NIS2 Compliance Evidence Pack

Clarivate Information Security & GRC

Confidential

June, 2026

Executive Summary

- NIS2 is regulatory - We are compliant, but certification doesn't exist
- NIS2 Compliance demonstrated via evidence and controls
  - Most NIS2 controls are addressed through ISO 27001
  - Gaps are covered through our SOC 2 and ISO 27017, 27018, 27701, 27032 and 22301 certifications
- Structured NIS2 readiness self-assessment completed with mapping of controls
- Controls implemented across governance, risk, and security

Clarivate™

Scope and Applicability

- EU-relevant entities and services
- Assessment covers risk, controls, incident response
- Includes supply chain and governance
- Entity classification – Clarivate is classified as an “Important Entity”

Clarivate™

Governance and Accountability

- Security governance framework
- Board-level oversight
- Information Security Policy
- Defined roles and responsibilities

A Structured CISO team covering SOC, Security Architecture, Product Security, Governance, Risk, Certification, Security Compile, and Security Engineering teams to deliver end-to-end enterprise security.

- SOC Team
- Security Architect Team
- Product Security
- Governance Team
- Risk Team
- Certification Team
- Security Compile Team
- Security Engineering Team

Clarivate™

Clarivate security framework and certification

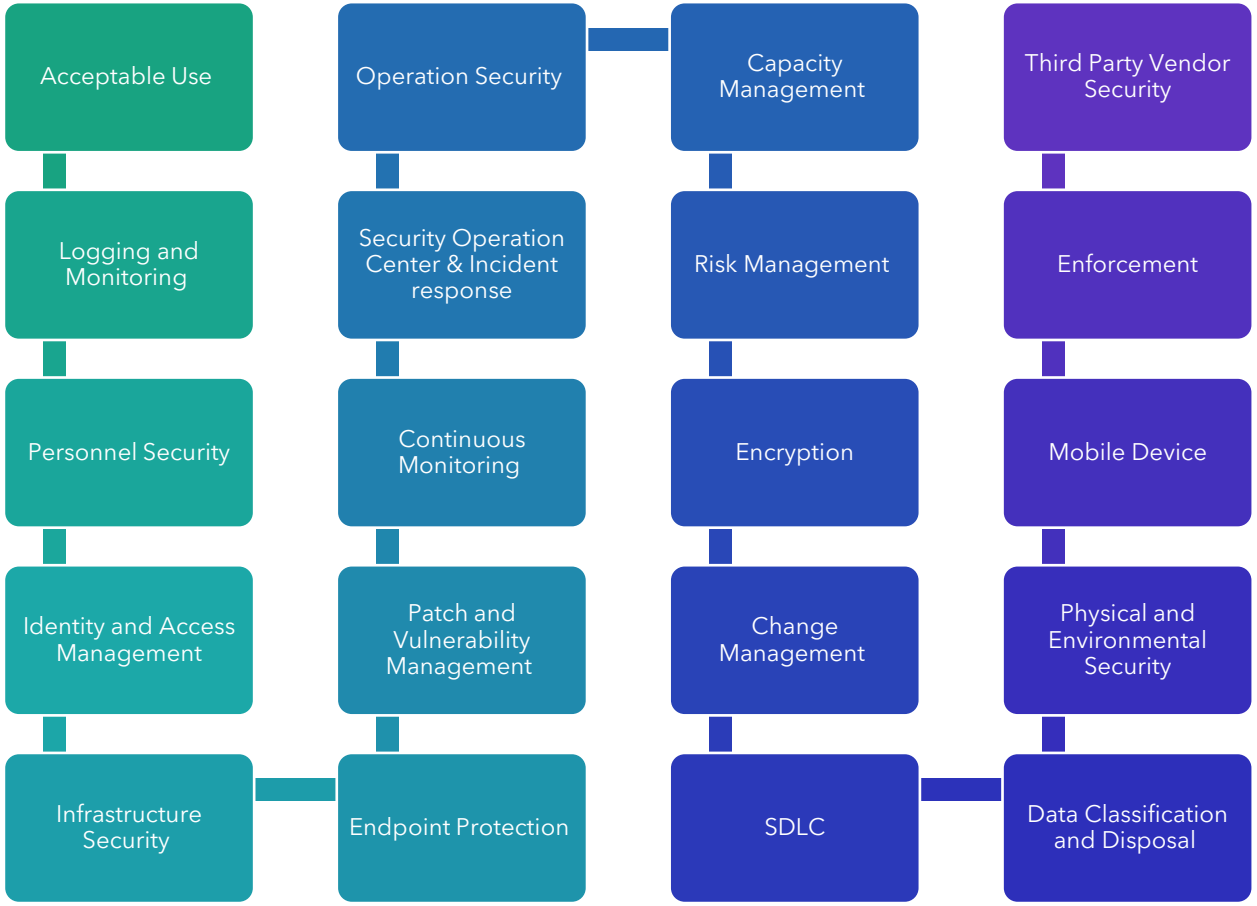
Standards used and followed across Clarivate

