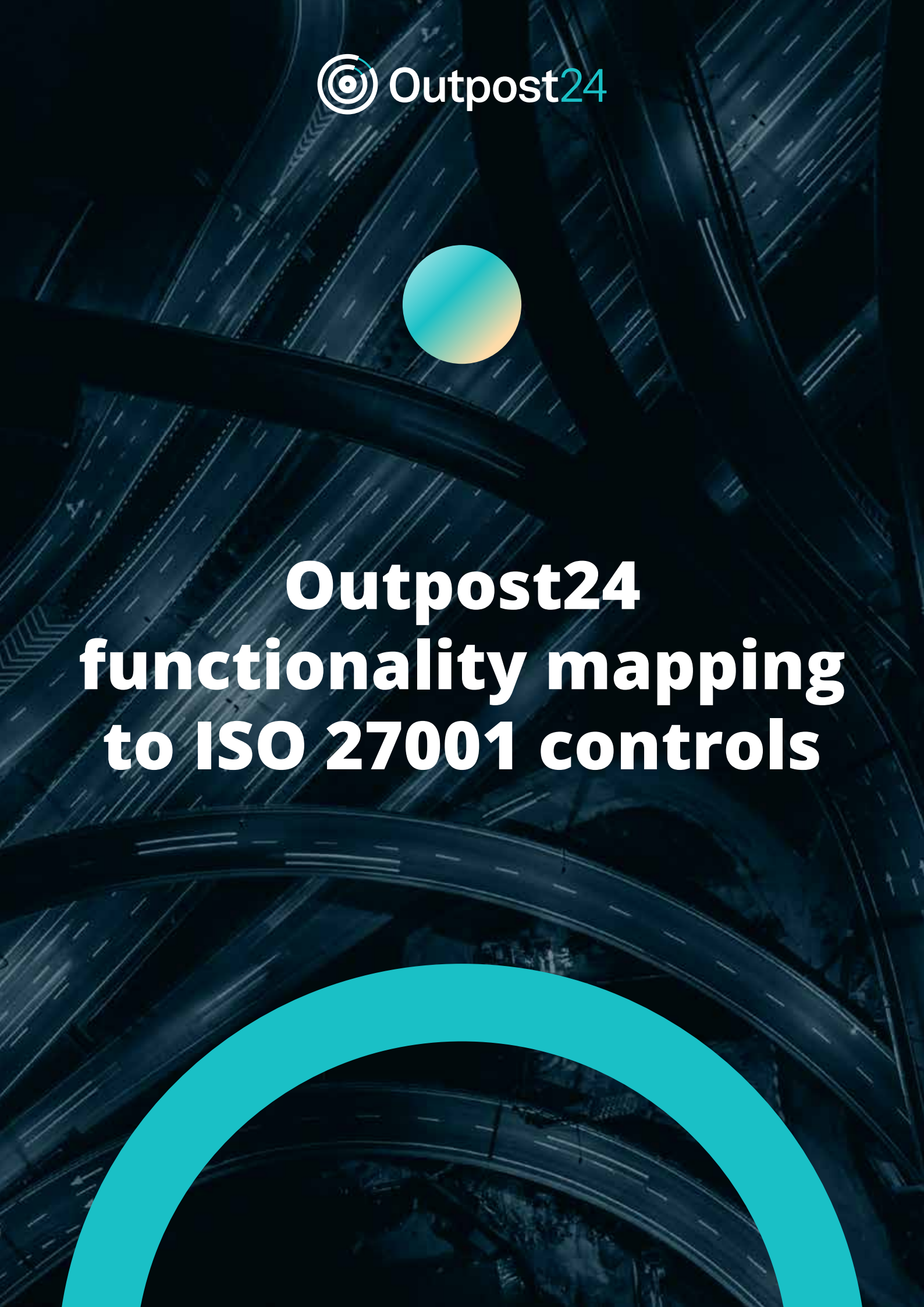

Outpost24

Outpost24 functionality mapping to ISO 27001 controls

The ISO/IEC 27000 series is an industry standard that has long defined and dictated base-level requirements for organizations' information security management systems (ISMS). Through more than a dozen standards, the framework helps organizations demonstrate management commitment to their ISMS as they regularly review and improve their systems and procedures.

By meeting the necessary requirements, organizations are awarded an ISO 27001 certification that lets customers and collaborators know they have robust security measures in place. For more information, see ISO/IEC 27001 compliance guide for CISOs and IT managers.

Outpost24 has been registered by Intertek as conforming to the requirements of ISO/IEC 27001. See certificate.

