Security Review

Enhance your organisation's security posture and effectiveness with our Security Review.

Our comprehensive Security Review is designed to objectively help you understand the current security posture, operating model and the compliance position of your organisation's cloud environments and business-critical workloads. This review takes your supporting polices, standards and processes into consideration and provides relevant guidance and actionable enhancements that are aligned to your organisation's security initiatives, and compliance goals and are based upon industry and technological best practices.

This engagement is executed by our skilled Security Advisory team which includes a security lead, a project manager, and different domain technical specialists to provide expert feedback and guidance. Proactively securing your business is no longer a choice – it's a necessity, and we are the trusted partner to support you on that journey.

Core components of the Security Review

Discovery Workshop

Understand your priorities, regulatory compliance requirements, framework compliance, policies, standards & processes. Understanding your stack and tooling & capture architecture state and any docs.

Identity Strategy Review

A review of your identity strategy, tooling and any gaps or enhancements plus security technical assurance.

Network Posture Assessment

Assess your cloud network design and implementation, adherence to your desired compliance frameworks, noting any deviations from best practices or reference architectures, and providing enhancements or improvements.

SDLC, DevSecOps & Software Supply Chain Review

Diving into your software development lifecycle processes, surrounding governance & security tooling. Analysing the use of 3rd party software, tools and dependencies and how supply chain interruption and compromise are managed. Generate enhancements and a gap analysis.

Landing Zone Review

A review of your Azure Landing Zone implementation against Microsoft's Cloud Adoption Framework.

Cloud Operating Model Review

Current Operating State Workshop

Explore your organisation's operating model – people, process & policies. Analyse and document the findings.

Desired Operating State Workshop

A round-table discussion to understand the desired operating model and note any known issues or pain points.

Security Policy, Standards & Process Review

A review of documents to ensure they follow best practices, are relevant and align with your business security initiatives.

Gap Analysis and Remediation Path

Generate a prioritised list of action items and changes to enhance cloud & security operations across the organisation.

Well-Architected Framework Reviews (Per Service)

We run a Critical Workload Discovery Workshop to identify and explore your key services. Following this, we conduct an expert-led workshop to understand each critical service and all its components and dependencies. We then perform a security and resilience review of each workload to clearly define the resilience and security posture of that service, offering recommendations to reduce risk and enhance resilience and security.

Advanced Threat Modelling (optional add-on to WAF Review per Service)

Performing threat modelling for business-critical workloads allows you to better understand potential threat vectors and defend against them. Threat modelling is conducted using the STRIDE framework, and diagrams and a report are provided.

Framework Specific Targeting (optional)

Where an organisation is aiming to achieve compliance with a specific standard or framework (e.g. PCI-DSS, HIPAA, Fed Ramp, CIS, Cyber Essentials/Plus, ISO270001) we can perform a customised review that assesses the current compliance posturing, identify any gaps or non-compliances, define a security improvement programme and devise a measurable plan to then implement improvements to achieve the desired compliance position.