WITH secure

The Cyber Security Checklist

A comprehensive list to help protect your organization

Are you wondering which configurations, software, and administrative cyber security projects your organization needs? Or perhaps you're unsure about the right prioritization and implementation plan?

WithSecure presents a comprehensive checklist, developed through collaboration with experts from multiple fields. This unique list provides a broad and unparalleled perspective on cyber security, organizing tasks by both priority and complexity. The checklist is specifically designed to help organizations protect their environments, with clear indicators showing where WithSecure can offer expert support.

The Cyber Security Checklist

1. Lay the Foundation →

Asset Management

- [ ] Gain a thorough understanding of IT systems like servers and computers, and their role in business processes and value chains.

Network and Endpoint Security

- [ ] Apply proper network security controls such as service, network, and endpoint firewalls, and implement endpoint protection software to safeguard devices (Workstation, Server and Mobile devices).

Identity and Access Management (IAM)

- [ ] Enable Multi-Factor Authentication (MFA) for all SaaS services, and ensure remote devices connect to the company's infrastructure only through VPN + MFA or other strong authentication and encryption methods.
- [ ] Minimize the number of admin accounts on all systems and services, including endpoints.

Patch Management

- [ ] Plan and implement an effective process for installing critical security updates to all technologies (operating systems, infrastructure devices, and software updates). Prioritize internet-facing assets.

Collaboration Protection

- [ ] Implement collaboration protection (Email, Cloud Storage, Collaboration platform) software to secure communications.

Business Continuity and Disaster Recovery (BC/DR)

- [ ] Set up regular backups to ensure data recovery.

Endpoint Management

- [ ] Apply centralized management to your servers and endpoints (workstations, mobiles) for better control.

Data Protection

- [ ] Encrypt your endpoints and sensitive data at rest to protect against unauthorized access.

Policy and Compliance

- [ ] Define acceptable use policies for how employees need to use company devices, networks, and data.
- [ ] Identify laws, standards, regulations (e.g. NIS2) and contractual agreements to which you must adhere.

Security Awareness and Training

- [ ] Train employees on cyber security hygiene and recognizing and responding to cyber threats.

2. Manage Visibility →

Logging and Monitoring

- [ ] Set up centralized logging, prioritizing critical systems.

Threat Detection, Monitoring and Response

- [ ] Implement Endpoint Detection and Response (EDR) software for computers and servers.
- [ ] Expand EDR to XDR: Implement Identity and Cloud Detection and Response capabilities.
- [ ] Get a managed detection and response service from an MDR provider or partner for continuous monitoring and response.
- [ ] Get incident response retainer service to ensure the availability of qualified incident responders.
- [ ] Implement advanced network traffic monitoring to detect anomalies.
- [ ] Establish SIEM capabilities, prioritizing critical systems for better threat detection.

Exposure and Risk Management

- [ ] Implement exposure management solution/service for comprehensive risk assessment, linking vulnerabilities and misconfigurations to identify attack paths and providing visibility into devices, identities, and cloud environments.

Software Asset Management

- [ ] Develop a comprehensive understanding of software applications and licenses, and their impact on business operations and compliance requirements.

Business Continuity and Disaster Recovery (BC/DR)

- [ ] Develop disaster recovery plans to ensure business continuity.

Threat Intelligence

- [ ] Leverage threat intelligence to stay ahead of emerging threats.

3. Harden and Monitor →

System Hardening

- [ ] Remove all unnecessary services and features from all used technologies, especially if they are remotely accessible. Restrict and harden the remaining services on a technical level to be as restrictive as possible (service hardening, attack surface minimization).

Application Portfolio Management (APM)

- [ ] Allow only approved software, software libraries, and scripts to run on your systems.

Business Continuity and Disaster Recovery (BC/DR)

- [ ] Set up immutable backups for critical systems.

Identity and Access Management (IAM)

- [ ] Implement single sign-on (SSO) to streamline access management.
- [ ] Privileged Access Management (PAM): Limit and monitor privileged accounts.
- [ ] Implement Zero Trust architecture: no user, device, or system should be trusted by default, enforcing strict identity verification and continuous monitoring for every access request, regardless of whether it originates inside or outside the network perimeter.
- [ ] Enforce remote session timeout to reduce the risk of unauthorized access and, if possible, set up a passwordless environment for enhanced security.

Network Security

- [ ] Deploy network segmentation based on asset purpose and criticality (e.g. accounting systems, sensitive data).

Threat Detection, Monitoring and Response

- [ ] Create detailed incident response plans and playbooks for various scenarios.

Data Protection

- [ ] Categorize data by sensitivity to apply appropriate protections and implement Data Loss Prevention (DLP) solutions to prevent data exfiltration.
- [ ] Implement a Data Encryption Everywhere strategy to ensure that all data is consistently encrypted, both at rest and in transit.

4. Verify and Certify

Exposure and Risk Management

- [ ] Identify key suppliers and third-party vendors in your supply chain, assess cyber security risks in the supply chain, and develop mitigation strategies for supply chain risks to ensure business continuity.

Business Continuity and Disaster Recovery (BC/DR)

- [ ] Conduct disaster recovery exercises to test and improve your plans.

Security Awareness and Training

- [ ] Implement regular phishing exercises for employees to enhance awareness.

Threat Detection, Monitoring and Response

- [ ] Conduct incident response exercises to test and improve your plans.
- [ ] Conduct a purple team exercise to test and improve your security posture.

Compliance and Governance

- [ ] Implement and maintain an Information Security Management System (ISMS) to establish a systematic approach to managing sensitive information, ensuring confidentiality, integrity, and availability, and aligning with standards like ISO 27001 for improved risk management and compliance.
- [ ] Start obtaining certifications like ISO 27001 or SOC2 to demonstrate compliance.
- [ ] Regular Audits and Assessments: Conduct independent reviews of your cybersecurity posture.

Priority/complexity traffic lights:

- — essential, critical
- — important
- — high cost, high maturity

WITH secure

Ready to strengthen your organization's cyber security?

Contact WithSecure today to get started with our comprehensive checklist and expert guidance. Book a meeting now!

URL www.withsecure.com/en/about-us/company-contacts/contact-us

WithSecure Corporation
Välimerenkatu 1
00180 Helsinki
Finland