Technical Information Assurance Team Structure

and Role Description

Introduction

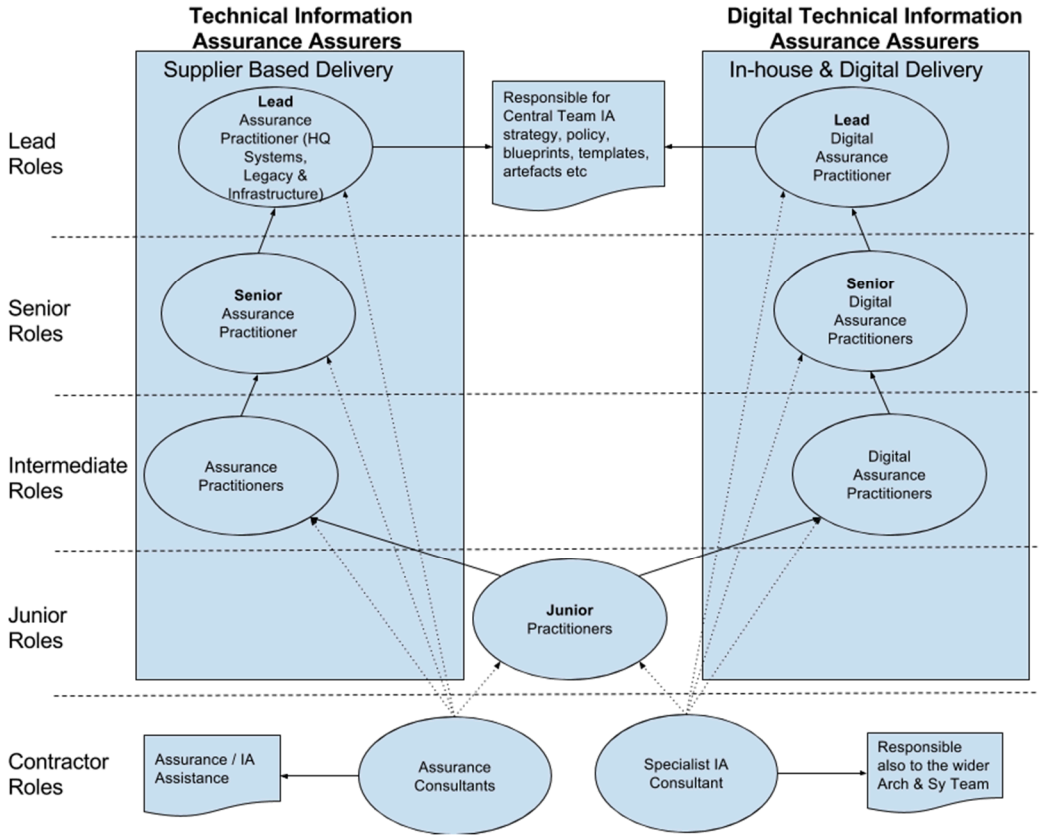
The Team is led by the Technical Information Assurance Leads. They are responsible for jointly managing the team, setting the strategy, designing the processes, principles and blueprints and have reporting responsibilities for the stream beneath their area of expertise Elaine Ventura, the Technical Information Assurance stream and Ray Neal, the Digital Products Technical Information Assurance stream.

The Assurance streams have responsibility for providing assurance activities for existing traditional supplier led delivery, including the legacy estate, TTP, Shared Services etc and the Digital Information Assurance stream for in-house developed products and solutions.

The diagram, below, shows the proposed structure of the Technical Information Assurance team. As can be seen, there are opportunities for all team members to progress through their roles to more senior positions.

There may also be an opportunity for personnel in non IA roles to change career and join the team as junior Assurance practitioners. This role has a very wide definition and typical functions may be Risk management, 27001, auditing, IA doc production and supporting assurance work for both Streams.

It is important that the job titles accurately describe the work we are carrying out and there are a number of suggestions against the job descriptions below.


