Nanorisk

Advanced Security for Advanced Threats

Capability & Services

An introduction to Nanorisk: who we are, how we work, and the full range of security assessments we deliver.

CREST Accredited | Cyber Essentials Plus | IASME Cyber Assurance | CCS Supplier

DOCUMENT
September 2026

CLASSIFICATION
Public

VERSION
1.0

Copyright © 2026 Nanorisk Limited. All rights reserved.

Contents

About Nanorisk

Nanorisk is a CREST accredited, UK-based cyber security consultancy delivering structured, evidence-led security assessments across infrastructure, applications, social engineering, and specialist environments.

We are an independent assessment consultancy. We do not sell security products, raw automated tooling output, or certification services. That independence is deliberate. It means our findings carry no commercial incentive to recommend a particular vendor, and no interest in discovering problems we would then charge to fix.

Engagements are delivered by experienced consultants holding recognised industry certifications from bodies including CREST, Offensive Security, and INE. Every engagement runs against a documented, standards-aligned methodology, and every deliverable passes independent quality assurance before it reaches the client.

Our approach

Nanorisk delivers a high-calibre professional service across every engagement, from initial consultation through to detailed, actionable reporting and post-assessment support, including retesting where applicable. Every engagement runs through the Nanorisk Security Portal, our own platform, where scoping, delivery, findings and reporting live.

Penetration testing is manual, evidence-led and risk-focused. Assessments are carried out by experienced consultants working the environment by hand, reasoning about how systems can be abused, chaining weaknesses together, and testing the logic and authorisation behind an application rather than its surface.

On penetration testing engagements, automated tooling plays a supporting role, giving breadth across large estates, but it is an input to the assessment and never the assessment itself. Business logic flaws, authorisation weaknesses and chained attack paths do not appear in scanner output, and those are frequently the findings that matter most.

2021	CREST	6	43
ESTABLISHED	ACCREDITED	ACCREDITATIONS	ASSESSMENT SERVICES

SELECTED CLIENTS

GOV.UK · Kindus · CHIPSIDE part of the unity5 group · OpenGenius · LMA Loan Market Association · TRIP iQ · KAI

Nanorisk Limited · Company No. 13809559 · The Work Place, Aycliffe Business Park, Heighington Lane, Newton Aycliffe, DL5 6AH

What Makes Us Different

Quality security services at affordable prices: professional penetration testing and security assessments without the premium price tag.

01

Quality-Driven Assessments

Every engagement follows structured, evidence-led methodologies with formal scoping, experienced consultants, and rigorous internal quality assurance. All of our consultants are UK based, and all testing is carried out from the UK.

02

Comprehensive Service Range

From vulnerability assessments to specialist red team operations, we offer a full spectrum of security testing services to meet any requirement.

03

Affordable Pricing

We deliver professional-grade security services at competitive rates, typically charging less than larger consultancies without compromising on quality.

04

Full Transparency

Clear communication throughout every engagement. No hidden costs, no surprises. You know exactly what you're getting and what it costs upfront.

05

Comprehensive Documentation

Detailed, actionable reports with clear findings, evidence, and practical remediation guidance. Our documentation supports your compliance and governance needs.

06

Dedicated Security Portal

All engagements managed through our secure portal providing real-time visibility, document management, finding tracking, and streamlined communication.

Accreditations & Credentials

Nanorisk holds accreditations that are independently assessed and continuously reviewed. Every credential below can be verified directly with the issuing body.

HELD AND INDEPENDENTLY VERIFIABLE

ACCREDITATION	WHAT IT DEMONSTRATES	REFERENCE
CREST Penetration Testing CREST · Accredited	Assessment of the organisation itself: methodology, data handling, personnel vetting, and quality assurance, not just individual qualifications	Accredited member company, listed in the CREST directory
Cyber Essentials IASME · Certified	Baseline technical controls independently certified	c7a00ac1-ccbc-41c2-8510-e770dd109646
Cyber Essentials Plus IASME · Certified Plus	Hands-on technical audit verifying those controls are correctly implemented	300a4a7d-946b-48e0-88ab-7bb0a140d84f
IASME Cyber Assurance Certified · Level One	Broader information assurance covering governance, risk and data protection	dafef168-9cda-4d32-a786-4a7995c8861e
IASME Quality Principles Certified	Assessed quality of service delivery	c75acb0e-087e-4313-b5a1-349266f061ec
Crown Commercial Service Approved Government Supplier	Approved to supply to UK public sector bodies	Government framework supplier

Why CREST accreditation matters

CREST accreditation is awarded to the company, not to an individual. It examines how the organisation scopes, delivers, evidences and quality assures its work, how it vets its people, and how it handles client data. It is the recognised mark that a testing provider operates to a professional standard.

> Every credential above can be verified directly with the issuing body. Certificates and verification links are published at www.nanorisk.co.uk/accreditations.

Our Team

Nanorisk's testing team is small, senior and directly accountable. You will know who is testing your environment, and you will deal with them directly on the technical work rather than through an account manager.

ROLE	RESPONSIBILITIES
Director / Senior Security Consultant	Scoping, engagement delivery, quality assurance and technical oversight
Business Development Executive	First point of contact for new enquiries, and commercial support through scoping and quotation
Security Consultant × 2	Engagement delivery across infrastructure, application and specialised assessments, and independent quality assurance of the Director's reports
Social Engineering & Physical Security Specialist	Social engineering, phishing and physical security assessments

Certifications held across the team

- CREST CRT
- INE eJPT, eCPPTv2 and eWPT
- Altered Security CRTP
- Cyber Essentials Assessor
- IASME Cyber Assurance Level One and Level Two Assessor

> Named consultants and their individual qualifications are confirmed at scoping and recorded in the Statement of Works, so you know before testing begins exactly who will be working on your environment.

Vetting and professional standards

All personnel and contractors are vetted once at onboarding, before they undertake any delivery work, and are bound by Nanorisk's Consultants Code of Conduct and Ethics Policy, its Information Security Policy, and contractual confidentiality, intellectual property and non-solicitation terms.

Personnel complete induction and onboarding training covering information classification and handling, cybercrime law, and the permitted and prohibited actions that govern our testing.

Capacity

Our personnel and capability list is maintained as a controlled document and reviewed whenever the team changes, and at least annually. It is available to clients and prospective clients on request.

How We Work

Every engagement runs against a single documented methodology, applied proportionately to the service and the agreed scope, so delivery is consistent and repeatable regardless of which consultant does the work.

Recognised frameworks and standards

Our methodology is aligned with recognised industry frameworks, applied according to the service delivered:

- **NIST SP 800-115**, Technical Guide to Information Security Testing and Assessment, for the overall assessment process
- **PTES**, Penetration Testing Execution Standard, for engagement structure
- **OWASP**, Web Security Testing Guide (WSTG), Application Security Verification Standard (ASVS), API Security Top 10, and Mobile Application Security Verification Standard (MASVS)
- **OSSTMM**, Open Source Security Testing Methodology Manual principles
- **MITRE ATT&CK**, for adversary simulation and red teaming
- **CIS Benchmarks** and vendor best practice, for configuration and cloud reviews
- The professional standards of the **CREST** and **CHECK** schemes

Testing phases

Within delivery, testing follows a structured, phased approach, applied proportionately to the service: information gathering and reconnaissance; enumeration and scanning; vulnerability identification; controlled exploitation and validation; post-exploitation where authorised; analysis; and reporting.

Standards applied by service

SERVICE	PRIMARY STANDARD APPLIED
Web Application	OWASP WSTG and ASVS
Web Service / API	OWASP API Security Top 10 and ASVS
Mobile Application (iOS / Android)	OWASP MASVS and MSTG
External / Internal Infrastructure	NIST SP 800-115, PTES, OSSTMM
Active Directory & Network Configuration	PTES, vendor and CIS best practice
Cloud Environment	CIS Benchmarks and cloud provider security best practice
Wireless	PTES wireless, OWASP guidance
Red Team	MITRE ATT&CK
Configuration & Build Review	CIS Benchmarks and vendor hardening guidance

Tooling

Testing uses only approved tools recorded in Nanorisk's tool inventory, governed by our Penetration Testing Tool Management Policy, which controls how tools are evaluated, selected, reviewed and kept current.

Risk rating

Nanorisk takes a contextual and pragmatic approach to severity. Rather than relying on automated scoring alone, every finding is evaluated on three factors, which together produce a qualitative severity rating:

Technical impact
The consequence to the organisation should the vulnerability be exploited.

Likelihood of exploitation
The probability of successful exploitation in the context of the target environment.

CVSS v4.0 Base Score
The industry-standard, repeatable measure of inherent severity.

Qualitative Severity Rating

Impact represents the potential consequence to the organisation should the vulnerability be exploited, considering the effect on confidentiality, integrity, availability, business operations, and potential regulatory or reputational harm. *High* means exploitation would likely result in major operational disruption, data loss, or reputational and regulatory consequences. *Medium* means moderate disruption or compromise of systems or data, with manageable impact. *Low* means minimal effect on operations or data.

Likelihood reflects the probability of a vulnerability being successfully exploited in the context of the target environment, considering exploit availability, exposure level, required access, user interaction, and the sophistication of the attack. *High* means exploitation is likely with minimal effort, often requiring little or no user interaction or access. *Medium* means exploitation is feasible but may depend on specific conditions, user interaction, or limited access. *Low* means exploitation is unlikely or would require significant effort, advanced access, or uncommon circumstances.

CVSS v4.0 provides the repeatable industry measure. Base metrics capture the inherent qualities of a vulnerability that are constant over time, threat metrics indicate whether it is actively being exploited, and environmental metrics allow the score to be tailored to your infrastructure and asset sensitivity. Incorporating threat and environmental metrics gives a more contextual and accurate rating than the base score alone.

EVERY FINDING IS RATED ON CVSS V4.0

Critical	High	Medium	Low	Informational
9.0 – 10.0	7.0 – 8.9	4.0 – 6.9	0.1 – 3.9	0.0

Every finding is also mapped to the **Common Weakness Enumeration (CWE)**. Ratings are applied consistently across consultants and engagements, supported by Nanorisk's maintained findings library, and the full rating methodology is reproduced in Appendix A of every report.

The Engagement Lifecycle

While each engagement is tailored to the client's environment and objectives, most assessments follow a common lifecycle.

01 **Enquiry and Scoping**
An engagement begins with an initial enquiry and scoping discussion to understand objectives, environment, constraints, and desired outcomes. Scope, assumptions, exclusions, and proposed timelines are defined during this phase.

02 **Formal Authorisation and Onboarding**
A quote and Statement of Work are issued through the Security Portal. Engagements commence only after contractual documentation has been reviewed and formally accepted.

03 **Prerequisites and Asset Onboarding**
Clients provide agreed prerequisites through the Security Portal. This information populates the asset catalogue, defining in-scope systems and environments for the assessment.

04 **Assessment Delivery**
Assessments are conducted within the defined scope and rules of engagement. Critical or high-risk findings are flagged promptly. Where appropriate, findings are visible within the portal as they are identified.

05 **Live Validation**
Where permitted, clients may remediate findings during the assessment window and request validation. This allows issues to be confirmed as resolved before the assessment concludes.

06 **Quality Assurance and Reporting**
All findings undergo internal quality assurance. Reports include engagement scope, detailed findings with evidence, risk context, and remediation guidance, delivered through the Security Portal.

07 **Wash-Up and Next Steps**
Clients may request a wash-up call to review findings, clarify report content, and discuss remediation priorities. This ensures findings are clearly understood and appropriately contextualised.

08 **Formal Retesting**
Post-engagement retesting validates remediation efforts and is delivered as a separate retesting report through the Security Portal. Retesting scope and timing are defined contractually.

Scope changes

Testing is conducted only within the authorised scope. Any action outside it requires your authorisation before proceeding, recorded through a formal Scope Change and Deviation Request.

Quality Assurance

Quality is treated as a defined, managed and auditable part of every engagement rather than an informal afterthought.

> No report is ever self-reviewed.

Reports are never self-reviewed

All assessment reports are subject to a formal, recorded quality assurance review before delivery, managed through the Nanorisk Security Portal:

01 **Submitted for QA**
On completion of the assessment, the consultant marks the report as “Ready for QA” in the Portal.

02 **Assigned to an independent reviewer**
The report is reviewed by a person independent of the author. The Director reviews a consultant's report; where the Director is the author, a separate suitably experienced consultant performs the review.

03 **Reviewed section by section**
The reviewer examines every section, executive summary, technical summary, narratives and findings, checking technical accuracy, completeness, correct risk rating, internal consistency, evidential support and clarity.

04 **Passed or returned**
If the report meets the standard, QA is marked as passed and it proceeds to delivery. If not, review comments are recorded against the relevant sections, QA is failed, and the report returns to the consultant.

05 **Repeated until it meets the standard**
The cycle repeats until the report passes QA. Only quality-assured deliverables are issued.

Commercial documents too

Statements of Works and Quotes are quality assured before issue, so the commercial basis, scope and deliverables agreed with you are checked before commitment.

Feedback and improvement

Client feedback, complaints and lessons learned feed back into the system through a defined issue and complaint handling process.

Reporting & Deliverables

The report is the product. Ours are structured to serve both the engineer who has to fix the problem and the board member who has to understand the risk.

