kumoco

Bringing NIS Compliance Strategies to Life

Learn how Kumoco can transform NIS compliance into action with tailored implementation strategies

Turning Strategy Into Solutions

Successfully implementing NIS compliance strategies is vital for maintaining cyber-security standards.

This section focuses on the practical aspects of executing and integrating these strategies into your operations with the expertise of Kumoco and the capabilities of the ServiceNow platform.

Requirements for your NIS Strategy	Kumoco's Solution
Do you have a systematic management of network and information systems, and implementation of policies and procedures on:	-anything with a hyphen we can do in ServiceNow **anything with two asterisks we can advise/consult
- Risk analysis	- Providing risk analysis and security policy consultancy with ServiceNow's Governance Risk and Compliance (GRC) Security Operations (SecOps), business continuity planning using Business Continuity Management (BCM) solutions, supply chain risk assessment with Vendor Risk Management, cybersecurity analytics with ServiceNow, and asset management via IT Asset Management solutions. ** Providing cyber-security training, encryption advice, lifecycle management for systems, and support for authentication solutions.
- Human resources	-Human resources security & access control using ServiceNow's HR solution.
- Security of operations	- Enhance security operations with ServiceNow's SecOps for incident handling, BCM solutions, and analytics for cyber-security risk assessment. ** We offer supply chain security consultancy, secure systems development guidance, cyber-security training, and advice on cryptography policies and procedures.
- Security of architecture	- Implement ServiceNow's (IT Operations Management) ITOM for network and systems management, integrating SecOps for incident response, using Application Vulnerability Response for prioritising vulnerabilities, employing Security Incident Response (SIR) for incident lifecycle management, managing vulnerabilities. ** Offering consultancy on secure architecture design, providing vulnerability assessment and penetration testing, guiding advanced security control implementation, advising on secure coding practices, and supporting multi-factor authentication and communication system security.

Kumoco
180 Strand, London
WC2R 1EA

kumoco.com
nis@kumoco.com
+44 (20) 7594 4000

Turning Strategy Into Solutions

- Secure data	- Utilising ServiceNow's suite for incident management, vulnerability response, data integrity, operational control, compliance, threat intelligence, HR security, and asset management. ** Offering data encryption consultancy, security training leveraging ServiceNow, consultancy on authentication solutions, and backup management aligned with ServiceNow's BCM for data resilience.
- System lifecycle management	- Implementing ServiceNow's suite ensures seamless management of assets, operations, services, inventory, vulnerabilities, incidents, security, policies, and business continuity throughout the system lifecycle. ** Providing guidance on secure development practices, consultancy on DevSecOps integration, and training programs on system lifecycle management emphasising security and compliance.
Have you implemented the physical and environmental security measures to protect from:	
- Encryption	- Utilising ServiceNow's IT Asset Management for tracking and securing encrypted data physical assets, using ITSM for managing access to encrypted data systems. ** Offering consultancy on physical security measures, data center practices, disaster recovery planning, risk assessments, training on security measures, and advising on compliance with data protection standards.
- System failure	- Implementing ServiceNow's BCM for disaster recovery planning, ITOM for environmental monitoring, IT Service Management (ITSM) for incident response and Security Incident Response for rapid reaction to security incidents. ** Consulting on physical security measures, redundant systems, compliance standards, and environmental monitoring to prevent system failure and optimise IT infrastructure conditions.
- Human error	- Utilising ServiceNow's HR Service Delivery for access control and ITSM/ITOM to automate where possible. ** Providing guidance on implementing double-checking and peer review processes, offering cyber-security training programs leveraging ServiceNow, consulting on physical security measures to prevent unauthorised access, and advising on environmental controls to mitigate human error risks in IT spaces.
- Malicious action	- Utilising ServiceNow's suite for managing security incidents and vulnerabilities caused by malicious actions, gathering threat intelligence, ensuring configuration compliance, real-time monitoring and security, access control management, and securing applications against malicious exploits. ** Providing consultancy on physical security solutions to safeguard IT infrastructure, environmental security measures against tampering, security awareness training for employees, and consultancy on multi-factor and continuous authentication solutions to bolster security against malicious access attempts.

