Our Checklist for Achieving NIS2 Compliance with Microsoft Security Solutions

1. General Preparations

An estimated 30,000 companies in Germany will be affected by NIS2. Even if you don‘t fall under the category of ‘Essential‘ or ‘Important Entities‘, you could still be obliged to meet NIS2 requirements through your customers, for instance, as a supplier. Our checklist will help you optimally prepare yourself for the most crucial points.

General NIS2 Preparations and Questions

1.	Do you have at least one security officer or a dedicated security team?	○
2.	Have you thoroughly familiarized yourself with the NIS2 regulations?	○
3.	Have you checked whether you are an ‘Essential Entity‘ or an ‘Important Entity‘ under NIS2?	○
4.	If not directly affected by NIS2: Have you reviewed your customer list to see if any of your customers fall under the regulations?	○
5.	If you need to comply with NIS2 regulations as an essential or important entity: Have you analyzed your supply chain and other business partners and informed them about the upcoming changes and relevant requirements?	○
6.	Have you established a project team consisting of the executive board/management, IT, IT security officer, and data protection officer?	○
7.	Have you trained the project team in cyber security and risk management?	○
8.	Is your company registered with the BSI (Federal Office for Information Security)?	○

2. Zero-Trust-Philosophy

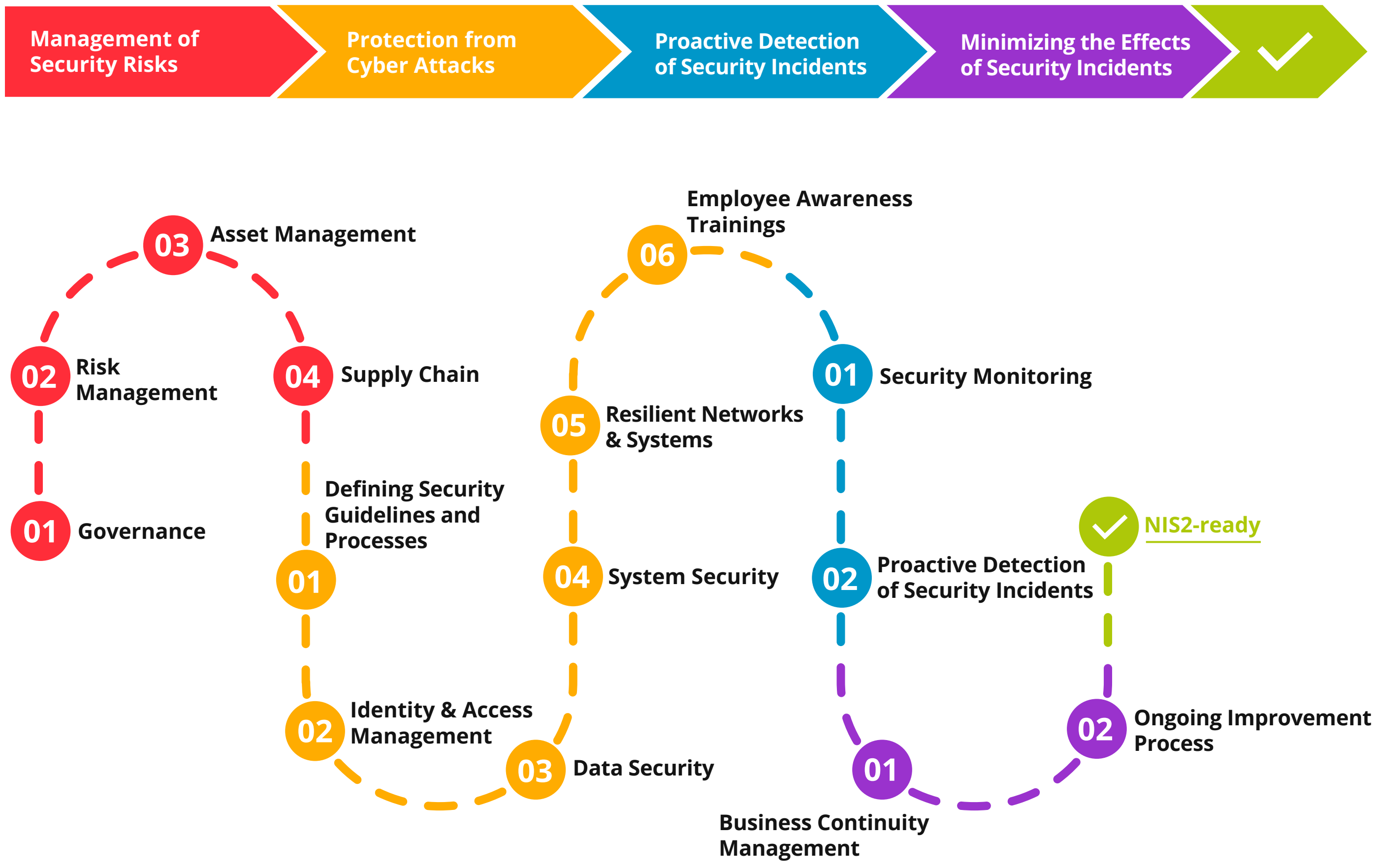
NIS2 is fully based on the Zero-Trust philosophy. Thanks to Microsoft Security Solutions, you can implement Zero-Trust principles easily to lay the foundation for NIS2-compliant protection of your company:

- **Principle of explicit control:** Who works from where with which device with which data and apps and with which services?
- **Principle of minimal necessary permissions** (Just-in-Time (JIT) / Just-enough-Access (JEA)): Provide your employees and possibly external service providers only with the permissions they need in the respective work environments.
- **Principle of monitoring, reporting and emergency planning:** Prepare for all cases because here too, preparation is the best security for as uninterrupted as possible continuation of your business activities!