WHAT A NANORISK REPORT CONTAINS

01	**Executive Summary**	What was found and what it means commercially, written to be read by a non-technical audience
02	**Technical Summary**	Scope, timeline, overview, remediation actions and caveats
03	**Assessment Findings**	Score cards, graphs and the assessment results at a glance
04	**Technical Details**	The issues themselves, with full narrative and supporting evidence
05	**Open-Source Intelligence Gathering Report**	A full OSINT report on your organisation's public exposure, included at no additional cost
06	**Threat Intelligence**	A threat intelligence report covering the environment assessed
07	**Post-Assessment Clean-Up**	Confirmation of what we removed and reverted
08	**Appendices**	Risk ratings explained, methodologies used, and tools used

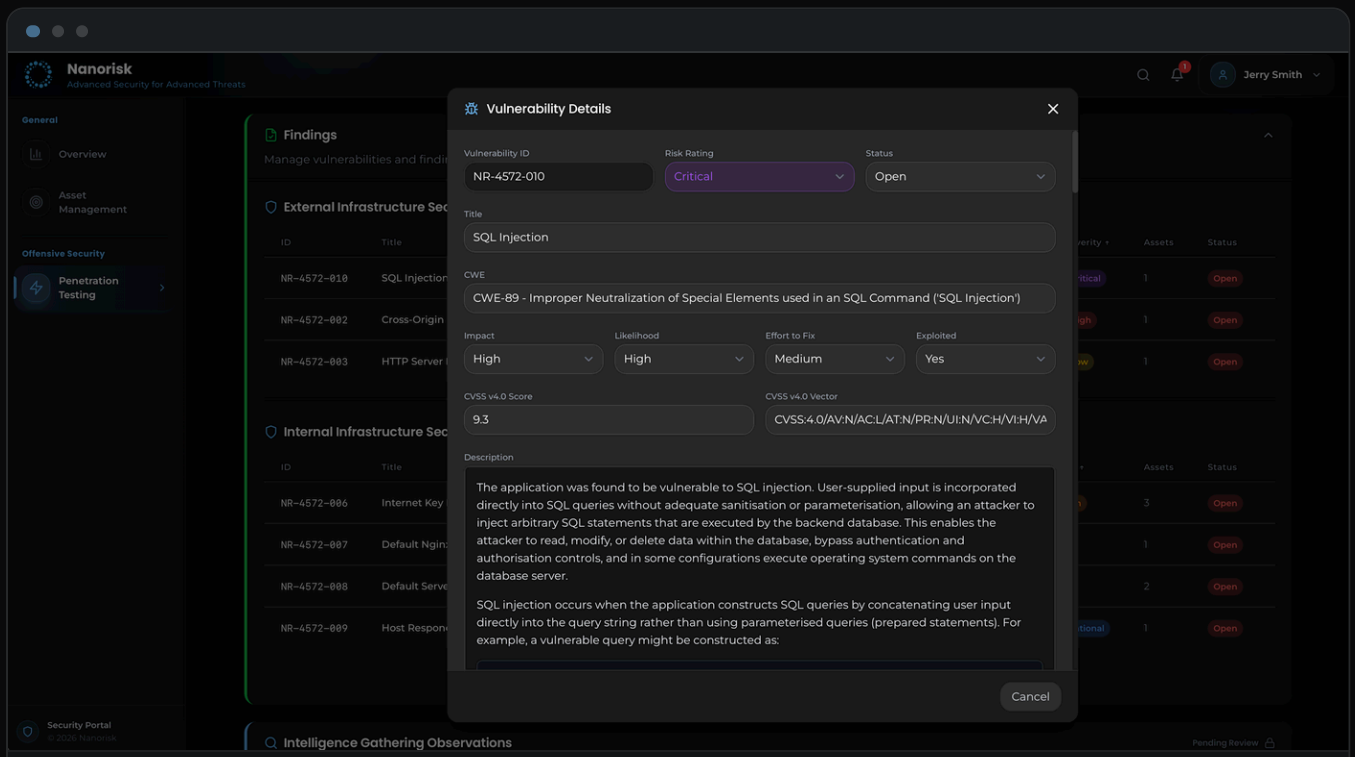
Alongside the report

Engagements are supported by an attestation letter suitable for sharing with your own clients, auditors or insurers, and by the Portal record of every finding, its status and its retest history.

A spreadsheet export of your current findings can be generated at any point, during the assessment as well as after it, giving you an up-to-date working list to hand straight to the teams doing the remediation, without waiting for the final report.

Every finding carries

- A CVSS v4.0 score and vector, and a CWE mapping
- Impact, likelihood and effort-to-fix ratings
- Whether the issue was successfully exploited during testing
- A full technical description, an impact description written in business terms, and specific remediation guidance
- Supporting evidence, sanitised or redacted where appropriate



A finding as the client sees it

CVSS score and vector, CWE mapping, exploitation status, business impact and specific remediation guidance, tracked individually rather than buried in a PDF appendix.

Retesting & Wash-Up

Finding the problem is only half of the job. Retesting is built into how we deliver rather than sold back to you afterwards.

Included with every assessment

- **Retesting of up to five findings of your choosing, free of charge**, for up to 60 days after the assessment. You decide which five matter most, rather than us deciding for you.
- **A wash-up call, free of charge**, to walk through what was found, clarify anything in the report, and talk through remediation priorities.
- Retest outcomes issued as a separate retesting report through the Nanorisk Security Portal, so you have written evidence that a fix has been verified.

Fixing issues during the assessment

You do not have to wait for the report to start fixing things. Where a finding is remediated while testing is still under way, you can mark it as **client closed** in the Portal. We will retest it during the assessment, and where the fix holds, close it out before the report is issued.

This means straightforward issues can be resolved in days rather than waiting for a scheduled retest cycle, and the final report reflects the state of your environment at the end of the engagement rather than the start.

Retesting beyond the included five

Additional retesting is chargeable, priced on the time required to test the extra findings. You will be told what that involves and what it costs before any work is booked, and it is issued through the Portal in the same way.

> The retest provision for your engagement is confirmed in the Statement of Works before testing begins.

The Nanorisk Security Portal

Every Nanorisk engagement is managed through the Security Portal, the central hub for engagement management, communication, and reporting.

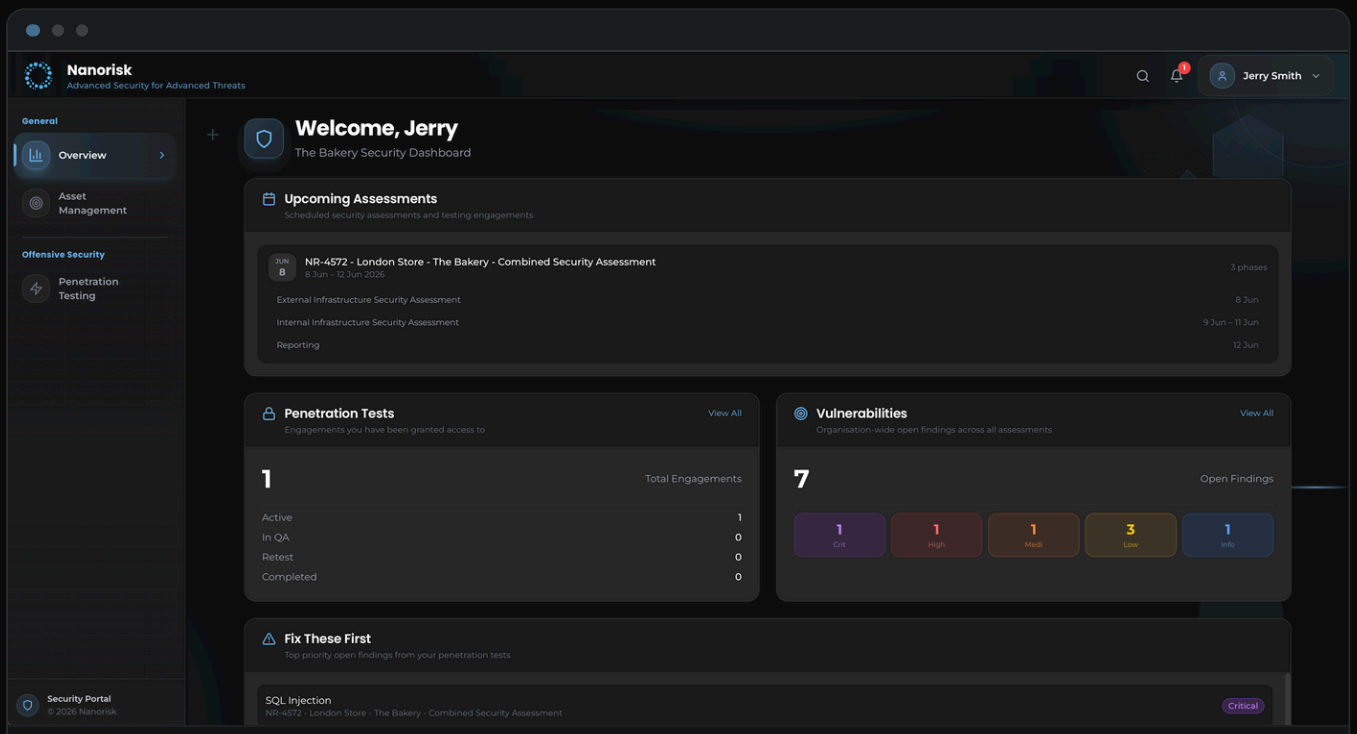
From scoping through to delivery and beyond, everything is accessible, documented, and auditable in one secure platform, eliminating the need for sensitive information to be exchanged over email. The portal is included with every engagement at no additional cost.

