SOFTTECO

Cybersecurity Audit Checklist 2025

Every year, cyber threats grow in complexity and severity, but an alarming number of businesses still follow the reactive approach to security. This checklist highlights the most common threats and provides a framework for cybersecurity strategy design that you can use to protect your business.

$4.4 million

the global average cost of a data breach

68%

the number of breaches that involved a human element

Core components of a cybersecurity checklist

- **Technical infrastructure:** assesses the existing firewalls, servers, routers, endpoints, and the architecture.
- **Data protection:** focuses on the way the sensitive data is stored, processed, and transferred within your organization and between its components.
- **Access controls:** checks identity and access management, meaning the way users and admins interact with the system.
- **Incident response:** checks the ability of your organization to react to occurring threats and the ability to recover quickly.
- **Regulatory compliance:** checks whether your organization complies with necessary regulations, both international and local
- **Employee behavior:** covers user behavior in terms of employee awareness on cybersecurity.
- **Penetration testing:** tests whether any vulnerabilities in the system can be exploited and is usually performed by an external vendor.

Cybersecurity audit checklist for businesses

Infrastructure and device security

Check the following:

- Configuration and security of your firewalls and routers
- Update the status for the OS system and third-party apps
- Performance of endpoint protection tools
- Remote access and VPN configurations
- Network security assessment

Pro tip: Use automation tools to speed up and facilitate specific processes at this stage. Use centralized tools like WSUS or Intune for automated patch management and deploy tools like Nessus or Qualys for automated vulnerability assessment.

Access control & identity management

Check the following:

- Password policies and authentication methods in use
- Role-based access controls
- The processes of account provisioning (and deprovisioning)
- Presence of inactive or dead accounts
- Audit logs and their management

Pro tip: Implement the least privilege access by default and regularly review user roles and their level of privilege. Consider using a password manager to minimize the chances of using weak passwords and to pair it with multi-factor authentication (MFA).

Data and access controls

Check the following:

- Encryption for the data at rest and in transit
- An effective backup strategy and several backup options
- Access control in cloud platforms
- Proper data retention, archival, and deletion policies
- Proper access logs and Data Loss Prevention policies

Pro tip: Follow the 3-2-1 rule, which means you need to have three copies of your data, stored on two different media types, and with one copy stored off-site.

Incident response and threat detection

Check the following:

- Real-time monitoring systems (tools like Splunk, Sumo Logic, etc.)
- Performance of intrusion detection systems
- Log monitoring and alerting configurations
- Documented IRP (incident response plan)
- Assigned roles in case of a data breach
- Reports on past incidents & disaster recovery plan

Pro tip: Make sure that everyone knows their assigned roles in case of an incident and their scope of responsibility. Use frameworks like MITRE ATT&CK to simulate possible attacks and evaluate your system's ability to detect them.

Regulatory compliance

Check the following:

- Internal security policies (especially the ones applicable to remote employees)
- Adherence to compliance frameworks (GDPR, HIPAA, NIST, CIS)
- Documentation of version control management
- Vendor and third-party security reviews

Pro tip: Use tools for automated compliance monitoring, which are especially useful during quick scaling or when processing sensitive customer data.

Employee behavior

Check the following:

- Availability of security training programs
- Phishing and social engineering susceptibility
- Measures against insider threats
- Guidelines for on-premises and remote work
- Reporting in case of suspicious activity

Pro tip: Use regular phishing simulators to display real examples of possible attacks and check how employees react to them. To check how well your organization is prepared for possible attacks and whether your existing vulnerabilities can be exploited easily, use penetration testing.

Cybersecurity audit checklist for businesses

Contact Us

softteco.com

info@softteco.com

SOFTTECO