Kumoco
180 Strand, London
WC2R 1EA

kumoco.com
nis@kumoco.com
+44 (20) 7594 4000

Turning Strategy Into Solutions

- Natural phenomenon	- Implementing ServiceNow's BCM for disaster recovery planning with ITSM/ITOM monitoring and event management. ** Offering redundant systems and backup locations for service continuity during natural disasters, consulting on tailored physical and environmental security measures, integrating environmental controls for infrastructure protection, and conducting risk assessments for natural event vulnerabilities.
Are there established and maintainable policies to ensure the security of supplies, including accessibility and traceability.	- Implementing ServiceNow supply chain security automation, risk assessment, log management and asset tracking. ** Guiding end-to-end NIS compliance processes, cryptography and encryption for sensitive supply information protection, training on cyber hygiene for supply chain staff, consulting on supply chain security policies including accessibility and traceability and advising on multi-factor authentication for system access security.
Do you have incident detection processes and procedures to ensure timely and adequate awareness of events, and continued testing and maintenance.	- Implementing ServiceNow for incident detection, vulnerability management, threat intelligence, operational monitoring, incident lifecycle management, asset tracking, and application-level incident response. ** Offering guidance on integrating physical and IT security, consultancy on tailored incident detection policies, training programs for IT staff using ServiceNow, and conducting penetration testing to improve incident detection.
Have you established incident reporting processes and procedures to ensure notification to necessary organisations, and to identify any system and/or security weaknesses.	- Implementing ServiceNow workflows to manage the reporting of Cyber incidents to your relevant internal teams. ** Providing consultancy on NIS compliant incident reporting policies, guidance on European and international standards compliance, training programs for incident detection and response, and advice on communication channels and protocols for incident notification.
Are there processes and procedures in place to ensure appropriate incident response, plus testing and reporting on the response.	- Implementing ServiceNow for automated incident response, structured management, vulnerability handling, business continuity integration, accurate asset tracking, threat intelligence utilisation, application vulnerability addressing, and real-time monitoring for timely response. ** Providing penetration testing to evaluate incident response, training on best practices using ServiceNow, consulting on NIS-compliant policies, advising on communication protocols, and offering continuous testing and maintenance for effectiveness.
Do you have incident assessment processes and procedures, including:	
- Incident analysis	- Implementing ServiceNow for SecOps automated incident assessment, Route Cause Analysis, tracking outcomes, identifying vulnerabilities, and leveraging threat intelligence. ** Providing advice on communication protocols for reporting incident analysis, consultancy on developing assessment policies, training on analysis techniques using ServiceNow, and conducting penetration testing to validate analysis and identify vulnerabilities.