Included
WITH EVERY ENGAGEMENT

Real-time
FINDINGS & REPORTS

Secure
ENCRYPTED COMMUNICATION

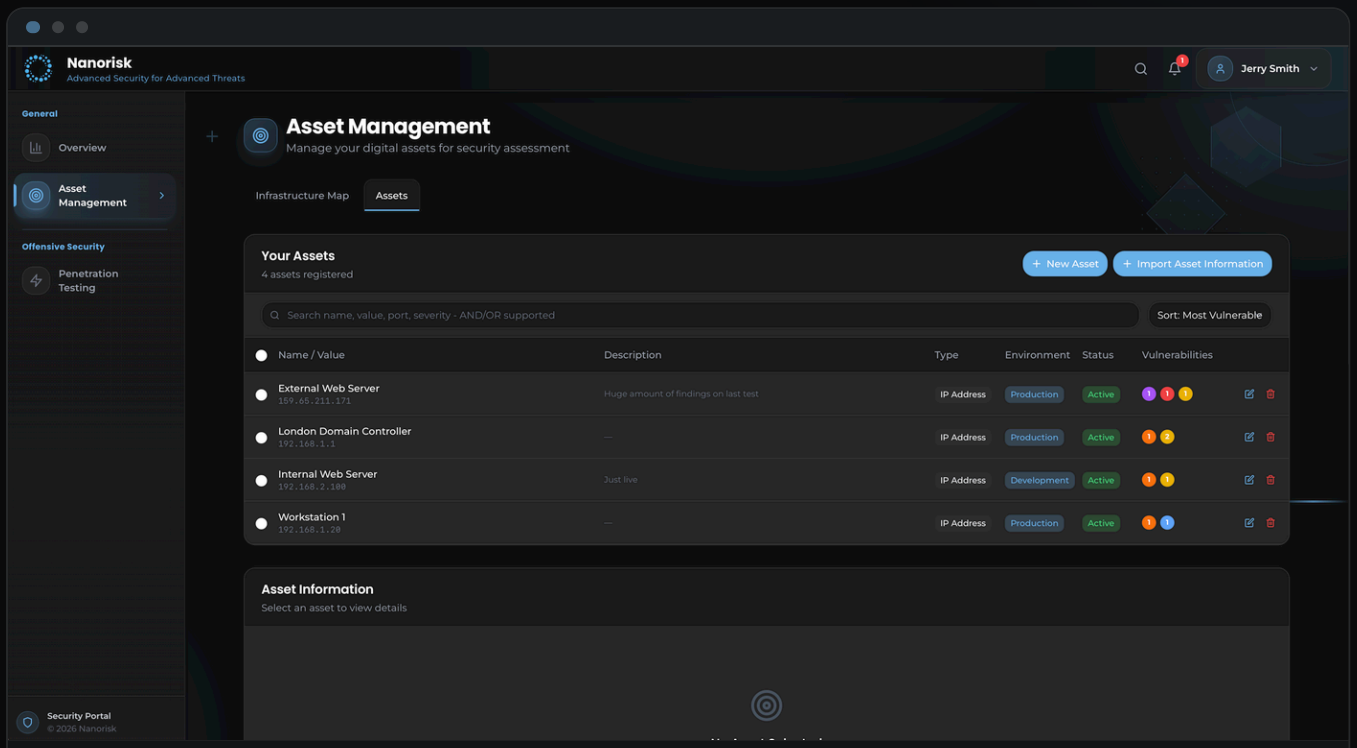
2FA
AUTHENTICATION



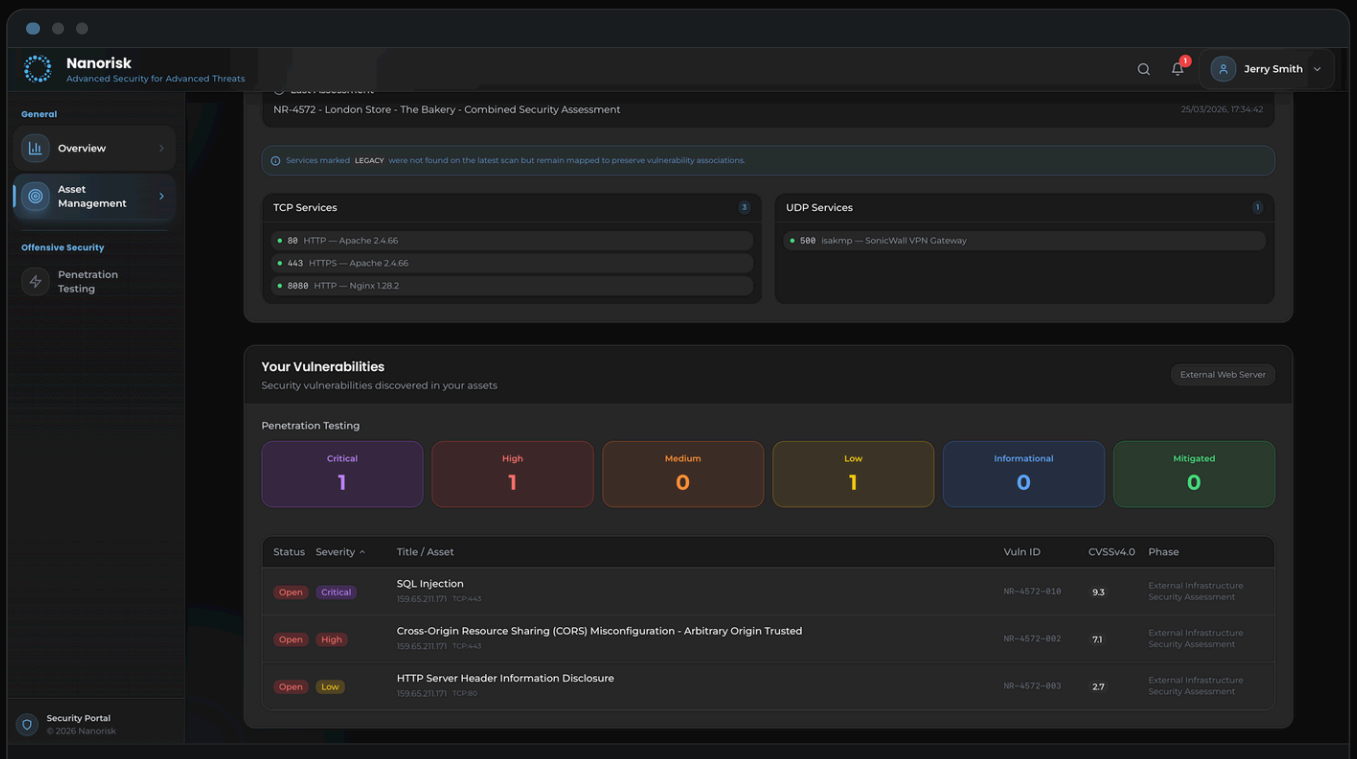
Overview Dashboard
Your security posture at a glance: an immediate, consolidated view across all active Nanorisk services, including your security score, module status, risk heatmap, threat intelligence, and activity timeline.

Asset Management

The Asset Management module maintains a full inventory of your digital assets, the servers, applications, APIs, cloud services, and infrastructure that form the scope of your assessments. Every vulnerability and finding is linked directly to the affected asset.



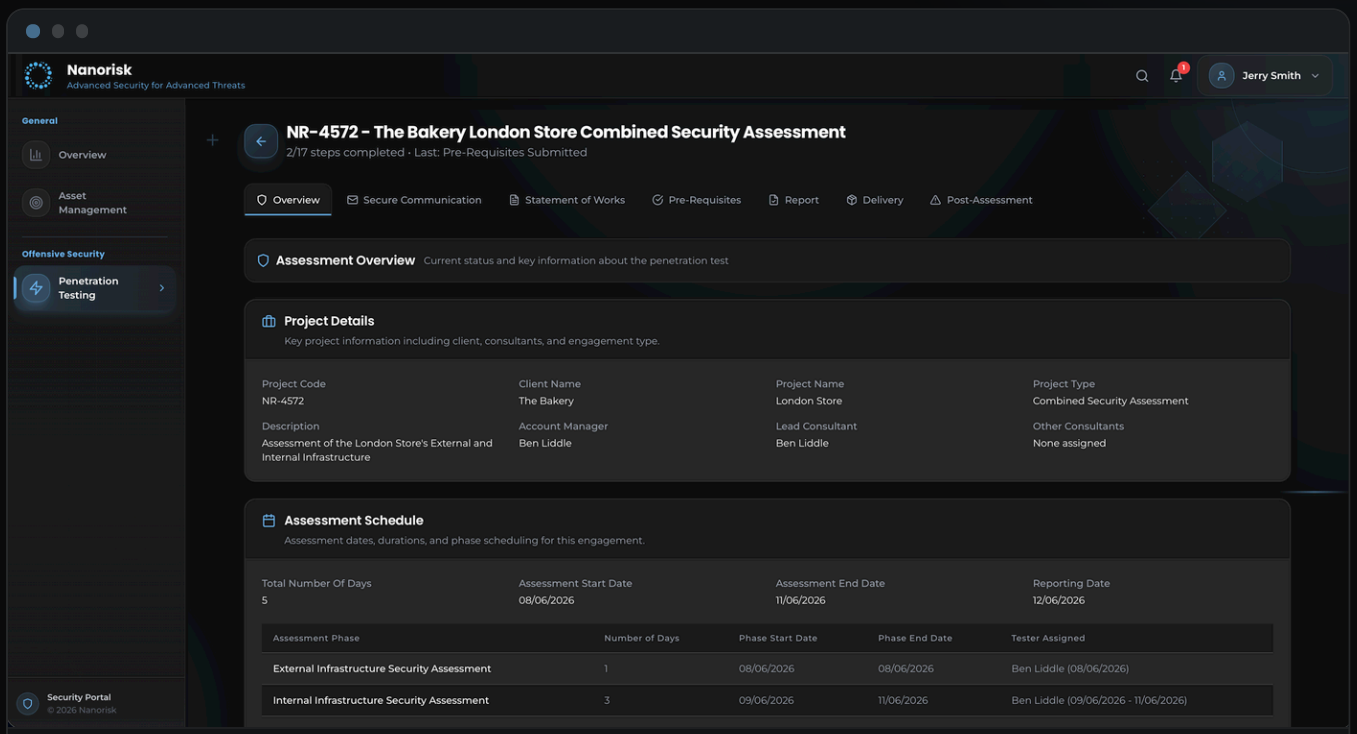
Asset inventory



Vulnerabilities by asset

Penetration Testing

Every penetration testing engagement is managed through the portal from initial scoping through to final delivery. Track progress, review documents, access findings, and communicate securely, all from a single project view.

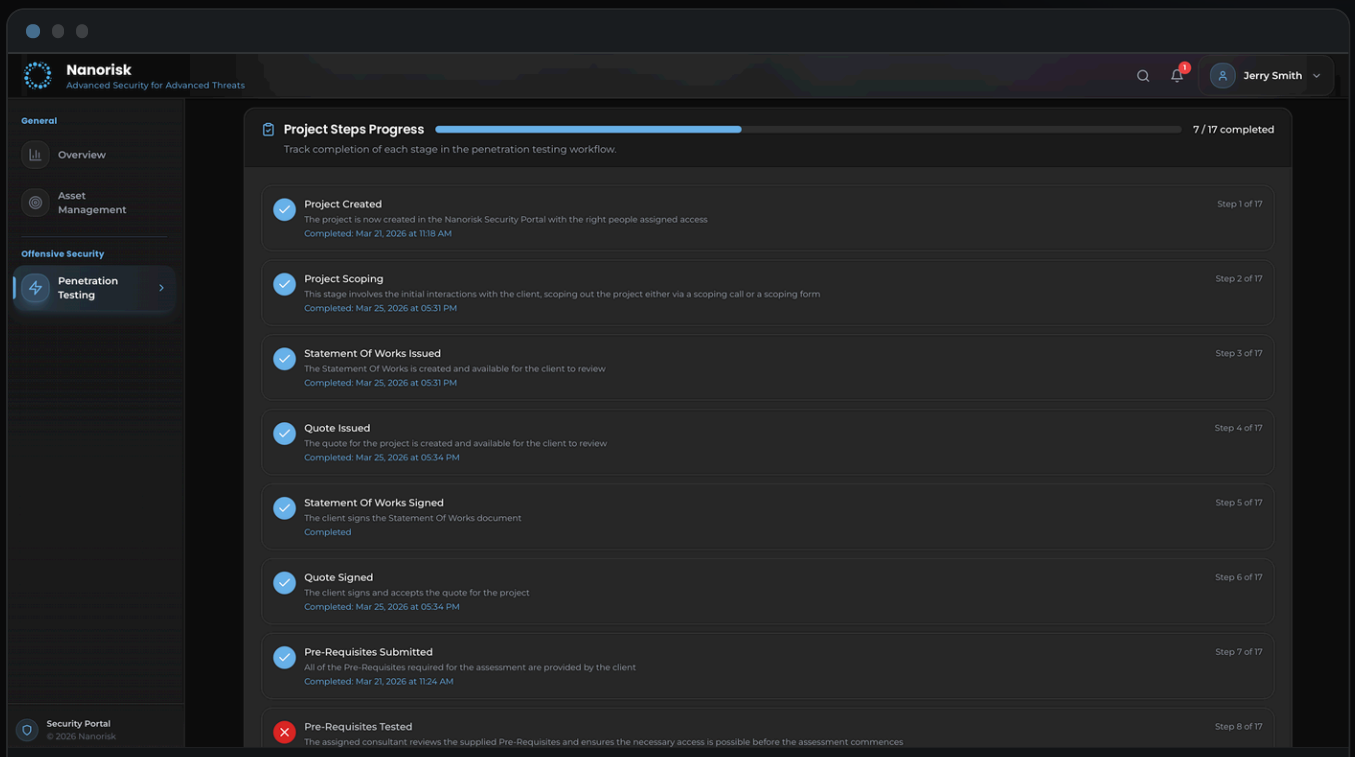


Engagement view

Scope, rules of engagement, prerequisites and deliverables in a single project view.

Engagement roadmap

We provide a step-by-step roadmap for each penetration testing project so you can see at any time what stage you're at and what's coming next. The portal tracks progress through each phase, from scoping and authorisation through to delivery and retesting.

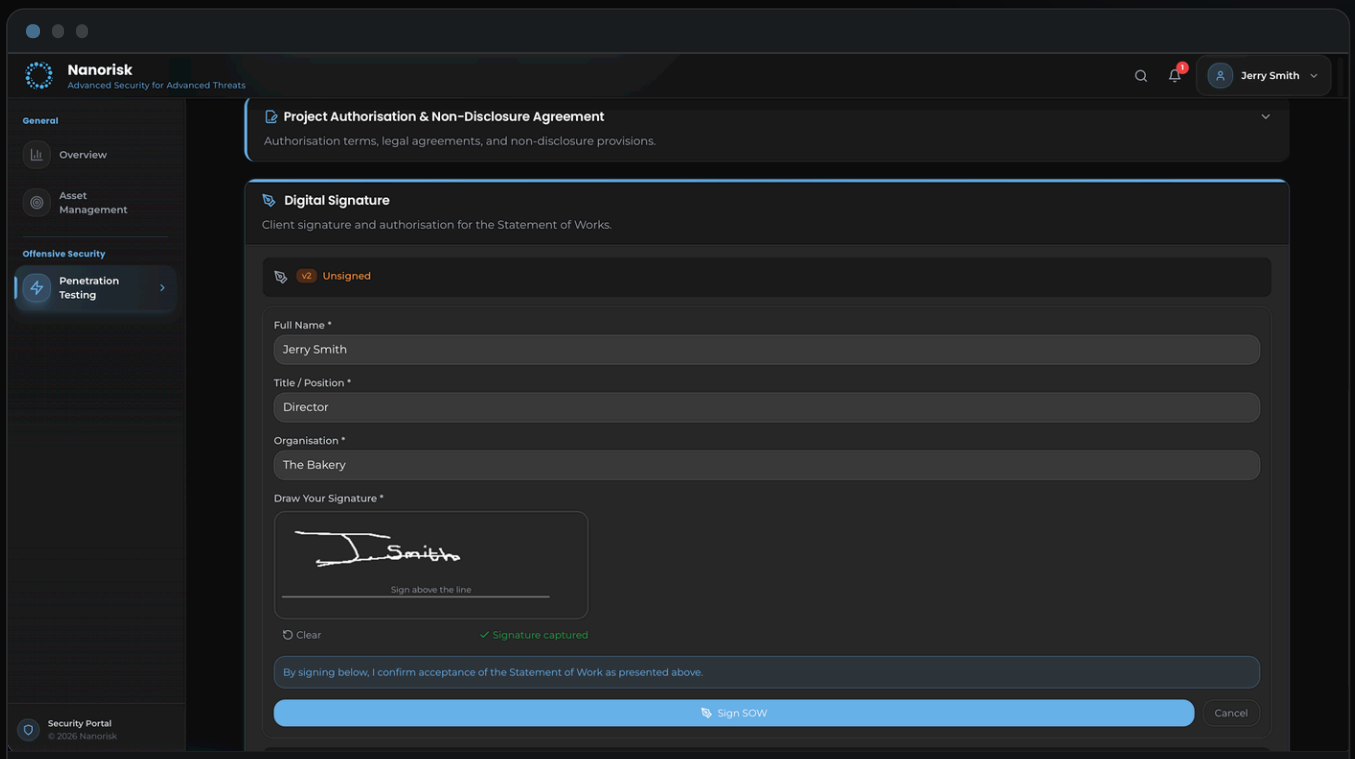


Engagement roadmap

Each phase tracked and timestamped, so you can see what stage you are at and what is next.

