Drive NIS 2 compliance for your clients with confidence

Acronis

The NIS 2 Directive is crucial for MSPs and their clients, mandating stricter cybersecurity measures and greater accountability to safeguard essential services across the EU.

By enabling clients to achieve NIS 2 compliance, MSPs can drive growth by offering differentiated services that improve cybersecurity, enhance client trust and solidify their reputation as reliable partners.

However, understanding and implementing NIS 2 measures can be highly challenging due to the Directive's complexity, extensive requirements and often ambiguous language. This makes it difficult to break down the Directive into clear, actionable steps, leaving many MSPs and businesses uncertain about where to start or how to ensure full compliance.

This document acts as a guide for MSPs, simplifying NIS 2 by breaking down its requirements and mapping them to Acronis products. It provides MSPs with clear, actionable steps to help their clients achieve compliance and confidently align with the Directive.

Acronis can assist in achieving NIS 2 compliance across the widest range of measures

NIS 2 measures	Acronis products / features	How Acronis helps
Risk management and governance Identifying, addressing and overseeing cybersecurity risks to ensure effective protection and compliance. **Article 20** (Governance Requirements) **Article 21** (Risk Management Measures)	**Acronis Cyber Protect Cloud — Device Sense**	Passive and active network discovery and inventory.
	Advanced Management (RMM)	Vulnerability assessment for operating systems and third-party applications. Software inventory
Incident handling and reporting Detecting cybersecurity incidents effectively and reporting them promptly to relevant. **Article 10** (Computer Security Incident Response Teams) **Article 23** (Reporting Obligations)	**Security + EDR**	Next-generation anti-malware and ransomware protection. Endpoint detection and response Extended detection and response integrations with identity, email and network. Integration with threat intelligence feeds. Automated response and remediation. AI copilot, featuring AI-generated incident summary.
	Email Security and Collaboration App Security for Microsoft 365	Phishing protection Anti-spoofing Anti-malware Anti-spam Anti-evasion Post-incident analysis Incident response service
	Advanced Management (RMM)	ML-based monitoring and smart alerting.
	Advanced Management (RMM)	Automated patch management

NIS 2 measures	Acronis products / features	How Acronis helps
Business continuity Maintain essential operations and quickly recover from disruptions or cyber incidents. **Article 21** (Risk Management Measures)	**Acronis Cyber Protect Cloud — Backup and Recovery**	Data protection for physical and virtual servers, applications and databases, workstations, Microsoft 365 and Google Workspace. Immutable cloud storage
	Advanced Backup	Continuous data protection Geo-redundant storage
	Disaster Recovery	Malware-free recovery Automated DR testing, failover and failback for physical and virtual workloads.
Supply chain security Assess and manage cybersecurity risks within the supply chain to protect essential services from external threats. **Article 21** (Risk Management Measures)	**Data Loss Prevention**	Reduce data leakage risks
	Acronis Cyber Protect Cloud — Acronis MSP Protection	Security-centric development practices, comprehensive training modules and more for service providers.
Training and awareness Ensure staff are regularly trained on cybersecurity risks and best practices to maintain a strong security posture. **Article 13** (National Strategy and Risk Management) **Article 18** (Cooperation Between Member States) **Article 19** (Information Sharing and Transparency) **Article 21** (Risk Management Measures)	**Security Awareness Training**	Curated security awareness training content Gamified phishing exercises Phishing simulations
Robust data protection Implement strong measures to safeguard personal and sensitive data against breaches and unauthorized access. **Article 10** (Cooperation with CSIRTs) **Article 13** (National Strategy) **Article 16** (Supervision and Enforcement) **Article 21** (Cybersecurity Risk Management Measures) **Article 22** (Incident Handling)	**Data Loss Prevention**	Reduce data leakage risks.
MFA Multiple authentication methods to enhance security and protect access to critical systems and data. **Article 21** (Cybersecurity Risk Management Measures)	**Enabled via Acronis Cyber App** **Advanced Management (RMM)**	Automated user account provisioning and deprovisioning. MFA enforcement for Microsoft 365 accounts via Microsoft 365 Security Posture Management.

Acronis products and services are essential tools for MSPs working toward NIS 2 compliance. However, true compliance also demands robust processes, governance and proactive oversight.

Discover how the Acronis #CyberFit Partner Program can help your MSP and clients achieve compliance — Click here to get started today!

VISIT NOW

Acronis

Learn more at
www.acronis.com