NIS2 Supplier Checklist

A practical lead magnet for companies that are not directly subject to NIS2 but work with customers who are. Use this checklist to assess whether you are prepared for a vendor questionnaire, security review, or contractual security requirements imposed by your customers.

How to Use This Checklist

- Mark each item that your organization has implemented and formally documented.
- If something is in place but cannot be evidenced, treat it as not implemented.
- At the end, calculate your total score and compare it with the readiness assessment model.

1. Access and Identity Management

	Control	Why It Matters	Evidence / What to Prepare
	All administrative accounts are assigned to named individuals and are not shared.	Customers need visibility into privileged access and how it is controlled.	List of admin accounts and owners
	Multi-factor authentication (MFA) is used for remote access, administrative accounts, and critical services.	One of the first requirements in vendor security assessments.	Policy screenshot / solution description
	A defined process exists for provisioning, modifying, and deactivating user accounts.	Reduces the risk of outdated or orphaned access.	Internal procedure or SOP
	Users do not have local administrative privileges unless justified and approved.	Least privilege is a fundamental security principle.	Policy / exception list
	Passwords and privileged credentials are stored securely (not in Excel files or email).	Customers assess how access credentials are protected.	Vault/policy solution description

2. Protection of Endpoints, Servers, and Workstations

	Control	Why It Matters	Evidence / What to Prepare
	All devices and servers have active endpoint protection (EDR/XDR or equivalent).	A baseline technical requirement for most vendors.	Solution name and coverage
	Systems are regularly updated through patch management.	Unpatched systems are a common attack vector.	Monthly patch report
	A centralized view of security alerts and protection status exists.	Customers want assurance that protection is actively monitored.	Dashboard / monthly report
	Critical servers and VPS instances are included in monitoring and protection.	Servers often represent the highest business risk.	Asset inventory with status
	A controlled process exists for managing security exceptions and whitelisting.	Uncontrolled exceptions weaken the security posture.	Exception register

3. Monitoring, Logging, and Incident Response

	Control	Why It Matters	Evidence / What to Prepare
	Security logs are collected from key devices, servers, or services.	Without logs, it is difficult to reconstruct events.	Log source documentation
	A designated person or team reviews alerts and escalates incidents.	Customers require accountability, not just tooling.	RACI / escalation matrix
	A defined incident response procedure is in place.	RACI / escalation matrix	IR playbook ili SOP
	You can document when an incident was detected, who responded, and what actions were taken.	Traceability is critical in supply chain assessments.	Incident record template
	You know when and how to notify customers if an incident affects their systems, data, or services.	A common contractual requirement under NIS2.	Notification procedure (internal or contractual)

4. Backup, Recovery, and Business Continuity

	Control	Why It Matters	Evidence / What to Prepare
	Critical systems and data are backed up regularly.	Without backups, customers see you as an operational risk.	Backup schedule / coverage
	Backups are isolated from production and protected from unauthorized changes or deletion.	Ransomware frequently targets backups.	Backup architecture description
	Restore procedures are tested periodically.	Customers care about recoverability, not just backup existence.	Restore test report
	A basic disaster recovery plan exists for major incidents or outages.	Business continuity is increasingly required in assessments.	DR/BCP summary
	Critical systems, data, and responsible recovery personnel are clearly identified.	Lack of prioritization prolongs recovery and increases impact.	Critical asset list

5. Policies, Documentation, and Evidence

	Control	Why It Matters	Evidence / What to Prepare
	Basic security policies or internal standards are defined.	Customers typically require policies for access, passwords, backups, and incidents.	Policy set
	You can respond to a security questionnaire without improvisation.	Clear and timely responses build trust.	Response template / vendor pack
	Security incidents, exceptions, and significant changes are documented.	Evidence is critical in vendor assessments.	Register or ticketing system
	A responsible person for IT and/or cybersecurity is formally assigned.	Customers expect a clear point of contact.	Name, role, contact details
	Contracts with subcontractors and cloud providers do not introduce security gaps.	NIS2 places strong emphasis on supply chain security.	List of key partners and controls

DIGITAL SYNERGY

Readiness Assessment Model

Score	Interpretation	Recommendation
0 - 8	High risk	The organization is likely not prepared for customer security assessments
9 - 16	Partial readiness	Foundations exist, but key controls and evidence are missing
17 - 22	Good readiness	Most vendor assessments can be passed with targeted improvements
23 - 25	Very good readiness	Strong foundation for working with security-mature customers

Common Documents Requested by Customers

- Overview of security measures and tools
- Incident response procedure
- Backup and restore summary
- Evidence of patch management and endpoint protection
- Security contact details
- Completed vendor security questionnaire

Glossary of Terms and Abbreviations

NIS2	EU Directive on measures for a high common level of cybersecurity
MFA	Multi-Factor Authentication
EDR	Endpoint Detection and Response
XDR	Extended Detection and Response
VPS	Virtual Private Server
SOP	Standard Operating Procedure
RACI	Responsibility assignment matrix (Responsible, Accountable, Consulted, Informed)
IR	Incident Response
DR	Disaster Recovery
BCP	Business Continuity Plan
Patch management	Process of applying updates and security patches
Least privilege	Principle of granting minimal necessary access
Whitelist	Approved list of entities (applications, IPs, etc.)
Vendor	Supplier within a business or supply chain context
Security review	Assessment of a supplier's security posture
Supply chain	Network of suppliers and dependencies
Gap analysis	Assessment of differences between current and desired state
Traceability	Ability to track and verify actions and events