

EXPERIENCE

Experience behind the approach

Six examples from Haroon Mahmood's previous in-house security roles and how that experience can support your business through Kurosec.

By Haroon Mahmood

These examples describe work from my previous in-house security roles. They are anonymised to focus on the problems, the work and its practical relevance. The final paragraph of each explains how I can apply that experience through Kurosec.

Giving a business its first security function

A security programme needs people who can make decisions and teams who know what is expected of them. The documents support that work, but they cannot do it on their own.

As the first dedicated Head of Information Security at a software business, reporting to the CFO, I established the security function and its direction. I set a risk-based roadmap and built the management framework around it: policies and standards, a risk assessment method, a risk register and a process for agreeing and following through on treatment.

I worked with business and technology owners to assess exposure, challenge weaknesses and agree practical improvements. Alongside that, I established and chaired a Security Committee. This gave senior leaders a regular view of material risks, control effectiveness, progress and decisions that needed their involvement. Control reviews and independent testing fed into the same programme of work.

The result was an established security capability with clearer ownership and leadership oversight. It also provided a basis for ISO 27001 readiness, with the work connected to the organisation's risks and operating needs.

Through Kurosec, I can help a business build those foundations in a form it can sustain. An engagement might establish the initial priorities, a usable risk register, clear control ownership and a reporting routine that brings decisions to the right people. The scope should reflect the business, its existing capabilities and the time its teams can realistically commit.

Deciding which suppliers need closer attention

A supplier's invoice tells you very little about the consequences of losing its service or exposing the information it handles. That distinction shaped the global supplier security programme I established and led in a technology organisation.

I developed a risk methodology that considered the service being provided, the business's dependency on it, access to systems and information, data sensitivity and operational impact. The

supplier inventory captured ownership and exposure so that assurance could be directed towards the relationships that mattered most.

I introduced different levels of assurance according to risk. For higher-risk and strategically important suppliers, the work included reviewing control evidence, challenging weaknesses and agreeing treatment. Procurement, Legal, business owners and suppliers all had a part in turning findings into actions, contractual commitments and decisions about remaining risk.

Some issues extended beyond a single supplier assessment. I established and chaired a cross-functional supply-chain forum to address those wider dependencies and ownership questions. This gave them a route to senior attention alongside the individual assessment and remediation process.

Through Kurosec, I can help turn a supplier list into a proportionate assurance programme. That can mean defining what makes a supplier critical, establishing a manageable evidence review and agreeing who owns each decision and follow-up action. The aim is to concentrate effort where failure or compromise would affect the business most, while keeping the process workable for the people who use it.

Making security requirements usable

Security requirements need to make sense to the people designing systems, running services and making business decisions. A policy may state the intention clearly and still leave those people unsure how to apply it.

In a global technology organisation, I worked on aligning enterprise security policies with ISO 27001 and consolidating separate standards into a coherent control framework. This sat alongside my wider security architecture and risk work across applications, infrastructure and technology programmes.

I worked directly with business units and engineering teams to translate enterprise requirements into practical guidance. I also defined application, system and infrastructure security requirements and helped teams incorporate controls into design and implementation. The work connected the organisation's expectations with the decisions being made in real projects.

The work brought separate standards into a common framework, with guidance that connected the requirements to design and delivery decisions. It gave the policy and technical work a shared structure while keeping attention on how the controls would be applied.

Through Kurosec, I can review an existing policy set or help establish one. I would look at how policies, standards and working procedures fit together, who owns them and what teams need in order to act on them. Depending on the starting point, the work might include consolidating requirements, making responsibilities explicit and writing guidance that explains the expected practice in plain language.

Turning an exercise into a programme of improvements

A tabletop exercise becomes useful when the discussion produces decisions the organisation can act on afterwards. The scenario gives people something concrete to work through; the follow-up is where the learning becomes part of everyday preparedness.

Within the security leadership function of a global technology organisation, I designed and led an enterprise tabletop exercise programme. It brought together technical and non-technical participants, including senior executives, to work through realistic security scenarios and structured decision points.

The programme covered escalation, communications, risk acceptance, prioritisation and recovery. I developed its methodology, governance and participation approach, creating a repeatable way to explore how different parts of the organisation would work together. That meant addressing the decisions around an incident as well as the technical response.

Findings were converted into specific improvement actions, assigned to accountable owners and tracked. The exercise capability was adopted across the security organisation, providing a repeatable way to bring teams together, examine decisions and follow through on what they found.

Through Kurosec, I can help an organisation plan and run an exercise around the decisions it most needs to examine. The work can include agreeing the purpose and participants, developing the scenario, facilitating the discussion and producing a prioritised action record. Follow-up can then test whether the agreed changes have been made and whether the remaining issues need another exercise, further assurance or a leadership decision.

Looking beyond the training completion rate

Completion figures can show that people have received training. They tell you much less about the situations that expose a business to risk or whether a particular intervention is useful.

In a global technology organisation, I reshaped an existing phishing and awareness programme around the risks people were encountering. I combined phishing simulation results with information from security systems, incidents, threat intelligence and business context to understand where exposure was concentrated.

That evidence informed the simulations, awareness activity and follow-up work. I also wrote focused guidance based on current threats and the risks visible in the organisation. The purpose was to make the material relevant to the situations people were likely to encounter and to direct effort towards the areas that needed attention.

Where the evidence pointed to a weakness in a business process, I worked with accountable owners on that process alongside the awareness activity. This connected targeted guidance with actions for the teams responsible for the underlying work, so the response could address both the task and the advice people received.

Through Kurosec, I can help review an awareness programme and identify what its evidence is actually telling you. An engagement could define a small set of relevant risk themes, develop practical

guidance and agree how to assess progress. It can also identify where a workflow or control change would help people work more safely, alongside the advice they receive.

Changing the way sensitive information is handled

Sometimes the most useful security recommendation changes the way a task is carried out. That was the case when I worked as the security partner to global HR and Finance functions in a technology organisation.

I identified unnecessary exposure from manual processes and locally held employee information. I recommended moving the relevant data handling into purpose-built managed applications. The business and IT teams built those applications, removing the need to download and process the sensitive data locally.

My security work included defining requirements and baseline controls for the applications, covering role-based access, logging and data minimisation. Bringing those requirements into the design stage connected the intended improvement in information handling with controls the delivery teams could implement.

The revised workflow reduced the need for people to handle sensitive information outside the managed applications. The business and IT teams delivered the applications; my role was to identify the exposure and define the security requirements that supported the change.

Through Kurosec, I can help examine how sensitive information moves through a process, identify unnecessary handling and define proportionate improvements. That could involve changing access, reducing the information used, improving an existing system or considering a different workflow. The appropriate answer depends on the task and the available capabilities; the starting point is understanding what people need to achieve and where the exposure arises.