ISO 27001 information security controls you can address with Outpost24

In reference to the information security controls listed in table A.1 of ISO/IEC 27001:2022, and aligned with those listed in ISO/IEC 27002:2022.

	AwareGo (Partner)	CORE	Outscan NX	Pen testing & Red Teaming	SWAT	Sweepatic	Threat Compass
5 - Organizational controls							
5.1: Policies for information security		x	x				
5.2: Information security roles and responsibilities	x	x	x	x	x	x	x
5.3: Segregation of duties	x	x	x	x	x	x	x
5.4: Management responsibilities	x						
5.7: Threat Intelligence							x
5.9: Inventory of information and other associated assets			x			x	
5.12: Classification of information		x	x				
5.14: Information Transfer			x			x	
5.16: Identity Management			x				
5.21: Managing information security in the ICT supply chain			x			x	
5.23: Information security for use of cloud services			x				
5.25: Assessment and decision on information security events			x				
5.32: Intellectual property rights			x				x
5.34: Privacy and protection of PII							x
5.35: Independent review of information security				x			
5.36: Compliance with policies, rules and standard for information security			x				
6 - People controls							
6.3: Information security awareness, education and training	x						
6.7: Remote working			x				

	AwareGo (Partner)	CORE	Outscan NX	Pen testing & Red Teaming	SWAT	Sweepatic	Threat Compass
7 - Physical controls							
7.1 - 7.14				x			
8 - Technological controls							
8.5 Secure authentication	x	x	x	x	x	x	x
8.7 Protection against malware	x						x
8.8 Management of technical vulnerabilities		x	x		x	x	
8.9 Configuration management			x				
8.12 Data leakage prevention							x
8.16 Monitoring activities				x			
8.20 Network security			x				
8.21 Security of network services			x	x			
8.25 Secure development life cycle				x	x		
8.26 Application security requirements					x		
8.28 Secure coding					x		
8.29 Secure testing in development and acceptance				x	x		

5 – Organizational controls

5.1: Policies for information security

- **CORE:** Aligns the information security policy with business requirements. Core provides a unified view of technical assets with business impact analysis and business logic mapping for review by management and relevant interested parties.
- **Outscan NX:** Provides compliance scanning against a set of rules including a pre-defined (CIS, HIPAA, PCI), or configurable, security standard. This ensures that your assets configurations are in alignment with the IT security policy.

5.2: Information security roles and responsibilities

- **All Products:** Supports and enforces granular access and control policies based on defined security roles and segregation of duties. This includes the designation of asset risk owners for acceptance of residual risks.
- **Outscan NX:** Supports reporting in technical detail for security analysts, high level reporting for management, or simple solutions-oriented reporting for the DevOps teams.

5.3: Segregation of duties

- **All Products:** Supports and enforces granular access and control policies based on defined security roles and segregation of duties.

5.4: Management responsibilities

- **AwareGO:** Provides management with the resources to ensure all personnel achieve a level of awareness of information security through ongoing education.

5.7: Threat Intelligence

- **Threat Compass:** Offers a continuous influx of threat intelligence data, bi-weekly executive briefing updates, and custom alerts when CVEs impact technologies and systems, to help security teams stay up-to-date with relevant security information. Monitor thousands of sources for the latest, actionable, and relevant content for your organization, including deep and dark web communities. Threat Compass also feeds risk-ratings to Outscan NX and CORE to help with vulnerability prioritization.

5.9: Inventory of information and other associated assets

- **Outscan NX:** Enhances asset inventory and vulnerability management with advanced risk-based vulnerability reporting.
- **Sweepatic:** Provides continuous discovery, mapping, and monitoring of all internet-facing assets associated with your business.

5.12: Classification of information

- **CORE:** Supports the classification of assets in alignment with business risk, and its importance to the organization.
- **Outscan NX:** Supports the classification of assets in alignment with business risk, and its importance to the organization.

5.14: Information Transfer

- **Outscan NX:** Supports TLS scanning to audit encryption settings against the NIST Encryption Standards to protect personal and business data in transit.
- **Sweepatic:** Monitors encryption certificates, including TLS protocols, to protect personal and business data in transit.

5.16: Identity Management

- **Outscan NX:** Supports SAML integration for SSO and simplifies the identity lifecycle, including providing or revoking specific access rights.

5.21: Managing information security in the ICT supply chain

- **Outscan NX:** Manages information security risks associated with ICT products through a network scan.
- **Sweepatic:** Manages information security risks associated with ICT products through an external attack surface scan.