3. NIS2 Objectives and Principles

The following graphic gives you an overview of the four objectives of NIS2 and its associated regulations.

Risk Management



Management of Security Risks

Protection from Cyber Attacks

Proactive Detection of Security Incidents

Minimizing the Effects of Security Incidents

✓

01 Governance

02 Risk Management

03 Asset Management

04 Supply Chain

Defining Security Guidelines and Processes

01

02 Identity & Access Management

03 Data Security

04 System Security

05 Resilient Networks & Systems

06 Employee Awareness Trainings

01 Security Monitoring

02 Proactive Detection of Security Incidents

01 Business Continuity Management

02 Ongoing Improvement Process

✓ NIS2-ready

* Note that the fulfillment of each principle does not have to follow the sequence shown.
The actual number of steps to be executed may vary depending on your systems security status.

The following checklist contains step by step how the requirements of each NIS2 principle can be met:

Management of Security Risks

Governance

1. Do you have a security policy in your company that complies with NIS2? ○
2. Do you regularly monitor compliance with regulations (e.g., GDPR)? ○

Risk Management

1. Have you established an information security management system (e.g., ISO27001)? ○
2. Do you or your external SOC team conduct regular audits on the status of your cyber defense? ○
3. Do you or your SOC team continuously improve your company's resilience against cyber attacks through action plans? ○

Asset Management

1. Are all devices (including private devices, if allowed) managed via Microsoft Intune? ○
2. Have you identified all available data storage (Cloud, local storage such as end devices or servers) in the company? ○

Supply Chain

1. Have you set up Multi-Factor-Authentication (MFA) for all employees of external service providers? ○

Protection from Cyber Attacks

Security Guidelines and Processes Definition

1. Have you documented the security strategy of your company in the form of comprehensive security policies and related processes? ○
2. Are there mechanisms in place that constantly check the deployment and effectiveness of your security strategy? ○

Identity & Access Management

1. Have you established Multi-Factor-Authentication (MFA) for all employees and possibly external service providers? ○
2. Are accesses to all applications, apps, and systems protected via Conditional Access? ○
3. Are the accesses of employees always adapted to their respective job requirements and work environments? ○
4. Are the accesses adjusted for internal job changes (e.g., trainees) to the new job roles? ○
5. Are regular authorization checks (e.g., on expiry date) conducted? ○

	Data Security	
1.	Have you encrypted company devices with Bitlocker?	○
2.	Have you classified data stored on cloud storages like OneDrive and SharePoint, especially protecting sensitive data from unauthorized access with solutions like SharePoint or Microsoft Purview?	○
3.	Is any data that’s added daily systematically classified and protected if sensitive?	○
	System Security	
1.	Are you relying on secure encryption in network communication?	○
	Resilient Networks and Systems	
1.	Do you continuously optimize your networks and systems based on analyses and results from cyber monitoring?	○
	Employee Awareness Trainings	
1.	Have you established regular trainings for employees on the awareness of cyber dangers as well as the emergency plan in the company?	○

Proactive Detection of Security Incidents

	Security Monitoring	
1.	Do you have your own or an external Security Operation Center (SOC) that can thwart threats early and take the necessary measures to contain them in the event of successful attacks?	○
	Proactive Detection of Security Incidents	
1.	Do you or your external SOC team use an early warning system or a Security Incident Event Management (SIEM) like Microsoft Sentinel?	○
2.	Have you developed reporting processes to meet your reporting obligations in terms of deadlines and scope?	○

Minimizing the Effects of Security Incidents

	Business Continuity Management	
1.	Do you have a detailed emergency plan including a process for dealing with security incidents that is continuously updated?	○
	Ongoing Improvement Process	
1.	Have you implemented a continuous improvement process that ensures findings and experiences from security incidents are used for optimization?	○

4. Strategic Positioning of NIS2 within Your Company

Use NIS2 as an opportunity to expand your resilience against cyber-attacks and define cyber security as a strategic corporate target. Furthermore, form an expert team for cyber security and invest in professional technologies for IT and cyber security.

5. Microsoft Security Solutions to Help You Meet NIS2 Requirements

Shape your company with Microsoft Security Solutions in compliance with NIS2 and build your resilience against cyber threats. In the following overview, we have compiled for you the coverage of NIS2 requirements by suitable Microsoft Security Solutions:

NIS2 Principles	Microsoft Solutions
Governance	Microsoft Defender CSPM, Entra, Microsoft Purview Compliance Manager
Risk Management	Microsoft Defender XDR, Microsoft Purview Insider Risk Management
Asset Management	Microsoft Defender XDR, Microsoft Purview Data Lifecycle Management
Supply Chain	Microsoft Defender XDR, Entra, Microsoft DevOps
Service Protection	Microsoft Defender XDR
Identity & Access	Entra
Encryption	Microsoft Purview Information Protection
System Security	Microsoft Defender XDR
Resiliente Netzwerke	Azure Network Security
Awareness Trainings	Office 365 Phishing Simulation and Learning Paths, Microsoft Purview in-app-Notifications and Policies
Security Monitoring	Microsoft Sentinel, Microsoft Purview Insider Risk Management
Proactive Security	Microsoft Defender XDR
Business Continuity	Microsoft Defender XDR, Azure Backup and Recovery, Microsoft Purview Insider Risk Management (Adaptive Scopes)
Incident Reporting	Microsoft Purview e-Discovery & Audit

6. Bottom Line

IT and cyber security are the backbone of your company. Our SITS expert teams accompany you on the path to NIS2 conformity. Just reach out to us.

Swiss IT Security Group
www.sits-group.ch
SALES@SITS.GROUP