Authorisation & Documentation

The authorisation form and quote are provided both on the portal and as a downloadable document. All signing is completed digitally via the portal unless otherwise requested, no printing, scanning, or emailing sensitive contracts.

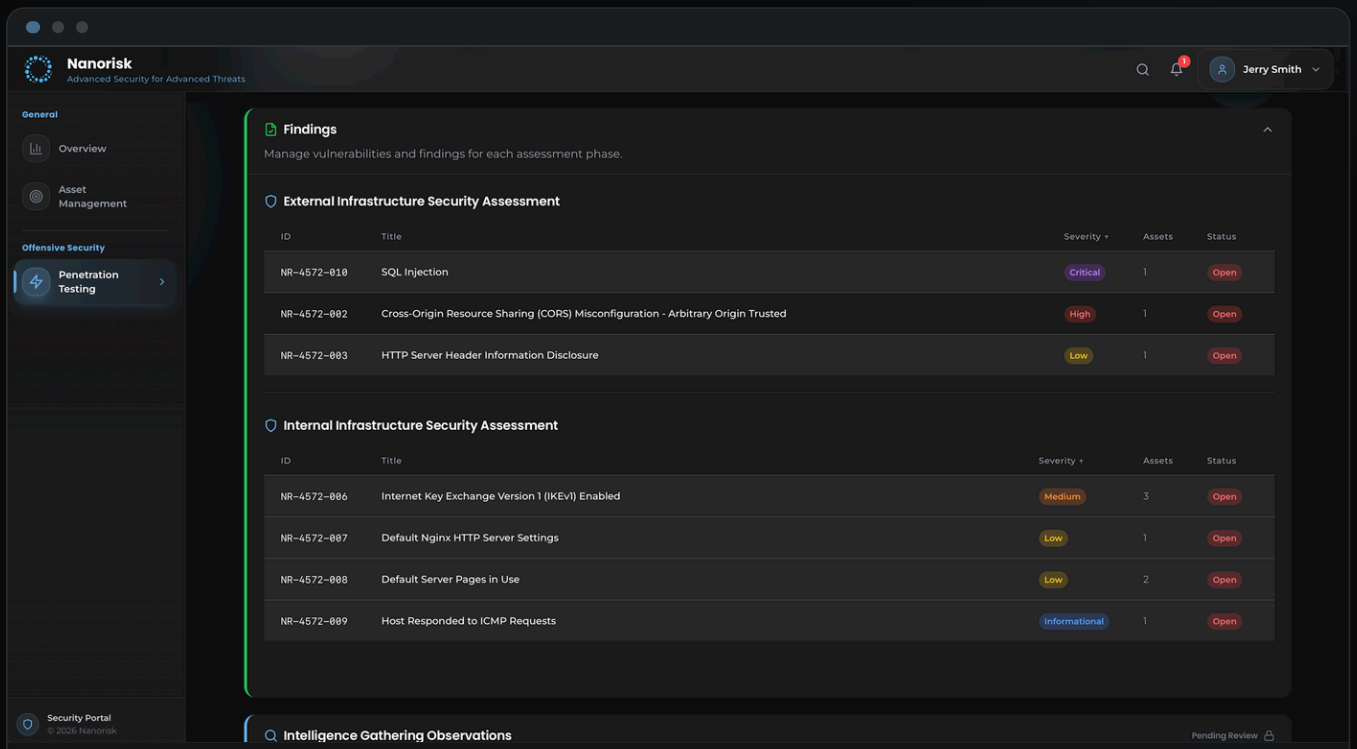


Digital signing, secure documents

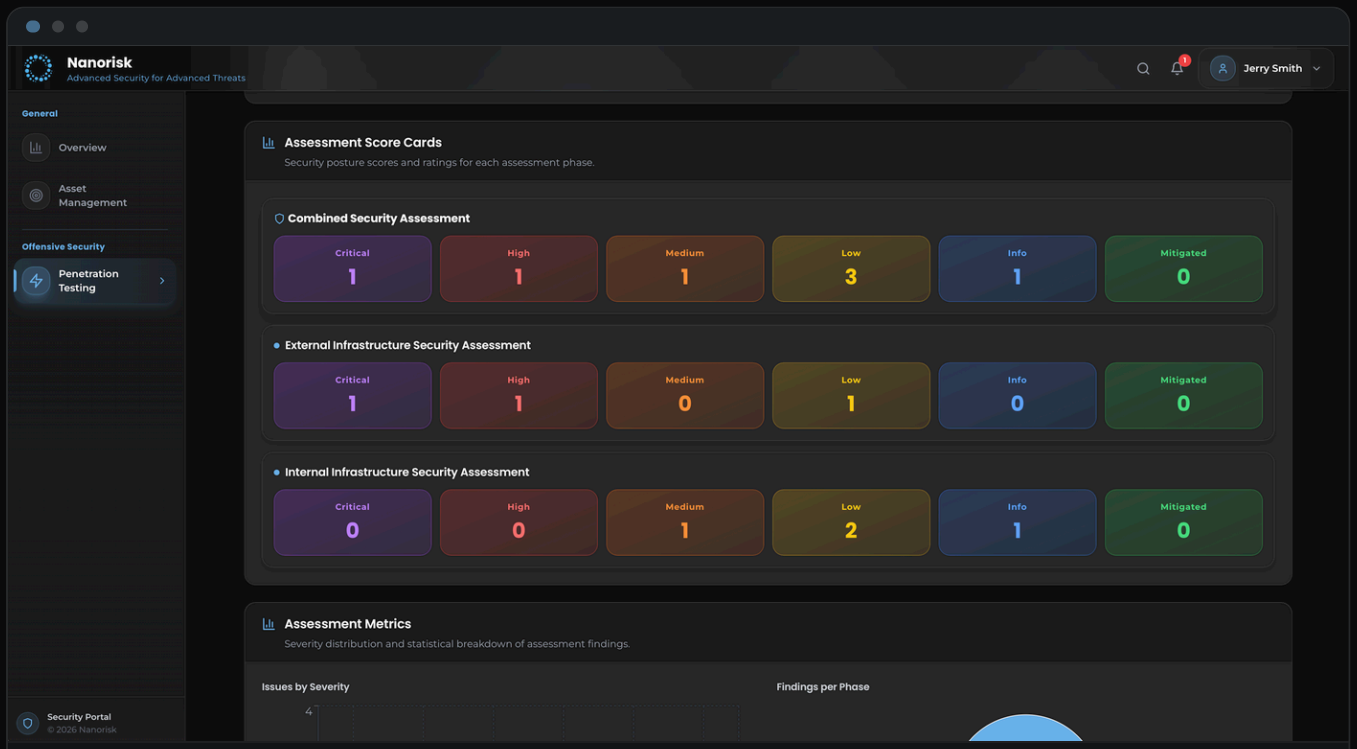
Statement of Works, quote and authorisation reviewed and signed digitally, with every version retained.

Findings & Remediation

All findings are viewable in real time on the portal. Each finding includes severity classification, CVSS scoring, affected assets, evidence, remediation guidance, and effort estimation.



Track every finding, manage every fix

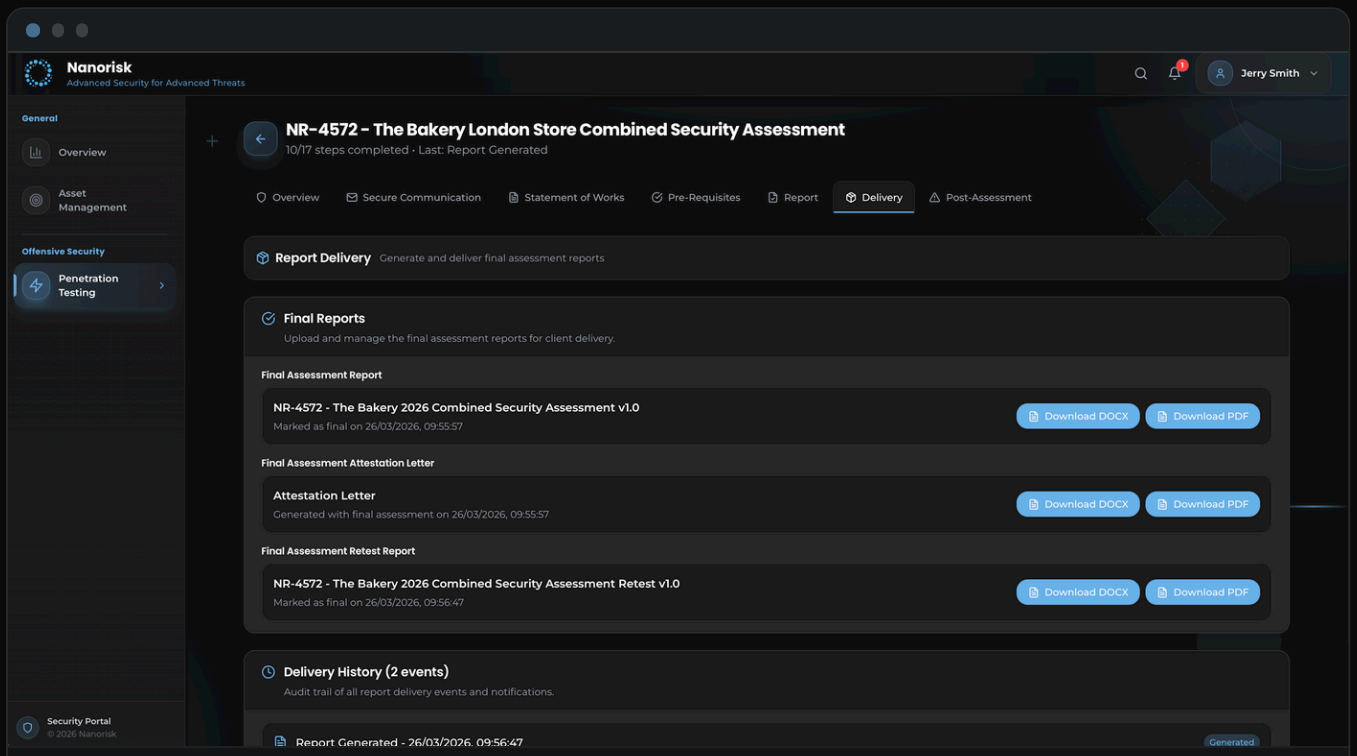


Security scoring

Reporting & Delivery

All reporting is viewable directly within the portal, with the option to download as PDF or Word. The same applies for retesting reports. We also provide formal attestation letters for every assessment, available in both PDF and Word formats.

- **Assessment reports**: executive summary, technical findings with evidence, CVSS scores, remediation guidance, and threat intelligence
- **Retesting reports**: following remediation, retesting validates that fixes are effective, delivered as a separate report
- **Attestation letters**: provided for every assessment as PDF or Word, supporting your compliance and governance requirements



Reports, retesting and attestation
Issued securely through the portal, with full version history.

Built for security professionals

The portal is designed with the same rigour applied to the assessments delivered through it.

01

Two-Factor Authentication

All accounts support TOTP-based 2FA with backup codes. Session management lets you view active sessions and terminate access from any device.

02

Role-Based Access

Granular access controls ensure each user sees only what they are authorised to see. Per-project permissions control access to sensitive documents.

03

Audit Trail

Comprehensive activity logging of all portal interactions supporting accountability, oversight, and compliance requirements.

04

Encrypted Communication

All sensitive information exchange happens through encrypted channels within the portal, never over email.

05

Controlled Documents

Secure storage and lifecycle management of all engagement documentation, NDAs, and artefacts with retention policy enforcement.

06

Session Security

View login history, active sessions with IP and device information, and terminate sessions remotely. Password strength enforcement and change tracking.

Portal access is governed by the Nanorisk Security Portal Terms of Use. Access is provisioned per engagement and controlled through role-based permissions.

Trusted by Organisations Across the Globe

Client feedback from recent engagements.

> Nanorisk penetration testers provide a personal level of service. Their team are quick to respond to queries. If there is an issue, they are always quick to work with us to find a quick resolution. They are accommodating to ensure our needs are met whether that's related to scheduling or to providing fast follow up to queries. On a technical level Nanorisk's team always demonstrate a strong level of technical knowledge, often finding vulnerabilities not found through other penetration tests. However, the team know how to break complex technical detail into higher level executive summaries that can be understood by management/C-Suite executives, something that has been valued by our clients.

Matthew Barrett Technical Project Lead, Kindus

> Ben was fantastic from the initial conversation through to completion. We received a comprehensive report outlining all issues found with clear suggested resolutions. Highly professional service throughout.

James Scott Systems & Network Ops Manager, TripIQ

> Competent scoping with minimal disruption to business operations. The high standard report with actionable steps and post-assessment discussion assisted with our risk management process.

Rory Carlton Head of Projects, Loan Market Association

SELECTED CLIENTS

GOV.UK Kindus CHIPSIDE part of the unity5 group OpenGenius LMA Loan Market Association TRIPIQ KAI

OUR SERVICES

43 assessment services, six families.

From a single vulnerability scan to full-scope adversary simulation.
Every service is described in full over the pages that follow.

2
ASSESSMENTS

Vulnerability Assessments

Point-in-time and ongoing identification of known technical weaknesses across agreed in-scope systems, reported through the Portal and tracked to closure.

20
ASSESSMENTS

Penetration Testing: Infrastructure

Assessment of networks, systems, devices and the services that support them, from the perimeter through to the internal estate.

8
ASSESSMENTS

Penetration Testing: Application

Assessment of applications across web, mobile, desktop and service-based architectures, including the code behind them.

4
ASSESSMENTS

Penetration Testing: Social Engineering

Controlled assessment of how an organisation's people and physical controls stand up to targeted manipulation.