5.23: Information security for use of cloud services

- **Outscan NX:** Supports security scans and assessments for all major cloud service providers with risk-based reporting to aid remediation efforts.

5.25: Assessment and decision on information security events

- **Outscan NX:** Supports configurable event notifications, including recipient target groups, to aid with coordinating and responding to information security events.

5.32: Intellectual property rights

- **Outscan NX:** Support granular tagging to group and identify assets with requirements to protect intellectual property rights.
- **Threat Compass:** Detects leaked company documents, and non-compliant use of your business mobile applications in the underground market.

5.34: Privacy and protection of PII

- **Threat Compass:** Detects leaked company documents that may contain personal information.

5.35: Independent review of information security

- **Penetration Testing and Red Teaming Services:** Reviews and audits the security of technologies and people of your business.

5.36: Compliance with policies, rules and standard for information security

- **Outscan NX:** Scans network and assets against the CIS hardening guidelines, via out-of-the-box policy templates, to ensure configurations are aligned with best practice.

6 – People controls

6.3: Information security awareness, education and training

- **AwareGo (Security awareness training partner):** Empowers your workforce with a complete and up-to-date security awareness training platform.

6.7: Remote working

- **Outscan NX:** Supports Agent-based asset scanning for remote employees.

7 – Physical controls

7.1-7.14

- **Red Teaming Services:** Covers the objectives of this entire control by attempting to access your premises (with your permissions) to gauge the level of security measures, and social engineering resistance.

8 – Technological controls

8.5 Secure authentication

- **All Products:** Supports two-factor authentication for all users accessing the platform.
- **Outscan NX:** Validates that the systems that you are running are using secure communication for the authentication flows.

8.7 Protection against malware

- **Threat Compass:** Retrieves stole credentials obtained by malware, and provides situational awareness, threat scoring, and classification of new malware to aid decision making and manage risk. Includes a Sandbox environment where customers can upload Malware files for the Threat Intelligence team to analyze.
- **AwareGO (Security awareness training partner):** Empowers your workforce with the skillset to identify and mitigate spread of malware.

8.8 Management of technical vulnerabilities

- **CORE:** Consolidates vulnerability data from different scanners and technology layers to simplify threat exposure management.
- **Outscan NX:** Combines vulnerability management with risk-based scoring to help address vulnerabilities with the biggest business impact.
- **SWAT:** Continuously monitors internet-facing web applications with context-aware risk coring to help address vulnerabilities with the highest risk.
- **Sweepatic:** Monitors the external attack surface, including known and unknown internet-facing assets, for vulnerabilities and attack paths.

8.9 Configuration management

- **Outscan NX:** Supports compliance scanning of servers and workstations as well as Cloud infrastructrure accounts to ensure that the configurations are aligned to best practices, or your own defined standards.

8.12 Data leakage prevention

- **Threat Compass:** Detects leaked document, credit cards, and credentials to minimize the business impact from already leaked data.

8.16 Monitoring activities

- **Penetration Testing and Red Teaming Services:** Enhances security monitoring and helps formulate baselines and gauge current defences.

8.20 Network security

- **Outscan NX:** Identifies, assesses, and prioritizes vulnerability remediation in your networks with risk-based insights.

8.21 Security of network services

- **Outscan NX:** Identifies, assesses, and prioritizes vulnerability remediations in your network services with risk-based insights.
- **Penetration testing and Red Teaming Services:** Manual infrastructure tests and assessments on internal and external networks.

8.25 Secure development life cycle

- **Penetration Testing:** Provides security guidance in the application development lifecycle, including API assessments, and mobile application assessments.

- **SWAT:** Provides security guidance in the web application development lifecycle via detailed risk assessments.

8.26 Application security requirements

- **SWAT:** Provides security guidance in the web application development lifecycle via detailed risk assessments.

8.28 Secure coding

- **SWAT:** Continuously monitors web applications, with up-to-date information about real-world threat and advice on remediation for continuous improvement.

8.29 Secure testing in development and acceptance

- **Penetration Testing:** Verifies the effectiveness of existing security controls, and helps minimize security gaps with a detailed report of the uncovered issues, including risk level and actionable guidance.
- **SWAT:** Combines the depth and precision of manual penetration testing with vulnerability scanning for continuous monitoring of internet facing web applications.

More information about our products

CORE, Continuous Threat Exposure Management

Outscan NX, Risk-based Vulnerability Management

SWAT, Web Application Security Testing

Sweepatic, External Attack Surface Management

Threat Compass, Cyber Threat Intelligence

More information about our services

Managed Services

Penetration Testing

Red Teaming

Security Awareness Training