

Reduce the risk that matters to your business within 90 days

You have security tools, teams and remediation backlogs. The difficult part is deciding which combination of issues threatens a critical service, what must change first, and how to demonstrate that the change worked. Our Risk Compression Sprint brings those decisions into one time-bound engagement. Deep InfoSec works with your security, cloud, identity and business-service owners; Deep Advisor supplies the attack-path analysis and scenario evidence.

Days 1-30 · Understand the real exposure

We agree the critical services in scope, connect authorized scanner, cloud and identity evidence, map dependencies and establish a reproducible risk baseline. We distinguish an isolated issue from a viable route to business impact.

Days 31-60 · Remove the most consequential paths

Your owners review the proposed remediations with our architects. We test mitigations, change identity and network controls where authorized, and prioritize work that breaks multiple attack paths rather than merely changes a severity score.

Days 61-90 · Prove the reduction and transfer ownership

We retest the paths affected by remediation, document the evidence, prepare a board-level decision record and hand over an ordered workstream for controls that remain.

Deliverables and responsibilities

You receive a critical-service dependency map, prioritized attack-path register, risk/impact/recovery view, remediation decision log, tested control changes and a 90-day executive report. Your team provides technical access, service ownership and change approval; Deep InfoSec provides analysis, engineering, verification and the handover pack.

First engagement

The programme begins with one bounded service or portfolio and can be extended into ongoing Deep Advisor monitoring or a managed engineering service.

Technical working notes

How the first scope is chosen

Select one essential business service, its technical owner, its critical dependencies and a measurable acceptance baseline. Confirm approved data inputs, testing windows, decision rights and the configuration evidence that can be compared after remediation.

What the assessment actually measures

Service reachability, identity privilege, exploitable multi-step paths, functioning compensating controls, business impact, recovery constraints and the validation state of each mitigation.

A practical decision record

Every prioritized attack path is linked to the affected service, its technical preconditions, a named remediation owner, the decision taken, the test result and the residual exposure. Leadership receives a concise view; operators receive the engineering detail.

Acceptance and continuation

The handover is accepted against the original service scope: critical paths analyzed, planned changes executed or explicitly deferred, retests completed, evidence recorded and remaining work assigned.

sales.advisor@deepinfosec.com | <https://deepinfosec.com>