assets if physical security is weak.

Assessment question	Yes	Partly	No	N/A
Is access to offices and areas containing sensitive information controlled?	☐	☐	☐	☐
Are visitors identified and managed appropriately?	☐	☐	☐	☐
Are important records stored in secure cabinets or rooms?	☐	☐	☐	☐
Are server rooms and network equipment areas restricted to authorised personnel?	☐	☐	☐	☐
Are computers and devices protected against theft or unauthorised use?	☐	☐	☐	☐
Are confidential documents removed from desks when no longer needed?	☐	☐	☐	☐

Are secure disposal arrangements available for paper records and storage devices?	☐	☐	☐	☐
Are physical access arrangements reviewed when staff or office arrangements change?	☐	☐	☐	☐

Evidence to check: Visitor records, access logs, physical security procedures, office inspections and disposal records.

13. Legal, Regulatory and Contractual Requirements

Information security obligations may arise from laws, regulations, contracts and industry requirements. Your organisation should identify the requirements that apply to its activities and the information it handles.

Assessment question	Yes	Partly	No	N/A
Has the organisation identified applicable information security requirements?	☐	☐	☐	☐
Have applicable personal data protection requirements been identified?	☐	☐	☐	☐
Are responsibilities for protecting personal information defined?	☐	☐	☐	☐
Are relevant contractual security requirements documented?	☐	☐	☐	☐
Are procedures available for responding to applicable data breach notification obligations?	☐	☐	☐	☐
Are relevant licences and software usage requirements observed?	☐	☐	☐	☐
Are records maintained to demonstrate compliance with applicable requirements?	☐	☐	☐	☐

Are information security obligations reviewed when laws, contracts or business activities change?	☐	☐	☐	☐

Evidence to check: Legal and regulatory registers, privacy notices, data protection policies, contracts, compliance reviews and relevant records.

ASTUTE
Business Consult
...System, Standard, Strategy

PART FOUR: UNDERSTANDING YOUR RESULTS

After completing the assessment, review all responses marked Partly or No.

These responses indicate areas where security controls may be missing, incomplete or inconsistently applied.

However, not every gap carries the same level of risk. A missing awareness record and an administrator account exposed to unauthorised access should not receive the same priority.

Use the following categories to organise your findings.

Critical priority

A serious weakness that could expose important information or systems to immediate or severe harm.

Examples include an active compromised account, unrestricted access to sensitive records or the absence of recovery arrangements during a major system disruption.

Action: Escalate immediately. Contain active threats and involve the appropriate technical and management personnel.

High priority

A significant weakness that could lead to data loss, unauthorised access or major business disruption.

Examples include missing multi-factor authentication for important accounts, untested backups or inadequate supplier access controls.

Action: Assign responsibility and establish a short, clear deadline for corrective action.

Medium priority

A weakness that increases exposure or reduces the effectiveness of existing security arrangements.

Examples include incomplete employee training, irregular access reviews or missing supplier assessments.

Action: Plan improvements, assign responsible persons and monitor completion.

Low priority

An improvement opportunity that strengthens documentation, communication or consistency without indicating an immediate serious exposure.

Examples include outdated internal guidance or incomplete records where the relevant security controls are already operating.

Action: Include the improvement in your routine review plan.

Remember: A low-priority documentation issue should not reduce the importance of a serious technical weakness. Prioritise findings according to their potential impact and likelihood.

ASTUTE
Business Consult
...System, Standard, Strategy

PART FIVE: INFORMATION SECURITY IMPROVEMENT PLAN

Use this table to record the gaps identified during your assessment. Assign each action to a responsible person and set a target completion date.

Identified gap	Priority	Corrective action	Responsible person	Target date	Evidence of completion

After assigning actions, review progress regularly. Do not close an item simply because someone reports that it has been completed. Check the evidence and confirm that the control works as intended.

PART SIX: INFORMATION SECURITY READINESS REVIEW

Use this short review to check whether your organisation has established the basic arrangements needed to protect its information.

Confirm that:

- Important information assets have been identified.
- Information security responsibilities have been assigned.
- Access to business systems and information is controlled.
- Important accounts have appropriate authentication protection.
- Devices and software receive necessary security updates.
- Confidential information is handled and stored appropriately.
- Important information is backed up and recovery arrangements are tested.
- Employees understand common information security threats.
- Security incidents can be reported and managed.
- Third-party providers are assessed where they handle business information.
- Applicable legal, regulatory and contractual requirements have been identified.
- Information security risks are reviewed when business operations change.

If essential controls are missing, assign responsibility for addressing them. The priority should depend on the information involved, the exposure created and the possible consequences for the business.

HOW ISO 27001 SUPPORTS INFORMATION SECURITY

ISO/IEC 27001 is an international standard that specifies requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS).

It provides a structured approach to identifying information security risks and selecting controls that address the organisation's needs.

For a business, this means moving beyond isolated security measures. Instead of relying only on passwords, antivirus software or individual employee actions, the organisation establishes a management system that connects policies, responsibilities, risk assessments, operational controls and continual improvement.

ISO 27001 can help organisations manage information security across their people, processes, technology and external relationships.

This checklist can support an initial review of your current arrangements. However, completing it does not establish conformity with ISO/IEC 27001 or guarantee that your information is secure.

Certification is not compulsory simply because a business wants to establish an ISMS. The first step is to understand the risks and put appropriate controls in place.

For more information, visit the International Organization for Standardization's ISO/IEC 27001 overview.

NEED HELP IMPROVING YOUR INFORMATION SECURITY MANAGEMENT SYSTEM?

Identifying information security gaps is an important first step. The next step is deciding which controls your business needs, assigning responsibilities and monitoring their effectiveness.

Astute Business Consult helps businesses assess and improve their management systems. This includes reviewing existing processes, identifying gaps and supporting management system implementation.

If your business needs help reviewing its management systems or preparing for ISO implementation, explore our Management System Diagnostic.

Astute Business Consult

Systems first. Standards second. Certification optional. Outcomes central.

IMPORTANT NOTE

This checklist is a general assessment aid. It does not replace a technical cybersecurity assessment, penetration test, legal review, data protection assessment or formal ISO/IEC 27001 audit.

Some information security controls require specialist technical knowledge. Where necessary, involve qualified IT, cybersecurity, legal or data protection professionals.

The person completing this checklist should select N/A only where a requirement genuinely does not apply to the organisation.