



DEEP INFOSEC / PUBLIC GUIDE

# Cybersecurity Audits, Pentesting & Assurance

A clear guide to authorized security testing, ISO-qualified audit services and evidence-led remediation.

Engineering, security and operating capability — brought together around the outcome your organisation needs.

[deepinfosec.com](https://deepinfosec.com) • [sales.general@deepinfosec.com](mailto:sales.general@deepinfosec.com)

# What this means for your organisation

Review the scope of typical assessments, how testing is controlled, and the reports and follow-up actions delivered.

## Security audits & assurance

An audit is valuable when its conclusions can be traced from a business requirement to a control, an observed fact and an accountable action. Our ISO-qualified auditors structure evidence sampling, assess the design and operation of controls, and provide findings that management can prioritize. Applicable PASC/OSPCRM assessment scopes are identified for the engagement, with clear separation between advice and independent assurance.

## Penetration testing

A useful penetration test answers how a real attacker could move through the environment and what would stop that movement. We work from written authorization and agreed test boundaries, examine applications, APIs, identities, infrastructure and selected industrial interfaces, and report reproducible findings with practical remediation guidance. Follow-up testing shows whether the corrective measures address the underlying path.

## Security consulting

Effective security consulting has to end in a system that works, not only in a maturity score. Our architects examine identity, networks, cloud, software supply chains and operational responsibilities together. They help teams set priorities, make changes safely, document the new operating model and retain a clear record of accepted residual risk.

# Workstreams and outputs

## Security audits & assurance

Internal audit support, external independent assessment or ongoing controls assurance; issuer, accredited entity and certification boundaries appear in the confidential assignment dossier.

- Governance and controls: risk-based control testing against defined ISO 27001/27002, ISO 22301, ISO 27701 and other applicable reference requirements.
- Technology and supplier assurance: identity, cloud, change management, logging, backup, vendor and software supply-chain review with evidence sampling.

What you receive: Audit charter, criteria, independence and sample-selection plan

## Penetration testing

One-time authorized test, recurring assessment or retest programme. PASC accreditation and the authorized testing entity are stated in the engagement-specific supplier dossier.

- Application and API testing: authorized web, API, mobile and business-logic assessments, including authentication, authorization and cross-tenant controls.
- Infrastructure and cloud offensive security: externally and internally scoped tests, identity attack paths, configuration validation and privilege escalation.

What you receive: Signed rules of engagement, test boundaries, contacts and stop conditions

## Security consulting

Advisory, embedded specialists, implementation sprint or managed improvement programme; integrate Deep Advisor and DeepShield where appropriate.

- CISO and security strategy: target operating models, security governance, board reporting, budgets, policies and a sequenced risk-reduction programme.
- Cloud, identity and DevSecOps: architecture reviews, IAM/SCIM reconciliation, privileged access, Kubernetes, pipelines, application and API security.

What you receive: Security maturity and exposure assessment tied to business services

# A practical engagement, from first scope to handover

## 01 Define the decision

We agree what must change, which systems matter, what the organisation already owns and what constitutes an acceptable outcome.

## 02 Evaluate on the right perimeter

A scoped assessment or pilot gives engineering teams sufficient information to choose a realistic deployment and acceptance plan.

## 03 Deliver with evidence

The team delivers designs, implemented controls or services, records decisions, tests outcomes and explains operating responsibilities.

## 04 Transfer operational capability

Documentation, knowledge transfer, maintenance pathways and follow-up are part of a sustainable programme.

## Talk directly to the specialist team

Explore the full offering at [deepinfosec.com](https://deepinfosec.com) and select the specialty matching your objectives. Public introductions are freely available; confidential technical and commercial dossiers follow a controlled customer process.

[deepinfosec.com](https://deepinfosec.com) · [sales.general@deepinfosec.com](mailto:sales.general@deepinfosec.com)