Technical Information Assurance Assurers
Digital Technical Information Assurance Assurers
Supplier Based Delivery
In-house & Digital Delivery
Lead Roles
Senior Roles
Intermediate Roles
Junior Roles
Contractor Roles
Lead Assurance Practitioner (HQ Systems, Legacy & Infrastructure)
Responsible for Central Team IA strategy, policy, blueprints, templates, artefacts etc
Lead Digital Assurance Practitioner
Senior Assurance Practitioner
Senior Digital Assurance Practitioners
Assurance Practitioners
Digital Assurance Practitioners
Junior Practitioners
Assurance / IA Assistance
Assurance Consultants
Specialist IA Consultant
Responsible also to the wider Arch & Sy Team

Technical Information Assurance Practitioner

Reporting

- Report to Senior Technical Information Assurer

Role/Purpose

- Provide assurance that solutions are delivered against information assurance requirements in a cost effective and proportionate manner
- Work with project teams and suppliers to ensure that there are no security issues affecting the capability of teams to deliver, and to ensure that delivery is within the businesses information risk tolerance and appetite
- Applying independent information security / assurance advice to projects to achieve assurance outcomes which are acceptable to the IAO and the SIRO (CISO?) throughout the lifecycle of the solution
- Work with project managers and suppliers to understand information risks for new and existing services
- Ensure that new and updated solutions are built and operated securely
- Assist with building a culture of continuous delivery and improvement, ensuring that key systems and infrastructures etc. are regularly risk assessed, maintained and improved
- Taking an active view of technological trends and market developments, identifying opportunities to shape the future approach to pragmatic security and assurance

Knowledge/Experience

- Requires a balanced skill-set between information assurance, business requirements, secure architectures, policy and risk management
- Understanding of the UK Government's Cyber Security and Digital strategies along with the implications and opportunities presented by such generally in central government but specifically in the context of MoJ Digital & Technology's current and future operating circumstances
- Proven experience of implementing HMG IA policy, guidance, risk assessment and management etc in a comparable organisation/department
- Experienced HMG IA professional, with effective and current knowledge of multiple ICT infrastructures and applications operating at multiple classifications and supported by multiple suppliers
- Good understanding/knowledge in at least one of the following areas and a good knowledge of the others:
    - Security architecture
    - Cloud hosting and services
    - Security auditing - e.g ISO27001
    - Cryptography
    - ITHCs and vulnerability testing
- Knowledge and understanding of the specific interpersonal and communication skills that are effective in operating with impact in a complex organisation (the emphasis being on building rapport, communicating strongly

through a range of channels, relationship building, and negotiation and influencing skills)
- Demonstrable credibility and integrity to facilitate effective working relationships with stakeholders, senior management and suppliers
- The ability to elicit information quickly and communicate effectively with business people and suppliers in face to face situations, and to analyse information obtained by a variety of formal and informal means
- Ability to design, review and produce proportionate IA documentation
- Current and constantly renewed working knowledge of applicable industry standards e.g. ISO/IEC:27001 and legislation e.g. Data Protection Act 1998

Core Competencies (Civil Service core competences (Level 4))

Leading and communicating
Making effective decisions
Changing and improving
Collaborating and partnering
Managing a Quality Service
Delivering at Pace

Professional Skills

SFIA skills:
Information security (SCTY 5)
Business Risk management (BURM 5)
Security Administration (SCAD 5)

Essential

CCP at minimum Practitioner Accreditor Level (or equivalent - including the new gov sec approach) - new incumbents
CCP, to be achieved within 6 months of appointment for internal personnel, at minimum Practitioner Accreditor Level (or equivalent - including the new gov sec approach)
Information Security/Assurance degree or relevant IA experience/knowledge
Willingness to undergo appropriate clearance
Ability to work closely with project and supplier teams to ensure information security controls and assurances are baked into solutions
Ability to carry out risk assessments and risk management following PACE (Pragmatic/Proportionate, Appropriate and Cost-Effective) in line with HMG policy & guidance
Understanding of HMG policy, guidance esp. requirements / controls around the Government Security Policy / Classification (OFFICIAL, SECRET, TOP SECRET)
Advanced & Specialist Digital Skills

Desirable

Basic knowledge of Security Architecture
ISO/IEC:27001 Auditor / Implementer
Creating policy and guidance
Codes of Connections / IA Conditions
CISSP

CISSP-ISSMP
ISACA-CISM
AMBCS or a willingness to obtain the appropriate qualifications
Any relevant IA skills or qualifications will be considered