

# 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

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

#### → 3. Harden and Monitor → 4. Verify and Certify **Asset Management** Logging and Monitoring System Hardening Set up centralized logging, prioritizing critical systems. Gain a thorough understanding of IT systems like Remove all unnecessary services and features from all servers and computers, and their role in business used technologies, especially if they are remotely processes and value chains. accessible. Restrict and harden the remaining services Threat Detection, Monitoring and Response on a technical level to be as restrictive as possible **Network and Endpoint Security** Implement Endpoint Detection and Response (EDR) (service hardening, attack surface minimization). software for computers and servers. Apply proper network security controls such as service, Application Portfolio Management (APM) network, and endpoint firewalls, and implement Expand EDR to XDR: Implement Identity and Cloud Allow only approved software, software libraries, and endpoint protection software to safeguard devices Detection and Response capabilities. (Workstation, Server and Mobile devices). scripts to run on your systems. Get a managed detection and response service from Identity and Access Management (IAM) Business Continuity and Disaster Recovery (BC/DR) an MDR provider or partner for continuous monitoring and response. Enable Multi-Factor Authentication (MFA) for all SaaS Set up immutable backups for critical systems. services, and ensure remote devices connect to the Get incident response retainer service to ensure company's infrastructure only through VPN + MFA the availability of qualified incident responders. Identity and Access Management (IAM) or other strong authentication and encryption methods. Implement single sign-on (SSO) to streamline access Implement advanced network traffic monitoring Minimize the number of admin accounts on all systems to detect anomalies. management. and services, including endpoints. Privileged Access Management (PAM): Limit and Establish SIEM capabilities, prioritizing critical systems Patch Management your security posture. monitor privileged accounts. for better threat detection. Plan and implement an effective process for installing Implement Zero Trust architecture: no user, device. **Exposure and Risk Management** critical security updates to all technologies (operating or system should be trusted by default, enforcing strict systems, infrastructure devices, and software updates). Implement exposure management solution/service for identity verification and continuous monitoring for every Prioritize internet-facing assets. comprehensive risk assessment, linking vulnerabilities access request, regardless of whether it originates and misconfigurations to identify attack paths and inside or outside the network perimeter. **Collaboration Protection** providing visibility into devices, identities, and cloud Enforce remote session timeout to reduce the risk of environments. Implement collaboration protection (Email, Cloud unauthorized access and, if possible, set up Storage, Collaboration platform) software to secure Software Asset Management a passwordless environment for enhanced security. communications. Develop a comprehensive understanding of software **Network Security** Business Continuity and Disaster Recovery (BC/DR) applications and licenses, and their impact on Deploy network segmentation based on asset purpose business operations and compliance requirements. Set up regular backups to ensure data recovery. and criticality (e.g. accounting systems, sensitive data). Business Continuity and Disaster Recovery (BC/DR) **Endpoint Management** Threat Detection, Monitoring and Response Develop disaster recovery plans to ensure business Apply centralized management to your servers and Create detailed incident response plans and playbooks continuity. endpoints (workstations, mobiles) for better control. for various scenarios. Threat Intelligence **Data Protection Data Protection** Leverage threat intelligence to stay ahead of emerging Encrypt your endpoints and sensitive data at rest Categorize data by sensitivity to apply appropriate threats. to protect against unauthorized access. protections and implement Data Loss Prevention (DLP) solutions to prevent data exfiltration. **Policy and Compliance** Implement a Data Encryption Everywhere strategy to Define acceptable use policies for how employees need ensure that all data is consistently encrypted, both at to use company devices, networks, and data. rest and in transit. Identify laws, standards, regulations (e.g. NIS2) and contractual agreements to which you must adhere. Security Awareness and Training

Exposure and Risk Mai	nagement
-----------------------	----------

П	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

#### 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:

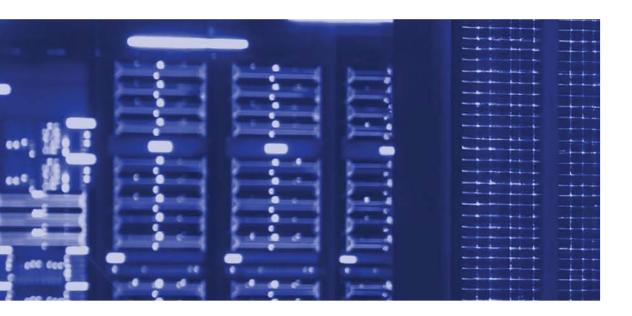
— essential, critic	;
---------------------	---

— important

- high cost, high maturity









### 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