Our Information Security Management System (ISMS) design and practices are based on these standards, which have a defined scope.

References:

- Trust Center
- Information Security Program
- Responsible Disclosure Program
- Security Compliance

Clarivate security policies and standards



Clarivate™

*For more information see our Summary of Standards

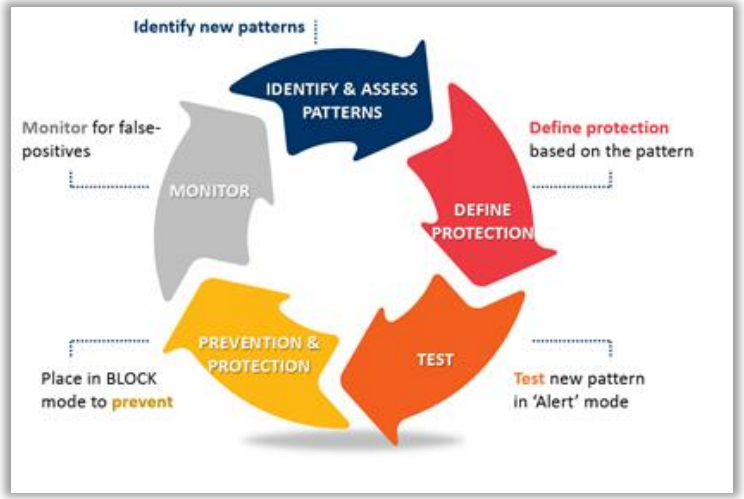
Risk Management

- Risk management policy
- Risk assessment methodology
- Enterprise risk register
- Risk treatment plans

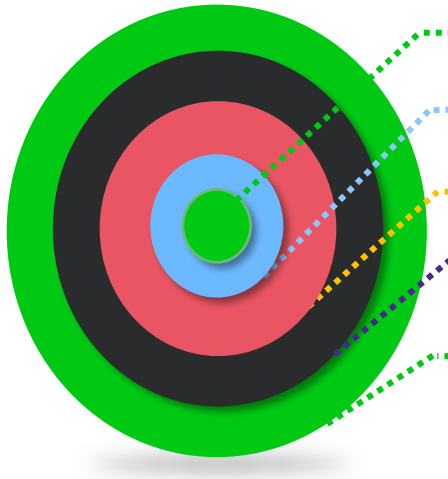
Clarivate™

Security Controls

- IAM and MFA
- Encryption standards
- Patch management
- Control monitoring



- Automatically block suspicious activity and continuously protect against new patterns



- Application protection
- Endpoint protection; disk encryption
- Vulnerability protection
- Firewall protection and network Segmentation
- Block malicious hosts

Clarivate™

Incident Management

- Incident Response Plan
- Classification and escalation
- Incident logs
- Monitoring capability

The Security Operations Center (SOC) monitors, detects and responds to security threats in real-time to protect assets and data.

