

Crown
Commercial
Service
Supplier



nine23

The High Assurance MSP

ADVISORY SERVICES

Threat, Vulnerability & Risk Assessment

SERVICE DEFINITION

nine23.co.uk

Service Definition

A TVRA is a systematic evaluation that identifies external threats and internal vulnerabilities to determine overall risk levels by analysing potential impacts.

TVRA delivers prioritised, data-driven strategies to mitigate exposure, ensure regulatory compliance, and enhance long-term organisational security and resilience.

Service Features

- **Compliance Alignment Auditing:** Matches security posture against NCSC CAF, NIST CSF, ISO 27001, or GDPR requirements.
- **Comprehensive Asset Discovery:** Identifies all hardware, software, and cloud-based digital resources.
- **Dynamic Threat Profiling:** Maps specific external adversaries against your organisation's unique footprint.
- **Automated Vulnerability Scanning:** Continuously detects technical weaknesses and outdated software across networks.
- **Impact Analysis Metrics:** Evaluates the potential operational and financial damage of breaches.
- **Likelihood Probability Scoring:** Determines the statistical frequency of specific security threats occurring
- **Prioritised Remediation Roadmaps:** Ranks critical fixes based on risk levels and urgency.
- **Security Control Validation:** Tests existing defences to ensure they function as intended.
- **Actionable Executive Reporting:** Provides clear, data-driven insights for high-level strategic decision-making.
- **Third-Party Risk Evaluation:** Analyses vulnerabilities introduced by external vendors and supply chains

Service Benefits

- **Proactive Risk Mitigation:** Identifies and fixes critical security weaknesses before attackers exploit them.
- **Enhanced Regulatory Compliance:** Ensures adherence to strict 2026 legal standards like GDPR and NIS2
- **Optimised Resource Allocation:** Directs cybersecurity budgets and personnel toward the highest-priority business risks.
- **Improved Operational Resilience:** Minimises costly system downtime by predicting and preventing potential disruptions.

- **Data-Driven Decision Making:** Provides executives with quantified financial risk metrics for strategic planning.
- **Strengthened Stakeholder Trust:** Demonstrates a commitment to security, boosting confidence for customers and partners.
- **Refined Incident Response:** Informs better emergency playbooks based on identified high-impact threat scenarios.
- **Third-Party Risk Visibility:** Uncovers hidden vulnerabilities within complex digital supply chains and vendors.
- **Reduced Insurance Premiums:** Lowers cyber-insurance costs by proving a proactive and mature posture.
- **Enhanced Security Awareness:** Fosters a culture of vigilant behaviour among employees and leadership.

Problems Solved

All organisations know that understanding and improving cyber resilience is a key business requirement in the digital age. But where to start?

Cyber security technology requires significant investment and the benefits in terms of cyber risk reduction and resilience will not be realised without an effective and well thought through risk assessment against which cyber security investments can be prioritised against the most impactful risks.

Outcomes

A risk assessment should be the starting point for all investment decisions regarding cyber security controls. The risk assessment ensures the key stakeholders can see which risks are most likely to occur and most impactful to cyber resilience.

This enables investment in security controls to be prioritised, the level of residual risk held by the organisation to be understood and is pivotal in providing a 'golden thread' with full traceability from business need through to the implementation and maintenance of security controls.

What Nine23 Do & Why

Nine23 is a veteran-owned **UK Sovereign, High-Assurance Managed Service Provider (MSP)** delivering cyber secure, resilient digital services for mission-critical operations.

Our service offerings include:

- InfoSec Advisory and Assurance
- Private/Hybrid Cloud
- Secure Collaboration
- Interoperability

Our solutions are built to meet the most stringent regulatory compliance requirements and are fully aligned with NCSC/DSIT guidance and Secure by Design principles. We enable individuals and organisations to operate with confidence, security and compliance.

Who Nine23 Work With

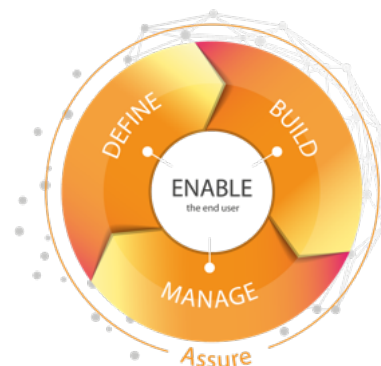
Nine23 delivers exceptional services to Discerning Clients in **UK Regulated Sectors who handle protectively marked data at above OFFICIAL**. We enable the HM Government, National Security and Public Safety, Defence Industry and their supply chains to collaborate and interoperate with simplicity, without ever compromising on security.

We have demonstrated significant achievements in difficult to break into sectors and have a stellar list of clients which demonstrates our credibility.

How Nine23 Work

Our Model

Our operating model builds security, usability, and compliance in from day one, so your technology, people, and processes work seamlessly together. As cyber threats evolve, so do we – keeping your users secure, empowered, and productive through continuous improvement, user-focused design, and UK sovereign solutions that meet national security standards.



Define - Your Problem

We understand information security and assurance as a business enabler, not a constraint. Our experts will conduct a comprehensive discovery phase to assess current capabilities and risks, define key security objectives, compliance standards, and end-user requirements, and develop a clear roadmap that enables digital transformation with high assurance at its core.

Build - Your Solution

We combine the best technology from the best vendors to create an environment that enables individuals to work together effectively and securely. Leveraging trust, innovation, and a depth of sector experience to provide collaboration and interoperability.

Manage - Your Service

We deliver high assurance and resilient managed services that enable seamless interoperability for teams to access the data and applications they need to work collaboratively. Our managed services include:

- 24/7 monitoring, proactive risk management, and compliance assurance
- Threat detection, response, and continuous security improvements
- A transparent Service Level Agreement (SLA) ensuring clear accountability.

Why Choose Nine23?

Enabling the end user is the heart of everything we do, empowering them to work with the same simplicity and usability they expect at home, without ever compromising on security. We are **trusted, proven experts with a strong track record** of delivering nationally accredited, user-focused solutions in complex and highly regulated environments.

We deliver high assurance solutions **accredited for use at OFFICIAL (including SENSITIVE and other caveats) through to SECRET**, meeting the most stringent cyber security requirements. As a fully UK-owned and operated company, with all staff, infrastructure, and data located in the UK, we provide genuine **100% UK data sovereignty**.

Above all, we are **refreshingly honest**. Building long-term relationships through transparency and integrity, with no jargon or hidden risks, just secure solutions that deliver real operational value.

