HYPERPORT

DATASHEET

NCSC CAF & NIS2 Compliance Mapping

The UK's National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) and the EU's Network and Information Systems Directive 2 (NIS2) establish comprehensive cybersecurity requirements for operators of essential services, digital service providers, and critical infrastructure organizations. Both frameworks emphasize governance, risk management, identity and access control, supply chain security, and incident response capabilities. This mapping document illustrates how the Hyperport Platform's unified, secure access architecture meets the technical and procedural requirements across both frameworks. By implementing zero-trust principles, enforcing least-privilege access, and providing comprehensive audit capabilities, Hyperport enables organizations to streamline compliance efforts while maintaining operational efficiency across on-premises, cloud, and hybrid environments.

NCSC CAF

The National Cyber Security Centre (NCSC) Cyber Assessment Framework provides guidance to organizations on assessing and improving cybersecurity posture across various domains, including governance, risk management, technical security measures, incident response, and supply chain security. It emphasizes the implementation of effective cybersecurity controls to mitigate risks.

NCSC CAF Coverage Summary

NCSC CAF Objective	Principle	Key Hyperport Capabilities
A. Managing Security Risk	A1. Governance	• Enables clear security policy implementation and enforcement • Supports role-based access management aligned with organizational structure • Provides audit capabilities for governance verification
	A2. Risk Management	• Identifies and monitors access-related security risks • Supplies detailed risk reporting for privileged activities • Implements compensating controls for legacy systems
	A3. Asset Management	• Discovers and inventories privileged accounts and access points • Monitors and controls access to critical assets • Enforces security policies based on asset classification
	A4. Supply Chain	• Secures third-party and vendor access to systems • Controls and monitors supplier activities • Implements zero trust principles for supply chain interactions

NCSC CAF Objective	Principle	Key Hyperport Capabilities
B. Protecting Against Cyber Attack	B1. Service Protection Policies and Processes	• Enforces access policies based on organizational requirements • Provides granular control over service access • Monitors policy compliance and implementation
	B2. Identity and Access Control	• Implements strong authentication mechanisms, including MFA • Enforces least privilege and separation of duties • Manages privileged account lifecycles • Provides detailed access audit trails
	B3. Data Security	• Secures data access through identity verification • Controls data movement and transfer • Creates secure channels for sensitive information
	B4. System Security	• Hardens system access points • Controls application and service execution • Manages configuration through privileged access controls
	B5. Resilient Networks and Systems	• Implements network segmentation through identity-based controls • Maintains access during degraded operations • Provides backup access methods for critical functions
	B6. Staff Awareness and Training	• Enforces security awareness through access workflows • Provides just-in-time context for security decisions • Records activities for training and improvement
C. Detecting Cyber Security Events	C1. Security Monitoring	• Monitors all access and authentication events • Identifies anomalous access patterns • Integrates with SIEM and security monitoring tools
	C2. Proactive Security Event Discovery	• Detects unauthorized access attempts • Identifies potential credential compromise • Monitors for privilege escalation and abuse
D. Minimizing the Impact of Cyber Security Incidents	D1. Response and Recovery Planning	• Supports incident response with detailed access information • Provides emergency access procedures • Enables rapid account and access containment
	D2. Lessons Learned	• Records detailed session and access information for analysis • Supports post-incident access review • Enables policy refinement based on incident data

NIS2

The Network and Information Systems Directive 2 (NIS2) mandates operators of essential services (OES) and digital service providers (DSPs) to implement cybersecurity measures ensuring the security and resilience of network and information systems. It establishes requirements for risk management, security measures, incident reporting, and cooperation with authorities to effectively address cyber threats.

NIS2 Coverage Summary

NIS2 Section	Requirement	Hyperport Platform Capabilities
Article 21	Governance and Risk Management	• Implements security policies based on risk assessment • Enforces security controls through access management • Provides audit and documentation capabilities
Section 85	Supply Chain Security	• Secures vendor and third-party access • Controls and monitors supplier activities • Implements zero-trust verification for supply chain access
Section 89	Zero Trust and Network Security	• Implements core zero-trust principles • Enforces continuous verification of identity and devices • Applies least privilege principles to all access requests • Enables network segmentation through identity-based controls
Article 23	Security Measures and Access Controls	• Enforces multi-factor authentication • Implements least privilege access policies • Controls privileged access to critical systems • Provides session monitoring and recording
Article 24	Incident Handling and Reporting	• Enables rapid detection of security incidents • Provides detailed forensic information for analysis • Supports containment through access control • Facilitates incident documentation and reporting
Article 27	Standardized Security Practices	• Aligns with industry best practices for access control • Implements standardized authentication methods • Provides consistent security across environments
Article 28	Security of Cloud Services	• Secures access to cloud resources • Implements consistent security across hybrid environments • Provides visibility and control for cloud service usage

NCSC CAF & NIS2 COMPLIANCE COVERAGE BENEFITS

1 **Unified Security Framework:** The Hyperport Platform provides a consistent security model across on-premises, cloud, and hybrid environments, simplifying compliance with both NCSC CAF and NIS2 requirements.

2 **Zero Trust Implementation:** By enforcing core zero-trust principles (explicitly verifying, using least-privileged access, and assuming a breach), the platform directly addresses key requirements in Section 89 of NIS2 and multiple principles in NCSC CAF.

3 **Supply Chain Risk Management:** The platform's comprehensive controls for third-party access help organizations meet the supply chain security requirements specified in both frameworks.

4 **Comprehensive Audit and Monitoring:** Detailed logging and session recording capabilities support both compliance demonstration and incident response obligations.

5 **Adaptable Security Controls:** The platform's policy-driven approach allows organizations to adapt security controls to specific regulatory requirements while maintaining operational efficiency.

CONCLUSION

The Hyperport Platform facilitates compliance with NCSC CAF and NIS2 by applying consistent security policies across environments, enforcing zero trust principles, and supporting incident response and auditability. It helps organizations streamline cybersecurity operations while meeting regulatory expectations.