6
ASSESSMENTS

Specialised Services

Adversary-focused and sector-specific assessments requiring detailed scoping and tightly controlled delivery.

3
ASSESSMENTS

Cyber Essentials

Assessment and preparation supporting Cyber Essentials and Cyber Essentials Plus certification, delivered via an accredited partner.

01

SERVICE FAMILY

Vulnerability Assessments

Point-in-time and ongoing identification of known technical weaknesses across agreed in-scope systems, reported through the Portal and tracked to closure.

2 ASSESSMENTS IN THIS FAMILY

- Vulnerability Scanning
- Vulnerability Management

VULNERABILITY ASSESSMENTS

Vulnerability Scanning

> Vulnerability Scanning provides a point-in-time assessment of technical vulnerabilities across agreed in-scope systems. The service is intended to help organisations establish a baseline understanding of exposure, validate security controls, or support specific assurance activities where ongoing scanning is not required.

How the Service Is Delivered

Vulnerability Scanning is delivered as a one-off engagement, formally scoped and authorised prior to execution. Scanning activity is strictly limited to the systems and environments defined in the agreed scope.

Assessments are conducted using industry-recognised vulnerability scanning technology, supported by appropriate configuration, validation, and review of results.

REPORTING AND RESULTS

Results are made available through the Nanorisk Security Portal, providing clients with secure access to identified vulnerabilities, supporting detail, and remediation guidance.

VULNERABILITY ASSESSMENTS

Vulnerability Management

> Vulnerability Management provides scheduled vulnerability scanning combined with lifecycle tracking, enabling organisations to maintain ongoing visibility of technical risk over time. The service is delivered on a subscription basis and is designed to support structured remediation and risk management rather than isolated, ad-hoc scanning.

How the Service Is Delivered

Vulnerability Management engagements are delivered through the Nanorisk Security Portal, which acts as the central platform for scan scheduling, asset management, and vulnerability tracking.

Scan frequency is agreed during scoping and may be configured on a monthly, fortnightly, weekly, or daily basis, depending on the client's environment and risk profile. All scanning activity is conducted strictly within an agreed and authorised asset scope.

Asset Bands

Asset bands define the number of in-scope assets covered by the subscription. The applicable band is agreed during scoping and confirmed in the Statement of Works.

02

SERVICE FAMILY

Penetration Testing: Infrastructure

Assessment of networks, systems, devices and the services that support them, from the perimeter through to the internal estate.

20 ASSESSMENTS IN THIS FAMILY

- Open-Source Intelligence (OSINT) Security Assessment
- External Infrastructure Security Assessment
- Internal Infrastructure Security Assessment
- Network Segmentation Security Assessment
- Network Device Configuration Security Assessment
- Environment Breakout Security Assessment
- Operating System Build Review Security Assessment
- Web Server Configuration Security Assessment
- Active Directory Configuration Review Security Assessment
- Cloud Environment Security Assessment
- Firewall Configuration Security Assessment
- VPN Configuration Review Security Assessment
- Voice Over IP (VoIP) Device Security Assessment
- Database Configuration Review Security Assessment
- Secure Network Development Security Assessment
- Stolen Device Security Assessment
- Mobile Device Configuration Security Assessment
- Mobile Device Management Security Assessment
- Wi-Fi Security Assessment
- Bluetooth Security Assessment

PENETRATION TESTING: INFRASTRUCTURE

Open-Source Intelligence (OSINT) Security Assessment

> The Open-Source Intelligence (OSINT) Security Assessment evaluates information about an organisation that is publicly accessible without requiring direct interaction with internal systems or networks.

The purpose of this assessment is to identify data points that may be leveraged by a threat actor during reconnaissance, social engineering, or the planning of more targeted attacks. By understanding what is visible externally, organisations can better manage their digital footprint and reduce unnecessary exposure.

Scope & Focus

The assessment may include, but is not limited to, the analysis of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Domain and subdomain discovery
- Public DNS and network information
- IP address attribution and hosting relationships
- Cloud asset identification
- Publicly exposed services and endpoints
- Metadata and configuration leakage
- Public code repositories and development artefacts
- References to breached or leaked data
- Public references to staff, roles, and organisational structure

Engagement & Delivery

The OSINT Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

This ensures that findings are both technically sound and operationally meaningful.

- automated discovery techniques for scale and coverage
- manual analysis for contextual accuracy and relevance

OUTPUTS & REPORTING

Clients receive:

Findings are prioritised to support informed decision-making and remediation planning.

- A dedicated OSINT Security Assessment report
- Identified exposures with contextual risk explanation
- Practical recommendations for reducing public-facing risk
- Secure access to findings via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment is **passive and non-intrusive**, involving no active exploitation or interaction with internal systems
- Findings reflect publicly available information at the time of testing and represent a point-in-time view of exposure
- The assessment does not guarantee identification of all public references or data sources

PENETRATION TESTING: INFRASTRUCTURE

External Infrastructure Security Assessment

> The External Infrastructure Security Assessment evaluates the security posture of an organisation's internet-facing systems and services.

The objective of this assessment is to identify vulnerabilities and weaknesses that could be exploited by external attackers without prior access to internal systems. It provides insight into how exposed the organisation is to real-world attack techniques originating from outside the network perimeter.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Public IP address ranges and externally accessible hosts
- Network services and exposed ports
- Internet-facing applications and management interfaces
- Perimeter security controls
- Authentication mechanisms and access controls
- Known vulnerabilities and misconfigurations
- Publicly exposed administrative services
- TLS/SSL configurations and certificate management

Engagement & Delivery

The External Infrastructure Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is performed in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- automated discovery for breadth and efficiency
- manual verification and exploitation for accuracy and realism

OUTPUTS & REPORTING

Clients receive:

Findings are structured to support both technical remediation and executive-level decision-making.

- A detailed External Infrastructure Security Assessment report
- Identified vulnerabilities with risk context and prioritisation
- Clear, actionable remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment is performed from an external attacker perspective and does not assume prior network access
- Findings reflect a point-in-time view of the environment during the assessment period
- The assessment does not guarantee identification of all vulnerabilities or attack paths

PENETRATION TESTING: INFRASTRUCTURE

Internal Infrastructure Security Assessment

> The Internal Infrastructure Security Assessment evaluates the security of systems, services, and controls within an organisation's internal network environment.

The objective of this assessment is to identify vulnerabilities and weaknesses that could be exploited by an attacker who has gained an initial foothold within the network, whether through compromised credentials, a malicious insider, or a successful external breach.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Internal network hosts and services
- Privileged and non-privileged user access
- Authentication and authorisation mechanisms
- Lateral movement opportunities
- Privilege escalation paths
- Network trust relationships
- Security controls and monitoring effectiveness
- Internal service and system misconfigurations

Engagement & Delivery

The Internal Infrastructure Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- automated discovery to identify exposure and attack surface
- manual analysis and exploitation to validate real-world risk

OUTPUTS & REPORTING

Clients receive:

Findings support both tactical remediation and strategic improvement of internal security posture.

- A detailed Internal Infrastructure Security Assessment report
- Identified vulnerabilities with risk context and prioritisation
- Clear, actionable remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment assumes some level of internal access and does not represent a perimeter-only security view
- Findings reflect a point-in-time view of the environment during the assessment period
- The assessment does not guarantee identification of all vulnerabilities or attack paths

PENETRATION TESTING: INFRASTRUCTURE

Network Segmentation Security Assessment

> The Network Segmentation Security Assessment evaluates the effectiveness of network segmentation controls within an organisation's environment.

The objective of this assessment is to determine whether systems, users, and data are appropriately separated to reduce attack surface, limit lateral movement, and contain the impact of a security breach.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Network zones, VLANs, and security boundaries
- Access control lists and routing policies
- Inter-segment trust relationships
- Segmentation enforcement mechanisms
- East-west traffic controls
- Privileged access pathways between segments
- Effectiveness of isolation between critical systems
- Design alignment with security and business requirements

Engagement & Delivery

The Network Segmentation Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- architectural review to understand segmentation design
- validation testing to assess enforcement and bypass potential

OUTPUTS & REPORTING

Clients receive:

Findings support improvements in both security architecture and operational resilience.

- A Network Segmentation Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to improve segmentation and containment
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on containment and control effectiveness rather than vulnerability discovery alone
- Findings reflect a point-in-time view of the environment during the assessment period
- The assessment does not guarantee identification of all segmentation weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Network Device Configuration Security Assessment

> The Network Device Configuration Security Assessment evaluates the security posture of network devices through the review of their configurations and operational controls.

The objective of this assessment is to identify misconfigurations, insecure settings, and deviations from security best practice that could expose the organisation to compromise or operational risk.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Routers, switches, and network appliances
- Device hardening and baseline compliance
- Management plane security
- Authentication and access controls
- Logging and monitoring configurations
- Network protocols and services
- Firmware versions and patch levels
- Resilience and failover configurations

Engagement & Delivery

The Network Device Configuration Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration review against recognised security benchmarks
- validation testing to confirm control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved security, stability, and operational resilience.

- A Network Device Configuration Security Assessment report
- Identified configuration weaknesses with contextual risk explanation
- Prioritised recommendations aligned with security best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on configuration and control effectiveness rather than active exploitation
- Findings reflect a point-in-time view of device configurations during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Environment Breakout Security Assessment

> The Environment Breakout Security Assessment evaluates the effectiveness of containment mechanisms designed to isolate systems, applications, or users within restricted environments.

The objective of this assessment is to determine whether it is possible to escape from constrained execution contexts and gain unauthorised access to broader systems, networks, or privileges.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Virtual machines and hypervisor isolation
- Containers and sandboxed environments
- Application-level isolation controls
- Privilege boundaries within restricted environments
- Inter-environment trust relationships
- Misconfigurations enabling escape or privilege escalation
- Host and orchestration security controls

Engagement & Delivery

The Environment Breakout Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- architectural and configuration review
- controlled testing to validate containment effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improvements in system design and security architecture.

- An Environment Breakout Security Assessment report
- Identified weaknesses in containment mechanisms with risk context
- Recommendations to strengthen isolation and boundary enforcement
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on isolation and containment rather than general vulnerability discovery
- Findings reflect a point-in-time view of the environment during the assessment period
- The assessment does not guarantee identification of all potential breakout paths

PENETRATION TESTING: INFRASTRUCTURE

Operating System Build Review Security Assessment

> The Operating System Build Review Security Assessment evaluates the security posture of operating system builds against recognised security best practice and hardening standards.

The objective of this assessment is to identify insecure configurations, unnecessary services, and deviations from baseline controls that could increase the risk of compromise or operational instability.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Operating system configuration baselines
- User and privilege management
- Service and process hardening
- Patch and update management
- Logging and monitoring settings
- Authentication and access controls
- Default configurations and inherited weaknesses
- Alignment with recognised hardening guidelines

Engagement & Delivery

The Operating System Build Review Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration and baseline review
- validation testing to assess control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved system resilience and security consistency across environments.

- An Operating System Build Review Security Assessment report
- Identified configuration weaknesses with contextual risk explanation
- Prioritised recommendations aligned with security hardening best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on configuration and build integrity rather than active exploitation
- Findings reflect a point-in-time view of system builds during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Web Server Configuration Security Assessment

> The Web Server Configuration Security Assessment evaluates the security posture of web server platforms through the review of their configuration and operational controls.

The objective of this assessment is to identify misconfigurations, insecure defaults, and deviations from security best practice that could expose hosted applications or data to compromise.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Web server software configuration and hardening
- Enabled modules and services
- TLS/SSL configuration and certificate handling
- Authentication and access controls
- Directory and file permissions
- Logging and monitoring settings
- Default configurations and inherited weaknesses
- Alignment with recognised security benchmarks

Engagement & Delivery

The Web Server Configuration Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration review against security best practice
- validation testing to assess control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved security, reliability, and consistency across web hosting environments.

- A Web Server Configuration Security Assessment report
- Identified configuration weaknesses with contextual risk explanation
- Prioritised recommendations aligned with security hardening best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on configuration and platform security rather than application logic
- Findings reflect a point-in-time view of server configurations during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Active Directory Configuration Review Security Assessment

> The Active Directory Configuration Review Security Assessment evaluates the security posture of an organisation's Active Directory environment through the review of its configuration, permissions, and operational controls.

The objective of this assessment is to identify weaknesses that could enable unauthorised access, privilege escalation, or compromise of identity and access management controls.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Domain and forest configuration
- User, group, and service account permissions
- Privileged access controls
- Group Policy configuration
- Authentication and authorisation mechanisms
- Trust relationships and delegation settings
- Replication and directory services security
- Alignment with recognised security best practice

Engagement & Delivery

The Active Directory Configuration Review Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration and permissions review
- validation testing to assess control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved identity security and reduction of systemic privilege-related risk.

- An Active Directory Configuration Review Security Assessment report
- Identified weaknesses with contextual risk explanation
- Prioritised recommendations aligned with security best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on identity and access control integrity rather than general vulnerability scanning
- Findings reflect a point-in-time view of directory configuration during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Cloud Environment Security Assessment

> The Cloud Environment Security Assessment evaluates the security posture of cloud-hosted infrastructure and services across public, private, or hybrid cloud environments.

The objective of this assessment is to identify configuration weaknesses, insecure deployments, and control gaps that could expose cloud resources, data, or services to compromise.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Cloud account and tenancy configuration
- Identity and access management controls
- Network security and segmentation within the cloud environment
- Storage and data protection mechanisms
- Virtual machine and platform security settings
- Logging, monitoring, and alerting configurations
- Exposure of cloud services to the public internet
- Alignment with recognised cloud security best practice

Engagement & Delivery

The Cloud Environment Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- architectural and configuration review
- validation testing to assess control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved visibility, control, and resilience across cloud environments.

