Overview

NRD Partners is a specialist cyber security consultancy committed to helping organisations build the confidence, capability, and resilience required to operate securely in an increasingly complex digital environment. We translate evolving threats, regulatory expectations, and technology challenges into clear, practical actions that support informed risk management and strengthen overall security posture.

Our consultants have deep experience across public sector, regulated industries, and large-scale enterprise environments. This enables us to understand operational realities, navigate organisational constraints, and provide advice that is both strategic and actionable. We collaborate closely with leadership and technical teams to ensure our recommendations align with business objectives, regulatory demands, and long-term security ambitions.

As an independent, vendor-neutral consultancy, we provide objective, evidence-based insights free from technology resale or partner incentives. Our approach combines structured methodologies with pragmatic delivery, giving clients clarity, control, and measurable progress whether the focus is cyber strategy, compliance uplift, governance, risk management, or resilience improvement.

About Us

NRD Partners Ltd is a trusted cyber security advisory firm dedicated to supporting organisations through their most significant security, compliance, and transformation challenges. Our team brings together consultants with strong backgrounds in security governance, architecture, cloud assurance, risk management, and operational resilience.

We work across public and private sectors, delivering clear, tailored guidance that enables organisations to address complex security issues while supporting day-to-day operations and strategic objectives. Our engagements are collaborative and transparent, ensuring recommendations are not only robust but also practical and achievable within the organisation's unique context.

Independence sits at the core of our model. With no vendor partnerships or product-led incentives, our clients receive advice that is impartial, context-aware, and rooted in their best interests.

Mission

Our mission is to empower organisations to operate securely and confidently in a constantly evolving digital landscape. We aim to simplify complexity, translate regulatory and threat pressures into meaningful action, and help clients embed strong, sustainable security foundations.

Through rigorous assurance, vendor-agnostic insight, and a commitment to continuous improvement, we support clients in optimising their control environments, reducing exposure, and enhancing resilience at every level of the organisation. Our goal is to ensure that security becomes an enabler of operational agility, innovation, and long-term growth.

Services Overview

NRD Partners delivers specialist cyber security advisory services that help organisations strengthen their resilience, meet regulatory expectations, and operate securely with confidence. Our services provide the structure, insight, and direction needed to navigate complex compliance frameworks and emerging security risks. We work collaboratively with stakeholders across the business to design and embed security practices that are clear, sustainable, and aligned with organisational goals.

Head Office 3rd Floor, 86-90 Paul Street, London, EC2A 4NE
www.nrdpartners.co.uk // **info@nrdpartners.co.uk**

Service Definition: NCSC GovAssure Support Services

NCSC GovAssure Support Services	
Summary	NRD Partners provides structured GovAssure support aligned to the NCSC Cyber Assessment Framework (CAF), helping public sector organisations prepare, validate, and evidence cyber security assessments. Our advisory-led service supports confident self-assessment, risk articulation, and independent assurance readiness in line with National Cyber Security Centre expectations.
Key Features	NRD Partners delivers a structured, evidence-led GovAssure support service aligned to the National Cyber Security Centre Cyber Assessment Framework (CAF). Our approach combines independent challenge, practical advisory support, and deep public sector experience to help organisations prepare, validate, and articulate cyber security assurance for critical systems in a clear, proportionate, and defensible manner. • End-to-end GovAssure advisory aligned to the National Cyber Security Centre Cyber Assessment Framework (CAF), supporting outcome-based assurance for critical systems • Structured approach spanning GovAssure planning, self-assessment, validation, and assurance readiness • Evidence-driven review of policies, technical controls, and operational practices against CAF principles and indicators of good practice • Independent and objective challenge to security assertions, risk statements, and management responses • Pragmatic, proportionate guidance reflecting departmental context, system criticality, and delivery constraints • Clear articulation of cyber risks, control gaps, and prioritised remediation actions aligned to business objectives
Benefits	By applying a consistent and outcome-focused approach to GovAssure, NRD Partners enables public sector organisations to strengthen assurance confidence while reducing delivery risk and rework. Our service supports informed, risk-based decision-making, helping senior stakeholders demonstrate credible cyber resilience aligned to UK Government expectations and organisational priorities. • Strengthens the quality, consistency, and defensibility of GovAssure submissions • Reduces assurance risk by identifying gaps early and minimising rework or challenge • Enables senior leaders to make informed, risk-based decisions with confidence • Supports proportionate cyber security improvements aligned to mission outcomes • Accelerates assurance readiness through structured, expert-led engagement • Builds sustainable alignment with UK Government cyber security strategy and assurance expectations

Service Definition: Virtual CISO (vCISO)

