
Excelium
Security
Engineering
Build security into every layer

Excelium Security Engineering - Designing secure systems. Enabling confident delivery.

Introduction

Attackers exploit gaps in design, identoty, automation, and operations not just unpatched systems. Excelium's security Engineering service line partners with you to build security into the fabric of your platforms, accelerating delivery and reducing risk.

Our approach provisions secure solutions design and implementation of security technologies to protect your organisation from cyber threats. We deliver secure-by-design architectures, guardrails, automation,m and detection so your teams can concentrate on what is important to the business.

What we solve

Excelium helps organisations design and engineer security that is resilient by default, reducing risk through secure architecture, hardened platforms, and a smaller attack surface.

- Transform security from policy to practice through engineered controls
- Prevent breaches by designing security into cloud, platforms, and infrastructure
- Reduce exposure by identifying and closing attack paths and misconfigurations
- Improve resilience by hardening systems against real-world threat
- Enable confident innovation through secure-by-design architecture and cloud adoption

Who we help

We help organisations that need security engineered into their environments, not retrofitted after incidents or audits.

- **Government and regulated entities** required to meet strict security and assurance frameworks
- **Cloud-first and hybrid organisations** modernising platforms while managing risk
- **Security and technology leaders** responsible for designing resilient, scalable architectures
- **Enterprises with complex infrastructures** seeking consistent hardening and attack surface reduction
- **Organisations undergoing transformation** such as cloud migration, platform uplift, or digital expansion

Core security engineering capabilities

Secure Architecture Design and Review

Foundational security architecture and design, security patterns and reference designs that scale with your business.

Our specialities include

- Testing Zero Trust network and identity architecture development
- Segmentation and least privilege patterns deployment
- Secure configuration review

All secure architecture and design activities are supported by archirecture decison records (ADRs), reference patterns, blueprint diagrams, control matrices.

Cloud Security Engineering

Our Cloud Security Engineering team delivers secure-by-design cloud foundations through hardened landing zones, robust identity and access controls, and comprehension cloud security assessments across Azure, AWS, and GCP.

Hardened landing zones and guardrails for Azure, AWS, and GCP

- Secure landing zone development (network, identity, logging)
- Multi-account/tenancy controls, conditional access, workload identities
- Cloud Control Assessments

Hardened, well-governed cloud foundations reduces misconfiguration risk, strengthens identity controls, and enables organisations to scale securely and confidently in the cloud.

Identity and Access Engineering

Robust Identity and Access Engineering establish resilient, least-privilege identity foundations through advanced IAM/PAM design, adaptive access controls, automated entitlement governance, and secure lifecycle management for people, services, and workloads.

Build strong identity foundations - the cornerstone of modern defence

- Enterprise IAM, PAM, and JIT/JEA designs
- Conditional access and adaptive authentication
- Fine-grained ABAC/RBAC, entitlement review automation
- Service account lifecycle, workload identity, key rotation

Role taxonomies, policy pacls, access review automation, onboarding/offboarding flows.

Attack Surface Reductions

Our Attack Surface Reduction capability strengthens platforms end-to-end by enforcing hardened baselines, securing containers and endpoints, and ensuring resilient recovery through immutable storage and validated backup integrity.

Infrastructure and Platform Hardening make compromise harder and recovery faster

- Baselines for Windows/Linux, Kubernetes, databases, messaging, and middleware
- Containers/Kubernetes security (admission control, runtime, PSP replacements)
- Endpoint hardening, configuration drift prevention, secure images and registries
- Backup integrity, immutable storage, and recovery rehearsals

CIS-aligned baselines, golden images, policy artefacts, compiance mappings.

Our Approach, Methodology

Our team utilises the latest industry standard frameworks, recognised engineering methodology and state of the art tolls.

A methodical approach to offensive security

- Build-Run-Transfer - We design and build initial capability, operate side-by-side, then transfer ownership with training and artefacts
- Platform Blueprint and Accelerator - A packaged set of secure landing zones, policies, pipelines, and detections to jump-start your programme in weeks, not months
- Threat-Led Control Uplift - Targeted uplift mapped to realistic attacker techniques affecting your sector, priositised by business impact

Our tried and tested approach and methodology aligned to strict engineering frameworks and provides guaranteed results.

Measurable Value

We define and track metrics that matter:

- Control coverage and policy enforcement rates
- Identity hygiene (privileged account reduction, stale entitlements)
- Hardening and drift (baseline adherence, remediation time)
- Executive roadmap and risk-to-control mapping
- Architecture decision records and reference designs
- Hardened infrastructure baselines and IaC modules

Why Excelium

- **Engineering-led:** Practitioners who design, build, and ship secure platforms - not just audit them
- **Threat-informed:** Controls mapped to real adversary techniques and business risk
- **Cloud-native and hybrid:** Azure, AWS, GCP, on-prem, and OT/ICS integration experience
- **Outcome-drive:** Tangible artefacts, automated guardrails, and measurable improvements.
- **Senior-led delivery:** Architects and principal engineers with hands-on credibility.

