Security Assurance Coordinator

Introduction

The Security Policy Framework (SPF), the framework of security policies that all Government Departments and Agencies operate in accordance with, states that: "All ICT systems that handle, store and process protectively marked information or business critical data"... "must undergo a proportionate accreditation process..."

Although private sector companies are not bound to the same rigorous process, it is recommended that they conduct appropriate Business Impact Assessments and Risk Assessments to arrive at an appropriate level of risk management and implementation of security controls.

Security Assurance Coordinator

Within Ministry of Defence (MoD) projects the accreditation process is usually facilitated by a Security Assurance Coordinator (SAC). The SAC is an Information Assurance (IA) expert, whose credentials will be supported by qualified membership of a professional Information Security body and/or certification in the CESG Listed Adviser Scheme (CLAS). Working for the project team, the SAC provides advice and guidance on all aspects of Cyber Security, including IA, Risk Management and Accreditation. With a sound understanding of electronic security measures, cryptographic requirements, configuration management practices and risk management – and adopting a holistic approach to the security requirements of the project and business area – the SAC provides the vital interface between the Accreditor, the supplier, the project team and the end user community, ensuring that all aspects of security are delivered throughout the project lifecycle.

In much the same way as it is necessary to employ a Safety Consultant to assure a system's safe design and subsequent use, so too is it necessary to employ an SAC to assure that the system and its sensitive information are secure, and the system will continue to operate as it should and when it should, regardless of any system vulnerabilities and threats posed to it.

It is doubtful that the Project Manager, although well versed in the area of project or programme management, is likely to have a full understanding of the latest HMG and MoD security policies and therefore, could not hope to see their system go through the security assurance rigours of, for example, a Penetration Test to meet the requirements for Security Accreditation. Neither are those managers likely to have the time to construct the Risk Management and Accreditation Document Set (RMADS) with all of the supporting documentation that this entails. It's also unlikely that the project manager could sit comfortably in a Security Working Group (SWG) surrounded by security risk owners and Accreditors and give correct responses to direct questions about

the latest endorsed techniques for security risk mitigations.

The employment of the SAC enables project managers to oversee the wider issues of the project; project costs, delivery dates, user satisfaction, etc, without having to worry about liaison with security regulators (Accreditors), production of security documents, changes to security policies, and an endless list of tasks or fact-finding processes that could otherwise be performed by the SAC.

Security Assurance Coordinator Responsibilities

To ensure the effective coordination of all project security aspects, all queries, document reviews, requests for advice and testing, requests will be channelled through the SAC before they reach the Information Asset Owner (IAO), Accreditor or Project Team. The SAC's in-depth knowledge, understanding of the project and coordination of all security aspects is invaluable throughout the entire project lifecycle. The SAC is responsible for ensuring that all security aspects are considered, coordinated, witnessed and conducted professionally, efficiently, on schedule, and in compliance with policy and legislative requirements. Considerable savings can be made, in terms of manpower, time and organisation because the work completed by the SAC enables other personnel to be utilised effectively within their primary roles, rather than having the additional burden of coordinating and considering the security aspects of a project (a specialist area in its own right).

The SAC monitors and reports to the Accreditor, Information Asset Owner and Project Management Team on all security matters relating to the project. They will attend all security meetings and may chair them on behalf of the Project Manager.

The primary tasks of the SAC are to:

- Ensure that personnel in all security roles required for the project have been identified, are aware of their responsibilities in fulfilling the role, and are suitably briefed;
- Coordinate, consider, witness, manage and report on all security requirements for the project, ensuring they are completed professionally, efficiently and to schedule, and that they are fit for purpose and compliant with relevant policy and legislation;
- Ensure all appropriate actions are taken to achieve accreditation;
- Provide advice on security policy (covering both policy that is already in place e.g., HMG Security Policy Framework (SPF), Departmental Policy, IEC/ISO 27001 controls and the creation of new security-related documents for the project, such as a RMADS), relevant legislation (e.g. Data Protection Act, Freedom of Information Act), technical solutions, risk management and IA;
- Ensure all cryptographic requirements are met;
- Monitor and report on project security requirements and issues as they arise, reporting unresolved issues to the IAO, Accreditor, Project Manager and supplier (where necessary);
- Organise the project security meetings and chair them on behalf of the Project Manager, if required;
- Be responsible for the production of all security deliverables (e.g., security documentation, testing witness reports) and ensuring they are fit for purpose and delivered on schedule; and,
- Create, update and manage the Security Risk Register and ensure it is reviewed at the security meetings.

Suffice to say the employment of the SAC in MoD projects is easily transferrable to wider Government, and indeed private sector projects.

Regency IT Consulting have the expertise and experience to fulfil the SAC role for projects and programmes within your business environment. Our security consultants are all senior people with long track records of delivering security services within the public and private sectors. All have gained their experience within Central Government in roles either within CESG (the UK National Technical Authority for Information Assurance), the military, or with blue chip suppliers providing secure IT systems to central government and the MoD. Regency's highly experienced consultants are able to deliver the full spectrum of specialist IA support to both public and private sector organisations throughout the UK and elsewhere.