Agile Security and the SPF

The Security Policy Framework was introduced to clarify and extend the security responsibilities of officers within government. It is a significant recasting and refinement of the Manual of Protective Security (MPS) providing clear definitions of policy, responsibilities and guidance. The changes were made in response to high-profile incidents; compliance is obligatory, with the emphasis on senior officers responsibilities. The requirements, which ensure compliance, are now more onerous and new guidance is published monthly, all of which has to be considered and acted upon. All this needs to be accomplished in an environment where pressure on budgets are immense.

Cornwell Business Consultants' have developed a portfolio of methodologies [see Cornwell Lean / Agile Approaches] designed to deliver business solutions quickly, reliably and cost-effectively. Part of the portfolio is "Agile Security". It deploys best-practice security, compliant with the SPF but keeping track of changes to configurations, threats and asset valuations – all of which effect the security case – continuously. By building agile security into the organisation, security can be improved, compliance assured, awareness increased and costs reduced

The agile approach keeps the Accreditor, SIRO, SRO's and IAO informed of the changing risk environment in response to emergence of vulnerability discoveries, changes to threat assessment and guidance publications. It provides a brief update of any changes and incorporates each change into a "dynamic" RMADS. The RMADS is kept up to date and changes tracked. The RMADS, and security case, is an agile document. This not only improves security but also ensures the workload on individuals is controlled while their understanding and awareness of issues is improved.

In a production environment, agile security links to change management, ideally compliant with ISO 20000, following ITIL guidance. It builds security evaluations into the Service Transition, Service Operation, and Continual Service Improvement aspects of the ITIL Lifecycle Phase. Risk management decisions are assessed against the SPF and Codes of Connection such as the GSI CoCo recommendations or derogations are enacted as part of the process.

In a development environment: Service Strategy and Service Design, Agile security can operate in two possible modes:

1. It can be built into the development, as part of the security case development following the classic OGC Gateway process defined in IAS 2. But it delivers updates to the security case incrementally throughout the development, rather than simply delivering a RMADS at each of the prescribed stages.
2. Security becomes one of the roles in XP, SCRUM or DSDM environments, The security case being part of the package of deliverables at each increment.

Cornwell has experience of steering many organisations through this process, using highly experienced CLAS consultants with knowledge of agile methods. Further details can be found in other Cornwell Publications : Agile Security – an introduction, Preparing a security policy for agile implementation, Scoping Systems using the VSM and Agile Accreditation to ISO 27000.

www.cornwellbc.co.uk
Tel: 01372 454648
E-mail: dominic.cornwell@cornwellbc.co.uk