- A Cloud Environment Security Assessment report
- Identified security weaknesses with contextual risk explanation
- Prioritised recommendations aligned with cloud security best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on configuration and control effectiveness rather than application-level testing
- Findings reflect a point-in-time view of the cloud environment during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Firewall Configuration Security Assessment

> The Firewall Configuration Security Assessment evaluates the security and effectiveness of firewall rules, policies, and associated controls within an organisation's environment.

The objective of this assessment is to identify misconfigurations, overly permissive rules, and control weaknesses that could expose systems or data to unauthorised access.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Firewall rule sets and security policies
- Network access control enforcement
- Ingress and egress filtering controls
- Management plane security
- Logging and monitoring configuration
- Change control and rule lifecycle management
- Alignment with network security architecture
- Compliance with security best practice

Engagement & Delivery

The Firewall Configuration Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration and policy review
- validation testing to assess enforcement effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved perimeter control and reduced exposure to network-based threats.

- A Firewall Configuration Security Assessment report
- Identified weaknesses with contextual risk explanation
- Prioritised recommendations aligned with security best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on policy and control effectiveness rather than device exploitation
- Findings reflect a point-in-time view of firewall configuration during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

VPN Configuration Review Security Assessment

> The VPN Configuration Review Security Assessment evaluates the security posture of Virtual Private Network (VPN) implementations used to provide remote or site-to-site connectivity.

The objective of this assessment is to identify misconfigurations, weak controls, and design weaknesses that could compromise secure remote access or network segmentation.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- VPN architecture and deployment design
- Authentication and access control mechanisms
- Encryption protocols and key management
- User and device access policies
- Management and administrative access controls
- Logging and monitoring configuration
- Integration with identity and security systems
- Alignment with recognised security best practice

Engagement & Delivery

The VPN Configuration Review Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration and design review
- validation testing to assess control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved remote access security and reduced risk of unauthorised network access.

- A VPN Configuration Review Security Assessment report
- Identified weaknesses with contextual risk explanation
- Prioritised recommendations aligned with security best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on configuration and control effectiveness rather than exploitation of endpoints
- Findings reflect a point-in-time view of VPN configuration during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Voice Over IP (VoIP) Device Security Assessment

> The Voice Over IP (VoIP) Device Security Assessment evaluates the security posture of VoIP systems and associated devices within an organisation's communications environment.

The objective of this assessment is to identify vulnerabilities, misconfigurations, and control weaknesses that could enable unauthorised access, service disruption, or interception of voice communications.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- VoIP endpoints and hardware devices
- Call management and signalling infrastructure
- Authentication and access control mechanisms
- Network exposure and segmentation controls
- Encryption of voice and signalling traffic
- Management interfaces and administrative access
- Firmware versions and patch levels
- Alignment with recognised VoIP security best practice

Engagement & Delivery

The VoIP Device Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration and architecture review
- validation testing to assess control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved reliability and security of voice communications.

- A VoIP Device Security Assessment report
- Identified weaknesses with contextual risk explanation
- Prioritised recommendations aligned with security best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on device and infrastructure security rather than call content analysis
- Findings reflect a point-in-time view of the VoIP environment during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Database Configuration Review Security Assessment

> The Database Configuration Review Security Assessment evaluates the security posture of database platforms through the review of configuration, access controls, and operational settings.

The objective of this assessment is to identify misconfigurations, weak controls, and deviations from security best practice that could expose sensitive data or enable unauthorised access.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Database platform configuration and hardening
- Authentication and access control mechanisms
- Privileged user and service account permissions
- Encryption and data protection controls
- Logging, auditing, and monitoring configuration
- Patch and update management
- Default configurations and inherited weaknesses
- Alignment with recognised database security best practice

Engagement & Delivery

The Database Configuration Review Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration review against security best practice
- validation testing to assess control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved protection of sensitive data and system resilience.

- A Database Configuration Review Security Assessment report
- Identified weaknesses with contextual risk explanation
- Prioritised recommendations aligned with security best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on configuration and access controls rather than application-layer testing
- Findings reflect a point-in-time view of database configuration during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Secure Network Development Security Assessment

> The Secure Network Development Security Assessment evaluates the security considerations embedded within the design and implementation of network environments.

The objective of this assessment is to identify weaknesses in network architecture, development practices, and design decisions that could introduce systemic security risks or operational vulnerabilities.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Network architecture and design documentation
- Security requirements and design controls
- Segmentation and trust boundary definition
- Secure configuration standards and baselines
- Integration of security within network development processes
- Change management and design governance
- Alignment with security and business requirements
- Adherence to recognised secure network design principles

Engagement & Delivery

The Secure Network Development Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- design and documentation review
- validation testing to assess control implementation

OUTPUTS & REPORTING

Clients receive:

Findings support long-term improvements in security architecture and resilience.

- A Secure Network Development Security Assessment report
- Identified design weaknesses with contextual risk explanation
- Practical recommendations to strengthen network security by design
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on security by design rather than operational vulnerabilities alone
- Findings reflect a point-in-time view of network design and development practices
- The assessment does not guarantee identification of all architectural weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Stolen Device Security Assessment

> The Stolen Device Security Assessment evaluates the security controls and operational readiness of an organisation in the event of a device being lost or stolen.

The objective of this assessment is to determine whether appropriate safeguards are in place to protect data, credentials, and systems from compromise following the loss or theft of a device.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Device encryption and data protection controls
- Authentication mechanisms and access restrictions
- Remote wipe and device management capabilities
- Local data storage and caching behaviour
- Credential storage and session handling
- Incident response procedures related to lost devices
- User awareness and reporting processes
- Alignment with recognised mobile and endpoint security best practice

Engagement & Delivery

The Stolen Device Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration and control review
- validation testing to assess protection effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved resilience against endpoint loss and unauthorised access.

- A Stolen Device Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to reduce risk associated with lost or stolen devices
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on control effectiveness rather than simulated theft scenarios
- Findings reflect a point-in-time view of endpoint protection and response capabilities
- The assessment does not guarantee identification of all control weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Mobile Device Configuration Security Assessment

> The Mobile Device Configuration Security Assessment evaluates the security posture of mobile devices through the review of their configuration and applied security controls.

The objective of this assessment is to identify misconfigurations, weak controls, and deviations from security best practice that could expose organisational data or systems via mobile endpoints.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Device security configuration and hardening
- Authentication and access control mechanisms
- Data encryption and protection settings
- Application permissions and restrictions
- Operating system patch levels and update management
- Local data storage and backup controls
- Integration with enterprise security systems
- Alignment with recognised mobile security best practice

Engagement & Delivery

The Mobile Device Configuration Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration review against security best practice
- validation testing to assess control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved security and management of mobile endpoints.

- A Mobile Device Configuration Security Assessment report
- Identified weaknesses with contextual risk explanation
- Prioritised recommendations aligned with mobile security best practice
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on configuration and control effectiveness rather than application testing
- Findings reflect a point-in-time view of mobile device configuration during the assessment period
- The assessment does not guarantee identification of all configuration weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Mobile Device Management Security Assessment

> The Mobile Device Management (MDM) Security Assessment evaluates the security posture and effectiveness of an organisation's MDM solution and associated controls.

The objective of this assessment is to identify weaknesses in policy enforcement, device governance, and management controls that could undermine the security of mobile endpoints and organisational data.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- MDM platform configuration and security settings
- Policy enforcement mechanisms
- Device enrollment and deprovisioning processes
- Authentication and administrative access controls
- Compliance and monitoring capabilities
- Integration with identity and security systems
- Incident response and device lifecycle management
- Alignment with recognised mobile management best practice

Engagement & Delivery

The Mobile Device Management Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in a controlled manner, aligned with agreed rules of engagement and designed to minimise operational impact.

- configuration and policy review
- validation testing to assess control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved control, visibility, and security of mobile environments.

- A Mobile Device Management Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to improve mobile governance and security
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on management and governance controls rather than individual device vulnerabilities
- Findings reflect a point-in-time view of the MDM environment during the assessment period
- The assessment does not guarantee identification of all control weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Wi-Fi Security Assessment

> The Wi-Fi Security Assessment evaluates the security posture of an organisation's wireless network infrastructure and associated access controls.

The objective of this assessment is to identify vulnerabilities, misconfigurations, and weaknesses that could enable unauthorised access to internal networks or compromise the confidentiality and integrity of wireless communications.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Wireless network architecture and design
- Authentication and access control mechanisms
- Encryption and key management practices
- Segmentation between wireless and wired networks
- Guest network controls
- Rogue access point detection
- Wireless management interfaces
- Alignment with recognised wireless security best practice

Engagement & Delivery

The Wi-Fi Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- configuration and architectural review
- controlled testing to validate security controls

OUTPUTS & REPORTING

Clients receive:

Findings support improved protection of wireless access and network integrity.

- A Wi-Fi Security Assessment report
- Identified weaknesses with contextual risk explanation
- Prioritised recommendations to improve wireless security
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on wireless infrastructure security rather than endpoint device security
- Findings reflect a point-in-time view of the wireless environment during the assessment period
- The assessment does not guarantee identification of all wireless security weaknesses

PENETRATION TESTING: INFRASTRUCTURE

Bluetooth Security Assessment

> The Bluetooth Security Assessment evaluates the security posture of Bluetooth-enabled devices and their associated communication mechanisms within an organisation's environment.

The objective of this assessment is to identify vulnerabilities, misconfigurations, and weaknesses that could enable unauthorised access, data leakage, or compromise through Bluetooth communications.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Bluetooth-enabled devices and peripherals
- Pairing and authentication mechanisms
- Encryption and communication security
- Device discoverability and visibility settings
- Firmware versions and patch levels
- Integration with enterprise security controls
- Exposure to known Bluetooth attack techniques
- Alignment with recognised Bluetooth security best practice

Engagement & Delivery

The Bluetooth Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- configuration and device review
- controlled testing to assess communication security

OUTPUTS & REPORTING

Clients receive:

Findings support improved control and reduced risk associated with short-range wireless communications.

- A Bluetooth Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to improve Bluetooth security
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on Bluetooth communications rather than general wireless network security
- Findings reflect a point-in-time view of Bluetooth security during the assessment period
- The assessment does not guarantee identification of all Bluetooth-related weaknesses

03

SERVICE FAMILY

Penetration Testing: Application

Assessment of applications across web, mobile, desktop and service-based architectures, including the code behind them.

8 ASSESSMENTS IN THIS FAMILY

- Web Application Security Assessment
- Web Service / API Security Assessment
- Android Application Security Assessment
- iOS Application Security Assessment
- Windows Desktop Application Security Assessment
- Thick Client Security Assessment
- Binary Exploitation Security Assessment
- Code Review Security Assessment

PENETRATION TESTING: APPLICATION

Web Application Security Assessment

> The Web Application Security Assessment evaluates the security posture of web-based applications and the logic, controls, and data flows that underpin them.

The objective of this assessment is to identify vulnerabilities and weaknesses that could be exploited to compromise application functionality, data confidentiality, or service availability.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Application authentication and session management
- Authorisation and access control logic
- Input validation and data handling mechanisms
- Business logic and workflow controls
- Client-side and server-side security controls
- Application configuration and deployment settings
- Exposure to common web application attack techniques
- Alignment with recognised web security best practice

Engagement & Delivery

The Web Application Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- manual security testing for depth and accuracy
- automated techniques for coverage and efficiency

OUTPUTS & REPORTING

Clients receive:

Findings support both immediate remediation and longer-term improvements in application security maturity.

- A Web Application Security Assessment report
- Identified vulnerabilities with contextual risk explanation
- Prioritised remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on application logic and security controls rather than infrastructure alone
- Findings reflect a point-in-time view of the application during the assessment period
- The assessment does not guarantee identification of all application vulnerabilities

PENETRATION TESTING: APPLICATION

Web Service / API Security Assessment

> The Web Service / API Security Assessment evaluates the security posture of application programming interfaces (APIs) and web services that enable system-to-system and client-to-server interactions.

The objective of this assessment is to identify vulnerabilities and weaknesses that could be exploited to compromise data integrity, confidentiality, or service availability through API endpoints.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Authentication and authorisation mechanisms
- Token handling and session management
- Input validation and data processing logic
- Rate limiting and abuse prevention controls
- Error handling and information exposure
- API configuration and deployment settings
- Exposure to common API attack techniques
- Alignment with recognised API security best practice

Engagement & Delivery

The Web Service / API Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- manual security testing for accuracy and context
- automated techniques for coverage and efficiency

OUTPUTS & REPORTING

Clients receive:

Findings support improved resilience and trust in application integrations and services.

- A Web Service / API Security Assessment report
- Identified vulnerabilities with contextual risk explanation
- Prioritised remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on API logic and security controls rather than underlying infrastructure alone
- Findings reflect a point-in-time view of API security during the assessment period
- The assessment does not guarantee identification of all API vulnerabilities

PENETRATION TESTING: APPLICATION

Android Application Security Assessment

> The Android Application Security Assessment evaluates the security posture of applications developed for the Android platform, including their code, logic, and interaction with underlying systems and services.