Virtual CISO (vCISO)	
Summary	NRD Partners provides Virtual Chief Information Security Officer (vCISO) services to support public sector organisations with strategic cyber leadership, governance, and assurance. Our service delivers proportionate, outcome-focused security oversight aligned to organisational priorities, enabling senior leaders to manage cyber risk effectively without the need for a full-time CISO.
Key Features	NRD Partners' vCISO service provides trusted, senior-level cyber security leadership tailored to the needs of public sector organisations. We combine strategic oversight with practical delivery support, helping organisations translate policy, risk, and assurance requirements into clear, actionable security direction. Key Features • Senior cyber security leadership delivered on a flexible, part-time basis • Strategic oversight of cyber risk, governance, and security posture • Development and review of cyber security strategies, roadmaps, and policies • Support for assurance activities including GovAssure, audits, and risk committees • Independent challenge and advice to senior stakeholders and boards • Coordination across technology, risk, and delivery teams • Alignment with UK Government cyber security expectations and frameworks
Benefits	By providing experienced cyber leadership without long-term overhead, NRD Partners' vCISO service enables public sector organisations to strengthen cyber resilience, improve assurance confidence, and make informed, risk-based decisions. Our approach supports sustainable security outcomes aligned to mission delivery and organisational maturity. Key Benefits • Access to experienced CISO-level expertise without permanent headcount • Improved clarity and ownership of cyber risk at senior levels • Stronger governance and decision-making across security initiatives • Enhanced confidence in assurance, audit, and regulatory engagements • Proportionate security investment aligned to organisational priorities • Increased resilience through consistent, strategic security leadership

Service Definition: IT Health Check (ITHC)

IT Health Check (ITHC)	
Summary	NRD Partners provides independent IT Health Check (ITHC) services to assess the security of critical public sector systems. Delivered in line with UK Government expectations and the National Cyber Security Centre CHECK principles, our service identifies technical vulnerabilities, control weaknesses, and cyber risks, supporting informed remediation and assurance decision-making.
Key Features	NRD Partners' ITHC service delivers a structured, risk-focused assessment of systems, applications, and supporting infrastructure. Our approach combines technical testing with contextual analysis to provide clear, actionable insight into cyber security weaknesses, aligned to system criticality and public sector risk appetite. Key Features • Independent, objective penetration testing aligned to NCSC CHECK principles • Scoping tailored to system architecture, data sensitivity, and threat exposure • Assessment of infrastructure, applications, and cloud environments • Identification of technical vulnerabilities and security control weaknesses • Risk-rated findings with clear prioritisation and remediation guidance • Evidence-based reporting suitable for assurance, audit, and governance purposes
Benefits	By applying a proportionate and outcome-focused ITHC approach, NRD Partners helps public sector organisations understand real cyber risk, not just technical findings. Our service supports confident remediation, strengthens assurance posture, and enables senior stakeholders to make informed, risk-based decisions. Key Benefits • Provides independent assurance over the security of critical systems • Identifies exploitable weaknesses before they can be used by adversaries • Supports prioritised remediation aligned to operational risk • Strengthens confidence in compliance and assurance activities • Produces clear, defensible outputs for senior stakeholders and auditors • Enhances overall cyber resilience in line with UK Government expectations

Service Definition: PCI DSS Consultancy Services

PCI DSS Consultancy Services	
Summary	NRD Partners supports organisations in understanding and meeting the requirements of the Payment Card Industry Data Security Standard (PCI DSS). Our advisory service provides a clear, structured approach to determining compliance scope, assessing current maturity, identifying gaps, and guiding remediation activities. We help clients reduce complexity, strengthen control effectiveness, and prepare for successful PCI DSS assessment outcomes.
Key Features	Scoping and Applicability Assessment A structured review of cardholder data flows, system boundaries, and third-party dependencies to define a precise and risk-appropriate PCI DSS scope. Readiness Assessment and Gap Analysis An evaluation of existing processes, technology, and controls against PCI DSS requirements to identify areas requiring enhancement. Remediation Planning and Advisory Support Targeted guidance to address identified gaps, prioritise remediation activities, and support effective implementation of required controls. Policy and Documentation Alignment Assistance with creating or refining policies, procedures, and evidence to align with PCI DSS expectations and auditor needs. Pre-Assessment Review A final validation of readiness prior to QSA engagement or SAQ submission, supporting smoother assessment outcomes and reducing the risk of rework. Ongoing Advisory Periodic support to maintain compliance, respond to requirement updates, and assist with year-on-year control assurance.
Benefits	Clarity and Confidence A structured and transparent approach that enables stakeholders to clearly understand PCI DSS expectations and compliance obligations. Reduced Compliance Burden Optimised scoping and focused remediation reduce the operational, financial, and technical effort required to achieve compliance. Enhanced Control Environment Targeted improvements strengthen the organisation's resilience against payment-related security threats. Efficient Assessment Preparation Well-organised evidence, documentation, and readiness activities support a more efficient assessment process with fewer delays. Independent, Objective Insight Vendor-neutral advice provides an unbiased view of control maturity, enabling informed decision-making for security and compliance leaders.