The SOC Center consists of:

- 24x7 System monitoring
- Security event log analysts
- Security and data protection incident response
- Incident management process
- Escalation process
- Ongoing status update
- Root cause analysis

Business Continuity

- BCP and DRP
- Backup processes
- Recovery testing
- Defined RTO/RPO

Clarivate™

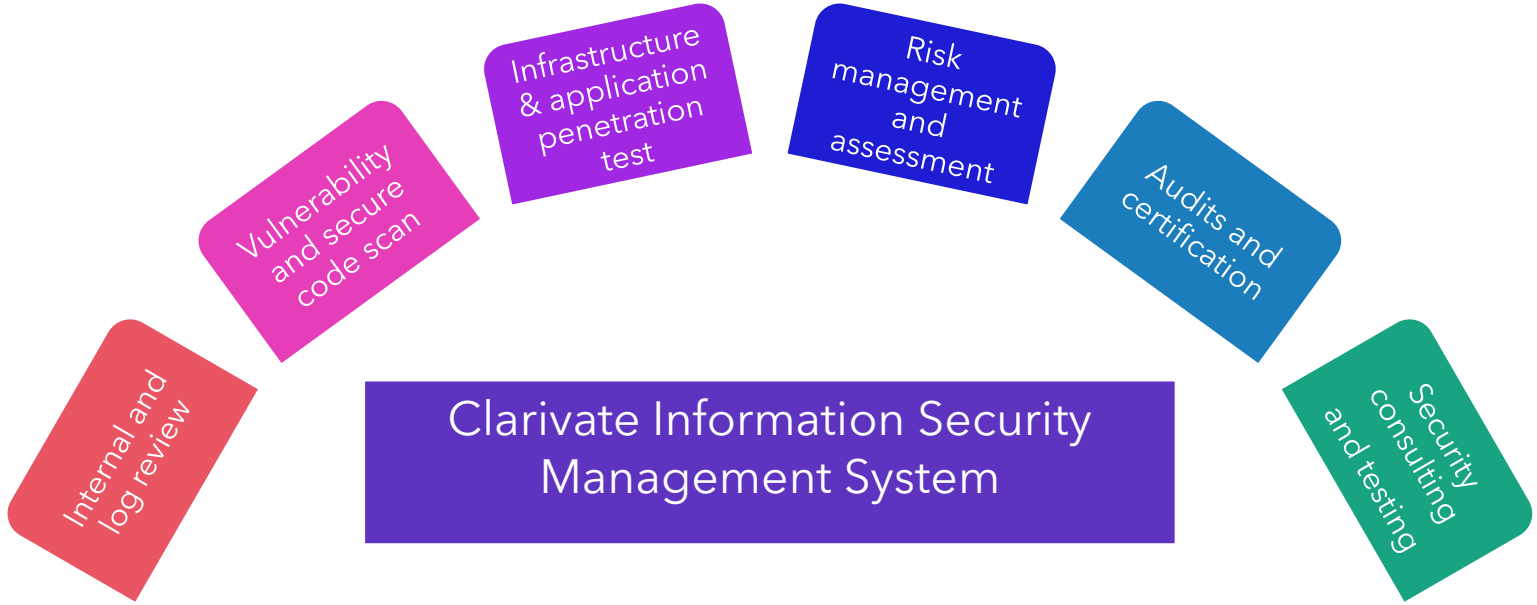
Third-Party Risk

- Vendor risk framework
- Due diligence
- Security assessments
- Contractual requirements

Clarivate™

Compliance & Audit

- NIS2 self-assessment
- Gap registration and remediation
- Internal and external audits
- Readiness assessment