The objective of this assessment is to identify vulnerabilities and weaknesses that could be exploited to compromise application integrity, data confidentiality, or user trust.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Application authentication and session handling
- Data storage and encryption mechanisms
- Inter-process communication and permissions
- Input validation and business logic controls
- Secure use of platform APIs and libraries
- Network communication security
- Protection against common mobile attack techniques
- Alignment with recognised Android security best practice

Engagement & Delivery

The Android Application Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- static and dynamic analysis techniques
- manual testing to validate real-world exploitability

OUTPUTS & REPORTING

Clients receive:

Findings support improved security and resilience of Android mobile applications.

- An Android Application Security Assessment report
- Identified vulnerabilities with contextual risk explanation
- Prioritised remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on application security rather than device configuration
- Findings reflect a point-in-time view of the application during the assessment period
- The assessment does not guarantee identification of all application vulnerabilities

PENETRATION TESTING: APPLICATION

iOS Application Security Assessment

> The iOS Application Security Assessment evaluates the security posture of applications developed for the iOS platform, including their code, logic, and interaction with underlying systems and services.

The objective of this assessment is to identify vulnerabilities and weaknesses that could be exploited to compromise application integrity, data confidentiality, or user trust.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Application authentication and session handling
- Data storage and encryption mechanisms
- Secure use of iOS platform APIs and frameworks
- Inter-process communication and entitlements
- Input validation and business logic controls
- Network communication security
- Protection against common mobile attack techniques
- Alignment with recognised iOS security best practice

Engagement & Delivery

The iOS Application Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- static and dynamic analysis techniques
- manual testing to validate real-world exploitability

OUTPUTS & REPORTING

Clients receive:

Findings support improved security and resilience of iOS mobile applications.

- An iOS Application Security Assessment report
- Identified vulnerabilities with contextual risk explanation
- Prioritised remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on application security rather than device configuration
- Findings reflect a point-in-time view of the application during the assessment period
- The assessment does not guarantee identification of all application vulnerabilities

PENETRATION TESTING: APPLICATION

Windows Desktop Application Security Assessment

> The Windows Desktop Application Security Assessment evaluates the security posture of applications developed for the Windows desktop environment, including their code, execution context, and interaction with the operating system.

The objective of this assessment is to identify vulnerabilities and weaknesses that could be exploited to compromise system integrity, application functionality, or sensitive data.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Application authentication and authorisation mechanisms
- Privilege usage and execution context
- Secure handling of sensitive data and credentials
- Inter-process communication and resource access
- Input validation and business logic controls
- Secure use of Windows APIs and libraries
- Protection against common desktop attack techniques
- Alignment with recognised desktop application security best practice

Engagement & Delivery

The Windows Desktop Application Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- static and dynamic analysis techniques
- manual testing to validate real-world exploitability

OUTPUTS & REPORTING

Clients receive:

Findings support improved security and resilience of desktop applications.

- A Windows Desktop Application Security Assessment report
- Identified vulnerabilities with contextual risk explanation
- Prioritised remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on application security rather than underlying operating system configuration
- Findings reflect a point-in-time view of the application during the assessment period
- The assessment does not guarantee identification of all application vulnerabilities

PENETRATION TESTING: APPLICATION

Thick Client Security Assessment

> The Thick Client Security Assessment evaluates the security posture of client-side applications that operate with significant local processing and system interaction.

The objective of this assessment is to identify vulnerabilities and weaknesses that could be exploited to compromise application integrity, local systems, or backend services.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Application authentication and session handling
- Local data storage and encryption mechanisms
- Interactions with backend services and APIs
- Privilege usage and execution context
- Input validation and business logic controls
- Secure use of local system resources
- Protection against common client-side attack techniques
- Alignment with recognised thick client security best practice

Engagement & Delivery

The Thick Client Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- static and dynamic analysis techniques
- manual testing to validate real-world exploitability

OUTPUTS & REPORTING

Clients receive:

Findings support improved security of client-side applications and their supporting services.

- A Thick Client Security Assessment report
- Identified vulnerabilities with contextual risk explanation
- Prioritised remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on client-side application security rather than server-side infrastructure
- Findings reflect a point-in-time view of the application during the assessment period
- The assessment does not guarantee identification of all application vulnerabilities

PENETRATION TESTING: APPLICATION

Binary Exploitation Security Assessment

> The Binary Exploitation Security Assessment evaluates the security posture of compiled binaries and executable components to identify weaknesses that could be exploited at the machine-code or memory level.

The objective of this assessment is to uncover vulnerabilities that may not be visible through higher-level application testing, including those affecting system stability, confidentiality, or control flow integrity.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Memory management and handling of input data
- Use of unsafe functions and insecure coding patterns
- Buffer handling and bounds checking
- Control flow integrity and exception handling
- Binary protections and exploit mitigation mechanisms
- Privilege boundaries and execution context
- Exposure to known binary-level attack techniques
- Alignment with recognised secure development and exploitation mitigation best practice

Engagement & Delivery

The Binary Exploitation Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All testing is conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- static and dynamic binary analysis
- controlled exploitation techniques to validate real-world risk

OUTPUTS & REPORTING

Clients receive:

Findings support improved resilience against low-level and advanced attack techniques.

- A Binary Exploitation Security Assessment report
- Identified vulnerabilities with contextual risk explanation
- Prioritised remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on binary-level security rather than source code quality alone
- Findings reflect a point-in-time view of the assessed components during the assessment period
- The assessment does not guarantee identification of all binary-level vulnerabilities

PENETRATION TESTING: APPLICATION

Code Review Security Assessment

> The Code Review Security Assessment evaluates the security posture of application source code through systematic analysis of implementation and design choices.

The objective of this assessment is to identify vulnerabilities, insecure coding practices, and logic flaws that could introduce security weaknesses into applications or systems.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Input validation and data handling logic
- Authentication and authorisation implementation
- Error handling and logging practices
- Use of cryptographic functions and key management
- Secure handling of credentials and secrets
- Business logic and workflow controls
- Compliance with secure coding standards
- Alignment with recognised secure development best practice

Engagement & Delivery

The Code Review Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- manual source code review for depth and accuracy
- supporting automated analysis where appropriate

OUTPUTS & REPORTING

Clients receive:

Findings support improved software quality and security by design.

- A Code Review Security Assessment report
- Identified vulnerabilities with contextual risk explanation
- Prioritised remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on source code and logic rather than deployed runtime behaviour alone
- Findings reflect a point-in-time view of the codebase during the assessment period
- The assessment does not guarantee identification of all security issues within the code

04

SERVICE FAMILY

Penetration Testing: Social Engineering

Controlled assessment of how an organisation's people and physical controls stand up to targeted manipulation.

4 ASSESSMENTS IN THIS FAMILY

- Email Phishing Security Assessment
- Vishing (Telephone Phishing) Security Assessment
- Smishing (SMS Phishing) Security Assessment
- Physical Security Assessment

PENETRATION TESTING: SOCIAL ENGINEERING

Email Phishing Security Assessment

> The Email Phishing Security Assessment evaluates an organisation's exposure to phishing attacks delivered via email, focusing on both technical controls and user susceptibility.

The objective of this assessment is to identify weaknesses in email security controls and user awareness that could enable successful phishing-based compromise.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Email security gateway configuration and filtering controls
- Authentication mechanisms such as SPF, DKIM, and DMARC
- User awareness and response behaviours
- Reporting and incident handling processes
- Protection against common phishing and spoofing techniques
- Monitoring and alerting capabilities
- Integration with broader security operations
- Alignment with recognised email security best practice

Engagement & Delivery

The Email Phishing Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment may combine:

All activities are conducted in accordance with agreed rules of engagement and designed to minimise operational impact and user disruption.

- controlled phishing simulations
- configuration and control review

OUTPUTS & REPORTING

Clients receive:

Findings support improved resilience against email-based social engineering attacks.

- An Email Phishing Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to reduce phishing-related risk
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on preparedness and control effectiveness rather than blame or individual performance
- Findings reflect a point-in-time view of phishing resilience during the assessment period
- The assessment does not guarantee prevention of all phishing attacks

PENETRATION TESTING: SOCIAL ENGINEERING

Smishing (SMS Phishing) Security Assessment

> The Smishing (SMS Phishing) Security Assessment evaluates an organisation's exposure to phishing attacks delivered via SMS and mobile messaging platforms.

The objective of this assessment is to identify weaknesses in technical controls and user awareness that could enable successful smishing-based compromise.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- User awareness and response behaviours
- Reporting and incident handling processes
- Mobile messaging security controls
- Protection against spoofed or malicious messages
- Integration with mobile security and monitoring systems
- Detection and response capabilities
- Alignment with recognised mobile and messaging security best practice

Engagement & Delivery

The Smishing Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment may combine:

All activities are conducted in accordance with agreed rules of engagement and designed to minimise operational impact and user disruption.

- controlled smishing simulations
- process and control review

OUTPUTS & REPORTING

Clients receive:

Findings support improved resilience against mobile messaging-based social engineering attacks.

- A Smishing Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to reduce SMS-based phishing risk
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on preparedness and control effectiveness rather than individual performance
- Findings reflect a point-in-time view of smishing resilience during the assessment period
- The assessment does not guarantee prevention of all smishing attacks

PENETRATION TESTING: SOCIAL ENGINEERING

Vishing (Telephone Phishing) Security Assessment

> The Vishing (Telephone Phishing) Security Assessment evaluates an organisation's exposure to social engineering attacks conducted via telephone communications.

The objective of this assessment is to identify weaknesses in procedural controls and user awareness that could enable successful voice-based social engineering attacks.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- User awareness and response behaviours
- Verification and identity confirmation procedures
- Call handling and escalation processes
- Protection against caller spoofing and impersonation
- Incident reporting and response mechanisms
- Integration with security and fraud detection processes
- Alignment with recognised social engineering defence best practice

Engagement & Delivery

The Vishing Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment may combine:

All activities are conducted in accordance with agreed rules of engagement and designed to minimise operational impact and user disruption.

- controlled vishing simulations
- process and control review

OUTPUTS & REPORTING

Clients receive:

Findings support improved resilience against telephone-based social engineering attacks.

- A Vishing Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to reduce voice-based social engineering risk
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on preparedness and control effectiveness rather than individual performance
- Findings reflect a point-in-time view of vishing resilience during the assessment period
- The assessment does not guarantee prevention of all vishing attacks

PENETRATION TESTING: SOCIAL ENGINEERING

Physical Security Assessment

> The Physical Security Assessment evaluates the effectiveness of physical controls designed to protect facilities, assets, and personnel from unauthorised access or interference.

The objective of this assessment is to identify weaknesses in physical security measures that could enable unauthorised entry, asset compromise, or support broader cyber or insider threats.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Access control systems and entry mechanisms
- Visitor management and security procedures
- Perimeter security controls
- CCTV and monitoring arrangements
- Secure areas and asset protection
- Tailgating and unauthorised access risks
- Alignment with recognised physical security best practice

Engagement & Delivery

The Physical Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment may combine:

All activities are conducted in accordance with agreed rules of engagement and local legal and safety requirements.

- physical control review
- controlled on-site testing where permitted

OUTPUTS & REPORTING

Clients receive:

Findings support improved protection of facilities and critical assets.

- A Physical Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to improve physical protection
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on physical security controls rather than cybersecurity controls alone
- Findings reflect a point-in-time view of physical security during the assessment period
- The assessment does not guarantee identification of all physical security weaknesses

05

SERVICE FAMILY

Specialised Services

Adversary-focused and sector-specific assessments requiring detailed scoping and tightly controlled delivery.

6 ASSESSMENTS IN THIS FAMILY

- Red Team Security Assessment
- Purple Team Security Assessment
- Ransomware Simulation Security Assessment
- IoT Security Assessment
- Operational Technology Security Assessment
- Web 3.0 Security Assessment

SPECIALISED SERVICES

Red Team Security Assessment

> The Red Team Security Assessment simulates realistic adversary activity to evaluate an organisation's ability to detect, respond to, and contain advanced, targeted attacks.

The objective of this assessment is to provide insight into how effectively security controls, processes, and people perform against coordinated, goal-driven attack scenarios designed to emulate real-world threat actors.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Attack path discovery and exploitation
- Detection and response capabilities
- Security monitoring and alerting effectiveness
- Incident handling and escalation processes
- Lateral movement and persistence opportunities
- Impact assessment against defined objectives
- Coordination between technical controls and operational processes
- Alignment with recognised adversary simulation best practice

Engagement & Delivery

The Red Team Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in accordance with agreed rules of engagement and designed to assess organisational resilience rather than isolated vulnerabilities.

- adversary-style testing techniques
- controlled, goal-oriented attack simulation

OUTPUTS & REPORTING

Clients receive:

Findings support strategic improvements in security posture and incident readiness.

- A Red Team Security Assessment report
- Observations on detection, response, and containment effectiveness
- Practical recommendations to improve resilience against advanced threats
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on real-world attack simulation rather than comprehensive vulnerability discovery
- Findings reflect a point-in-time view of organisational resilience
- The assessment does not guarantee identification of all potential attack paths or defensive gaps

SPECIALISED SERVICES

Purple Team Security Assessment

> The Purple Team Security Assessment provides a collaborative security testing approach that combines offensive testing techniques with defensive capability validation.

The objective of this assessment is to improve an organisation's detection, response, and overall security effectiveness by facilitating close cooperation between testing specialists and internal security teams.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Detection and response capabilities
- Effectiveness of security monitoring and alerting
- Incident handling and escalation procedures
- Visibility across security controls and tooling
- Validation of defensive assumptions against realistic attack techniques
- Integration between security operations and technical controls
- Alignment with recognised security operations best practice

Engagement & Delivery

The Purple Team Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in accordance with agreed rules of engagement and designed to enhance organisational security maturity rather than purely identify vulnerabilities.