Kumoco
180 Strand, London
WC2R 1EA

kumoco.com
nis@kumoco.com
+44 (20) 7594 4000

Turning Strategy Into Solutions

- Collection and submission of relevant information to your regulator	- Implementing ServiceNow workflows to manage the reporting of Cyber incidents to your local GOV Computer Security Incident Response Team (CSIRT). ** Providing consultancy on NIS compliant incident reporting policies, guidance on European and international standards compliance, training programs for incident detection and response, and advice on communication channels and protocols for incident notification.
- A continuous improvement process	- Utilising ServiceNow for cyber-security performance tracking, continuous improvement, incident and vulnerability management, service process enhancement, accurate asset information, continuity planning, and application security and IT operations optimisation. ** Offering consultancy for tailored continuous improvement in cyber-security and compliance, providing training on best practices and methodologies, guiding feedback loop implementation, and conducting workshops on cyber-security trends for ongoing learning.
Do you have the ability to maintain/restore services to acceptable pre-defined levels by means of contingency planning and disaster recovery.	Implementing ServiceNow's BCM, ITSM, ITOM, Configuration Management Database (CMDB), Application Vulnerability Response, SIR, Vulnerability Response, and IT Asset Management for comprehensive service restoration and security incident management. ** Offering training on disaster recovery and business continuity, advising on backup management, providing consultancy on crisis management, developing aligned plans with NIS requirements, and guiding authentication integration in contingency planning.
Are there policies concerning systems assessment, inspection and verification, including:	
- Observations to assess systems are operating as intended	- Utilising ServiceNow's ITOM for continuous monitoring, Performance Analytics for assessment, CMDB for accurate configurations, ITSM for management, Vulnerability Response for identification, SIR for analysis, Application Vulnerability Response for security, Threat Intelligence for informing, and BCM for testing disaster recovery plans. ** Consultancy for policy development ensuring system integrity, guidance for continuous improvement, staff training on assessment techniques, and external testing services for security validation.
- Verification that guidelines are being followed	- Utilising ServiceNow tools snd reporting for monitoring compliance with guidelines. ** Training emphasises policy adherence via ServiceNow tools, with guidance on continuous improvement and verification processes. Workshops educate staff on guideline importance and ServiceNow usage for compliance.
- Ensuring records are accurate	- ServiceNow's automation and discovery, CMDB for IT asset records. ** Training on data integrity using ServiceNow, automation guidance to reduce errors, security testing to validate records, consultancy on record-keeping policies, and integration of third-party systems for comprehensive record maintenance.

Kumoco
180 Strand, London
WC2R 1EA

kumoco.com
nis@kumoco.com
+44 (20) 7594 4000

Turning Strategies Into Solutions

- Ensuring that efficiency and effectiveness targets are met	- Utilising ServiceNow's reporting tools, KPI dashboards are available to monitor all aspects of NIS2 requirements. ** Consultancy to define the relevant KPIs needed to ensure that your organisation is NIS complaint.
Where appropriate, do you follow accepted international standards such as ISO 27001 and/or ISO 22301.	- We implement ServiceNow modules for ISO compliance, covering ITSM, BCM, SIR, CMDB, Vulnerability Response, Performance Analytics, Threat Intelligence, and ITOM, ensuring adherence to standards like ISO 22301 and 27001. ** We create ISO-compliant security and continuity guidance, documenting ISO 27001 and 22301 testing, advising on authentication and encryption, providing ISO certification consultancy, and delivering ISO standards training with ServiceNow.

Talk to Kumoco now and we can empower your NIS strategy, and drive NIS compliance.

In order to do this, Kumoco can leverage several specific ServiceNow modules within its platform, each designed to address different aspects of the regulatory requirements:

- **Security Incident Response (SIR):** Quickly manage and resolve security incidents, aligning with NIS 2018's emphasis on effective incident handling.
- **Governance, Risk, and Compliance (GRC):** Streamline compliance with NIS 2018 through risk management, policy enforcement, and compliance tracking.
- **IT Operations Management (ITOM):** Improve IT infrastructure visibility and resilience, supporting NIS 2018's security and availability requirements.
- **Business Continuity Management (BCM):** Enhance organisational resilience with continuity planning and response strategies, key to NIS 2018 compliance.
- **Performance Analytics:** Utilise real-time analytics for monitoring compliance and security performance, aiding continuous improvement under NIS 2018.

Kumoco
180 Strand, London
WC2R 1EA

kumoco.com
nis@kumoco.com
+44 (20) 7594 4000

kumoco

Take the Next Step with Kumoco

Ready to elevate your cybersecurity compliance and navigate the new NIS Directive with confidence?

Contact us today to learn how Kumoco can empower your telecommunications company for a secure and compliant digital future.

nis@kumoco.com

kumoco.com

References:

UK Gov	https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
Ofcom	https://www.ofcom.org.uk/consultations-and-statements/
EU	https://digital-strategy.ec.europa.eu/en/policies/nis2-directive