Our experience

Great Barrier Reef Marine Park Authority

The Great Barrier Reef Marine Park Authority (GBRMPA) engaged Excelium to conduct an independent security review and uplift of its Microsoft cloud environment, encompassing Azure, Microsoft 365, and Microsoft Purview. The engagement was undertaken to provide assurance that cloud services were securely configured, compliant with the Australian Government Information Security Manual (ISM), and aligned to the Protective Security Policy Framework (PSPF), as well as relevant whole-of-government cloud blueprints and benchmark guidance.

Optus - Department of Health, Disability and Ageing

Optus engaged Excelium to conduct a Secure Configuration Review of its Department of Health, Disability and Ageing (DHDA) Secure Access Service Edge (SASE) environment, based on Zscaler, with a specific focus on Microsoft 365 (M365) split tunnelling. As DHDA's workforce increasingly relies on Microsoft cloud services, the objective of the engagement was to ensure that network security controls were aligned with Microsoft-recommended design guidance, while continuing to enforce robust inspection and policy controls for all non-Microsoft traffic.

Raiders Group

Raiders Group engaged Excelium to deliver a Security Engineering Organisational Uplift, designed to strengthen foundational cyber security controls and embed sustainable security practices across the organisation. The engagement focused on improving clarity of accountability, translating policy intent into enforceable technical controls, and strengthening prevention measures across key security domains. Rather than isolated technical fixes, the uplift delivered a structured, repeatable framework that aligned people, process, and technology.

They trust us

CANBERRA RAIDERS

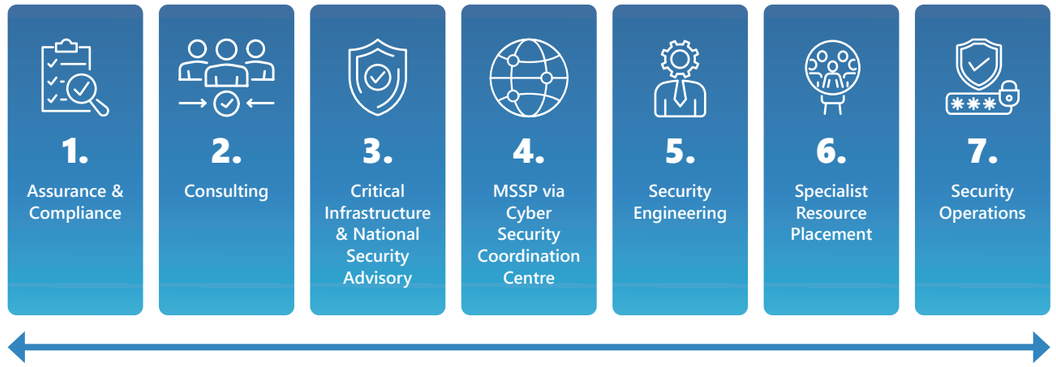
AINSLIE GROUP

SARONIC

FEDERAL GOLF CLUB CANBERRA

How we operate

Excelium's Seven Pillar model positions us as a true full-stack cyber and risk management partner. Our seven service lines combine to deliver end-to-end capability and full solutions across the entire security lifecycle from strategy to assurance, engineering to operations, and compliance to resilience. Each pillar is powerful in its own right and together they form the basis of a service which can provide a holistic resilience framework for our clients.



Excelium's Seven Pillars

- **Assurance & Compliance:** Security framework achievement, certification readiness, and continuous compliance.
- **Consulting:** Strategic cyber advice, regulatory compliance, cyber security maturity assessments, and cyber uplift roadmaps.
- **Critical Infrastructure & National Security Advisory:** *Security of Critical Infrastructure Act 2018* compliance, 'All Hazard' risk assessments, Critical Infrastructure Risk Management Plans, Hosting Certification Framework accreditation, transport security plans and compliance, and national security risk management.
- **Managed Security Services (via CSCC):** Proactive threat monitoring, SOC/SIEM integration, and rapid cyber incident response.
- **Security Engineering:** Secure-by-design architecture, system integration, and security hardening and attack surface reduction.
- **Specialist Cyber Resource Placement:** Embedding skilled professionals (CISO, ITSA, Analyst, Architect and GRC personnel) for immediate impact and long-term capability.
- **Security Operations:** Offensive penetration testing, digital forensics, incident response, operational defence, cybersecurity exercising

Our Cyber Security Coordination Centre (CSCC) underpins the model, acting as a central command hub for managed services and rapid incident response, enabling faster mobilisation, coordinated resourcing, and continuous monitoring tailored to each client's environment - all under a single contract and single account manager.

Get in touch

Mark Farley-Thompson
Security Operations & Engineering Partner
0412883750
Mark.Farley-Thompson@excelium.com.au

ACT – Head Office
Ground Floor
Unit 2,14 Brisbane Avenue
Barton ACT 2600

NSW
Level 11
66 Clarence Street
Sydney, NSW 2000

QLD
167 Eagle Street
Brisbane 4000 QLD