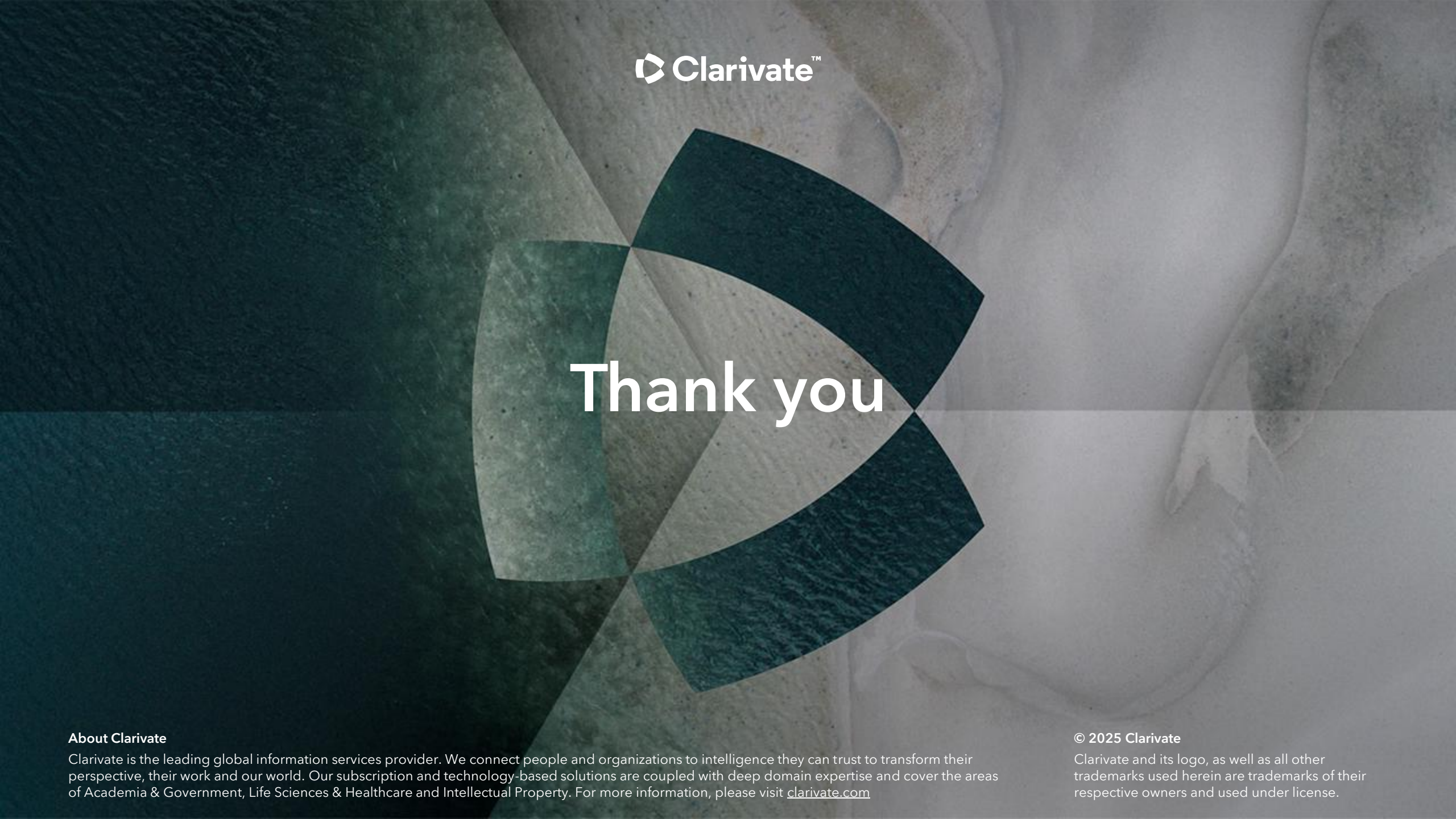


Clarivate™

Mapping: NIS2 to ISO 27001 & SOC 2

- Risk Management → ISO27001 A.6/A.8 → SOC2 CC3
- Access Control → ISO27001 A.9 → SOC2 CC6
- Incident Response → ISO27001 A.16 → SOC2 CC7
- Business Continuity → ISO27001 A.17 → SOC2 A1
- Supplier Risk → ISO27001 A.15 → SOC2 CC9

Clarivate™



About Clarivate

Clarivate is the leading global information services provider. We connect people and organizations to intelligence they can trust to transform their perspective, their work and our world. Our subscription and technology-based solutions are coupled with deep domain expertise and cover the areas of Academia & Government, Life Sciences & Healthcare and Intellectual Property. For more information, please visit clarivate.com