Service Definition: Cyber Maturity

Cyber Maturity	
Summary	NRD Partners provides Cyber Maturity Reviews designed to help organisations understand the effectiveness of their current security capabilities, identify priority areas for improvement, and support strategic decision-making. Our reviews assess governance, processes, technology, and culture against recognised best-practice frameworks, giving leaders a clear, evidence-based view of their security posture and the organisational changes required to strengthen resilience.
Key Features	Structured Maturity Assessment Assessment of security domains such as governance, risk management, identity, network security, data protection, incident response, and resilience. Framework-Aligned Approach Reviews aligned to industry-recognised frameworks (e.g., NCSC CAF, ISO 27001, CIS Controls, NIST CSF), tailored to the organisation's environment and sector. Stakeholder Workshops & Evidence Review Interviews with key stakeholders, document analysis, and validation of existing processes and controls. Maturity Scoring & Gap Identification Clear view of strengths, weaknesses, and maturity levels, with prioritised gaps mapped to strategic objectives and risk appetite. Practical Improvement Roadmap Actionable recommendations and a phased remediation plan that supports informed budgeting, planning, and transformation activities. Executive-Level Reporting Clear, concise reporting for senior leadership, enabling confident communication with internal and external stakeholders.
Benefits	Strategic Clarity A transparent view of the organisation's current maturity and the improvements required to meet business, regulatory, and risk expectations. Prioritised Investment Helps leaders focus time and budget on the areas that provide the greatest security uplift and risk reduction. Enhanced Governance & Control Effectiveness Strengthens oversight, accountability, and alignment to best practice, supporting stronger and more sustainable security operations. Improved Resilience & Preparedness Identifies weaknesses across people, processes, and technology, enabling targeted enhancements to incident response and operational resilience. Decision-Ready Insights for Leaders Executive-friendly outputs support strategic planning, board reporting, and communication with auditors, regulators, and partners.

Service Definition: Security Architecture

Security Architecture	
Summary	NRD Partners provides Security Architecture Review services that help organisations design and maintain secure, resilient, and scalable technology environments. Our consultants assess existing and planned architectures across cloud, hybrid, and on-premise infrastructures to ensure alignment with best practice, regulatory expectations, and business objectives. We provide independent, vendor-neutral guidance that strengthens architectural controls, reduces complexity, and supports secure transformation initiatives.
Key Features	Architectural Assessment & Validation Review of current and target-state architectures, including network, identity, cloud services, data flows, and integration points. Framework & Standards Alignment Assessment aligned to recognised standards such as NCSC Cloud Security Principles, Zero Trust Architecture models, ISO 27001, and CAF/NIST architectural guidance. Threat & Risk Analysis Identification of architectural weaknesses, threat exposures, and design-level risks impacting confidentiality, integrity, and availability. Secure-by-Design Recommendations Actionable guidance to enhance design patterns, segmentation, identity models, data protection, and cloud/hybrid controls. Cloud Security Architecture Review Assessment of major cloud platforms (AWS, Azure, GCP) including landing zones, identity governance, configuration, network patterns, and service deployment models. Target-State Design Support Development of high-level target-state architectural models and patterns that align to business goals and transformation programmes.
Benefits	Stronger Architectural Foundations A clear, structured approach to validating that architecture decisions support robust, scalable, and secure operations. Reduced Risk & Attack Surface Identification of gaps that could lead to compromise, helping organisations mitigate risks early in design and build phases. Accelerated Transformation Security embedded in architectural decision-making, reducing delays and rework during cloud or digital transformation. Improved Alignment with Best Practice Architectures mapped to recognised principles and frameworks, supporting compliance, assurance, and stakeholder confidence. Better Long-Term Resilience Enhancements that improve maintainability, operational readiness, and resilience against future threats and technology changes.

Service Definition: Governance, Risk & Compliance

Governance, Risk & Compliance	
Summary	NRD Partners provides Governance, Risk and Compliance (GRC) services that help organisations establish the structures, processes and controls needed to manage security risks effectively and meet regulatory expectations. Our GRC advisory is designed to give leadership clear oversight, ensure accountability across the organisation, and embed security practices that are proportionate, sustainable and aligned with strategic objectives. We bring clarity to complex regulatory landscapes and support the development of governance frameworks that strengthen decision-making, improve control maturity and enable secure, compliant operations.
Key Features	Governance Framework Development Design and refinement of security governance structures, roles, responsibilities and reporting lines. Risk Management Process Design Implementation of risk assessment, treatment and reporting processes aligned to recognised frameworks. Policy and Standards Development Creation or enhancement of cyber security policies, standards and procedural documentation. Regulatory and Framework Alignment Assessment against, and advisory support for, frameworks such as ISO 27001, NCSC CAF, GDPR, PCI DSS and Cyber Essentials. Control Effectiveness Review Evaluation of existing security controls to assess maturity, coverage and alignment with risk appetite. Assurance and Oversight Support Establishment of oversight mechanisms, KPIs and reporting models for executive and board-level visibility.
Benefits	Improved Accountability and Governance Clearer structures and responsibilities enhance coordination and decision-making across security and risk functions. Consistent Approach to Risk A formalised risk management process supports prioritisation and evidence-based security investment. Stronger Compliance Position Better alignment with regulatory expectations reduces exposure to audit findings and compliance gaps. Enhanced Visibility for Leadership Structured reporting gives leaders the insights needed to understand and manage organisational risk. Sustainable Security Foundations Robust governance, policies and controls help create a resilient, repeatable and scalable security model.