- controlled adversary-style testing
- collaborative working sessions with defensive teams

OUTPUTS & REPORTING

Clients receive:

Findings support improved collaboration between offensive and defensive security functions.

- A Purple Team Security Assessment report
- Observations on detection and response effectiveness
- Practical recommendations to improve security operations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on operational security effectiveness rather than vulnerability discovery alone
- Findings reflect a point-in-time view of detection and response capabilities
- The assessment does not guarantee identification of all defensive gaps

SPECIALISED SERVICES

Ransomware Simulation Security Assessment

> The Ransomware Simulation Security Assessment evaluates an organisation's preparedness, resilience, and response capabilities against ransomware-style attacks.

The objective of this assessment is to simulate key elements of ransomware activity in a controlled manner to assess the effectiveness of preventive, detective, and response controls without introducing real ransomware into the environment.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Initial access prevention controls
- Lateral movement and privilege escalation pathways
- Detection and alerting effectiveness
- Backup, recovery, and business continuity arrangements
- Incident response and crisis management processes
- Segmentation and containment capabilities
- Alignment with recognised ransomware resilience best practice

Engagement & Delivery

The Ransomware Simulation Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in accordance with agreed rules of engagement and designed to minimise operational risk and disruption.

- controlled simulation of ransomware techniques
- validation of detection and response processes

OUTPUTS & REPORTING

Clients receive:

Findings support improved readiness for ransomware-related incidents.

- A Ransomware Simulation Security Assessment report
- Observations on preparedness, detection, and response effectiveness
- Practical recommendations to improve resilience against ransomware threats
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment does not involve deployment of live ransomware
- Findings reflect a point-in-time view of ransomware preparedness
- The assessment does not guarantee prevention of all ransomware attacks

SPECIALISED SERVICES

IoT Security Assessment

> The IoT Security Assessment evaluates the security posture of Internet of Things (IoT) devices and the ecosystems in which they operate.

The objective of this assessment is to identify vulnerabilities, misconfigurations, and control weaknesses that could expose IoT devices, associated data, or connected systems to compromise.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- IoT device configuration and hardening
- Authentication and access control mechanisms
- Firmware versions and update management
- Network exposure and segmentation controls
- Data transmission and encryption mechanisms
- Integration with enterprise systems
- Exposure to common IoT attack techniques
- Alignment with recognised IoT security best practice

Engagement & Delivery

The IoT Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- configuration and architecture review
- controlled testing to validate control effectiveness

OUTPUTS & REPORTING

Clients receive:

Findings support improved control and reduced risk across IoT environments.

- An IoT Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to improve IoT security
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on device and ecosystem security rather than traditional IT infrastructure alone
- Findings reflect a point-in-time view of the IoT environment during the assessment period
- The assessment does not guarantee identification of all IoT-related vulnerabilities

SPECIALISED SERVICES

Operational Technology Security Assessment

> The Operational Technology (OT) Security Assessment evaluates the security posture of industrial control systems and operational environments that support physical and industrial processes.

The objective of this assessment is to identify vulnerabilities, misconfigurations, and control weaknesses that could impact safety, reliability, or operational continuity.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Industrial control systems and supervisory platforms
- Network segmentation between IT and OT environments
- Access control and authentication mechanisms
- Remote access and vendor connectivity controls
- Monitoring and incident detection capabilities
- System hardening and configuration management
- Exposure to known OT-specific attack techniques
- Alignment with recognised OT security best practice

Engagement & Delivery

The OT Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

The assessment combines:

All activities are conducted in accordance with agreed rules of engagement and with particular emphasis on safety and operational continuity.

- architecture and configuration review
- controlled validation testing appropriate for safety-critical environments

OUTPUTS & REPORTING

Clients receive:

Findings support improved protection of industrial operations and critical systems.

- An OT Security Assessment report
- Identified weaknesses with contextual risk explanation
- Practical recommendations to improve OT security and resilience
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment prioritises safety and reliability alongside security objectives
- Findings reflect a point-in-time view of the OT environment during the assessment period
- The assessment does not guarantee identification of all OT-related vulnerabilities

SPECIALISED SERVICES

Web 3.0 Security Assessment

> The Web 3.0 Security Assessment evaluates the security posture of decentralised applications, blockchain-based systems, and associated smart contracts and infrastructure.

The objective of this assessment is to identify vulnerabilities and weaknesses that could compromise the integrity, confidentiality, or trustworthiness of decentralised platforms and assets.

Scope & Focus

The assessment may include, but is not limited to, the evaluation of:

The specific scope is defined during formal engagement scoping and confirmed prior to commencement.

- Smart contract logic and implementation
- Blockchain interaction and transaction handling
- Authentication and key management mechanisms
- Integration between decentralised and centralised components
- Data integrity and immutability controls
- Exposure to common Web 3.0 and blockchain attack techniques
- Secure development and deployment practices
- Alignment with recognised Web 3.0 security best practice

Engagement & Delivery

The Web 3.0 Security Assessment is delivered under formal scoping and explicit authorisation and is managed through the Nanorisk Security Portal.

Testing combines:

All activities are conducted in accordance with agreed rules of engagement and designed to minimise operational impact.

- smart contract and platform review
- controlled testing to validate security controls and exploitability

OUTPUTS & REPORTING

Clients receive:

Findings support improved security and trust in decentralised systems.

- A Web 3.0 Security Assessment report
- Identified weaknesses with contextual risk explanation
- Prioritised remediation recommendations
- Secure access to findings and engagement artefacts via the Nanorisk Security Portal

IMPORTANT NOTES

- This assessment focuses on decentralised application and smart contract security rather than traditional web application security alone
- Findings reflect a point-in-time view of the Web 3.0 environment during the assessment period
- The assessment does not guarantee identification of all Web 3.0-related vulnerabilities

06

SERVICE FAMILY

Cyber Essentials

Assessment and preparation supporting Cyber Essentials and Cyber Essentials Plus certification, delivered via an accredited partner.

3 ASSESSMENTS IN THIS FAMILY

- Cyber Essentials: Self Assessment
- Cyber Essentials Plus
- Cyber Essentials: Guided Assessment

CYBER ESSENTIALS

Cyber Essentials: Self Assessment

> Self-assessment options are available based on organisation size. Each includes direct access to the Cyber Essentials self-assessment portal and the certification fee.

Organisation Sizes

- Micro: 0–9 employees
- Small: 10–49 employees
- Medium: 50–249 employees
- Large: 250+ employees

What's Included

- Direct access to the Cyber Essentials self-assessment portal
- Certification fee
- Cyber Essentials certification upon successful completion

CERTIFICATION DELIVERED THROUGH IASME

CYBER ESSENTIALS

Cyber Essentials: Guided Assessment

> An auditor-led Cyber Essentials assessment providing structured guidance throughout the self-assessment process. Ideal for organisations that would benefit from expert support in completing the questionnaire accurately.

What's Included

- Expert guidance through the self-assessment questionnaire
- Support in understanding and meeting Cyber Essentials requirements
- Structured approach to completing the assessment accurately
- Clarification of technical requirements and terminology

Prerequisites

Requires the purchase of a Cyber Essentials assessment (Micro, Small, Medium, or Large based on organisation size).

Benefits

- Reduced risk of assessment errors or misunderstandings
- Faster completion with expert assistance
- Greater confidence in assessment responses
- Support for first-time applicants

CERTIFICATION DELIVERED THROUGH IASME

CYBER ESSENTIALS

Cyber Essentials Plus

> A technical audit that verifies the Cyber Essentials controls are properly implemented through hands-on testing of systems and configurations.

What's Included

- Cyber Essentials Plus audit
- Certification fee
- Associated assessor expenses
- Cyber Essentials Plus certification upon successful completion

Prerequisites

A valid Cyber Essentials certification is required before pursuing Cyber Essentials Plus.

Additional Audit Day

An additional audit day may be required to support completion of a Cyber Essentials Plus assessment. This may be needed for complex environments with multiple locations, large organisations with extensive infrastructure, or where additional time is needed to complete the audit.

CERTIFICATION DELIVERED THROUGH IASME

Trust, Governance & Responsibility

Nanorisk operates under a defined governance framework covering professional conduct, confidentiality, data protection, and incident handling.

Professional Standards. We operate in accordance with recognised UK security and assurance principles, aligned with CREST professional standards and NCSC guidance.

Data Protection & Privacy. Fully compliant with UK GDPR and the Data Protection Act 2018, with formal data protection and privacy governance in place.

Formal Authorisation. Formal authorisation to test is obtained for every engagement, covering the full assessment lifecycle from scoping through to delivery.

Responsible Testing. Controlled testing practices designed to minimise operational risk and business disruption throughout the engagement.

Supply Chain Governance. Sub-processors and suppliers are carefully vetted and contractually bound to security and data protection requirements.

CONDUCT
All consultants operate under a mandatory Code of Conduct and Ethics Policy

IMPROVEMENT
Continuous improvement of methodologies, tools, and governance practices

ENCRYPTION
All client data protected using encryption at rest and in transit

RETENTION
Robust data retention and secure deletion policies

ACCESS
Strict access controls and role-based permissions

SCOPE
All testing conducted within clearly defined scopes and rules of engagement

COMMUNICATION
Secure communication for all client interactions and document exchange

NON-DESTRUCTIVE
No denial-of-service or destructive testing unless explicitly authorised

ESCALATION
Real-time escalation procedures for critical and high-risk findings

INSURANCE
Comprehensive Professional Indemnity, Cyber, and Public Liability Insurance

Nanorisk maintains a documented governance framework covering commercial, operational, security and delivery obligations. The documents below are maintained as controlled publications and are available to clients on request.

Commercial and contractual

- Statement of Works: scope, objectives, rules of engagement, deliverables and retesting
- Quote: pricing and commercial terms
- Terms and Conditions: the legal and commercial framework
- Data Processing Agreement: UK GDPR Article 28 compliance
- Portal Terms of Use, and our public Privacy Notice

Security and data protection

- Information Security Policy, Access Control Policy and Encryption Policy
- Data Handling, Data Retention and Deletion, and Information Classification policies
- Records of Processing Activities (UK GDPR Article 30) and Sub-processor Register
- Audit Log Retention Policy and Incident Response Policy

Delivery and quality

- Penetration Testing Methodology and service-specific standards
- Quality Management System, and Internal Quality Audit and Service Review
- Automated Testing Review and Vulnerability Validation Process
- Penetration Testing Tool Management Policy
- Prohibited and Permitted Actions and Techniques
- Scope Change and Deviation Request process

People

- Consultants Code of Conduct and Ethics Policy
- Employee Vetting, Induction and Onboarding, and Offboarding and Access Control
- Contractor and Partner Due Diligence
- Information Handling and Cybercrime Law awareness training

Working With Us

Getting started is a conversation, not a form.

Getting started

Get in touch with an outline of what you need assessed, even a rough one. We would normally arrange a short scoping call from there, because it is usually the quickest way to get to the right scope. If a meeting is not convenient, we are happy to work through the scoping questions by email instead. Either way we then issue a written Quote and Statement of Works, and once accepted, testing is scheduled around your operational constraints.

What we will need from you

Prerequisites depend on the type of assessment. The exact requirements for your engagement are listed clearly in the Nanorisk Security Portal and tracked there until they are met, so nothing holds up the start of testing. Typically they include:

- An accurate list of in-scope targets
- Any credentials or test accounts required for authenticated testing
- Relevant documentation and named points of contact
- Written confirmation that you have authority over the in-scope systems, and that any third-party permissions have been obtained

What you can expect

- Honest scoping. We will tell you if a cheaper service is the right one
- Controlled testing within agreed windows, designed to minimise operational impact
- Immediate escalation of anything materially serious, rather than waiting for the report
- A quality-assured report that serves both your engineers and your board
- Retesting, and a wash-up call to talk it through

A note on limitations

Assessments represent a point-in-time evaluation of the in-scope environment based on the information and access available during testing. While reasonable care is taken to identify security weaknesses, it is not possible to guarantee that all vulnerabilities or attack paths will be identified. System configurations, threat landscapes and vulnerabilities change over time.

Testing is performed using controlled techniques intended to minimise risk. As with any technical assessment, there is an inherent possibility of unintended system behaviour. Any material issues identified during testing are communicated in accordance with the agreed escalation procedures.

Contact

Get in touch for a free consultation and no-obligation quote. We typically respond within 24 hours.

24hr	Free	UK
RESPONSE TIME	CONSULTATION	BASED & OPERATED

TELEPHONE	+44 191 369 2434
EMAIL	info@nanorisk.co.uk
WEB	www.nanorisk.co.uk
CLIENT PORTAL	portal.nanorisk.co.uk
ADDRESS	The Work Place, Heighington Lane, Aycliffe Business Park, Newton Aycliffe, County Durham, DL5 6AH
CONNECT	LinkedIn · X · Instagram · Facebook · WhatsApp
COMPANY	Nanorisk Ltd · Registered in England & Wales · Company No. 13809559

ACCREDITED AND INDEPENDENTLY ASSESSED

CREST Penetration Testing · Cyber Essentials Certified · Cyber Essentials Certified Plus · IASME Cyber Assurance Certified Level One · Quality Principles Certified · Crown Commercial Service Supplier

Security disclosure

If you believe you have found a security issue affecting Nanorisk's own systems, our vulnerability disclosure policy is published at www.nanorisk.co.uk/vulnerability-disclosure, with machine-readable contact details at /.well-known/security.txt.

Copyright © 2026 Nanorisk Limited. All rights reserved. This publication is protected by copyright. No part of this document may be reproduced, distributed, or transmitted in any form or by any means without the prior written permission of Nanorisk Limited.