This Role Profile has been produced using content provided by the SFIA*plus tool* with amendments to reflect the particular work environment.

The content is general in nature and does not replace the content or purpose of the associated Job Description.

The Role Profile and associated Job Description contents provides a background for career development through the University's Development Appraisal Review (DAR) process.

Role Profile

Information Assurance Manager

Issue 1.1a

January 2014

Job Role:	Information Assurance Manager		
SFIA Status:	Standard	**Status:**	V1.1a

Summary

Develops corporate Information security policy, standards and guidelines. Prepares and maintains organisational strategies that address the evolving business risk and information control requirements. Operates as a focus for Information assurance governance expertise for the organisation, working effectively with strategic organisational functions such as legal experts and technical support to provide authoritative advice and guidance on the requirements for security controls. Ensures architectural principles are applied during design to reduce risk, and advances assurance standards through ensuring rigorous security testing.

SFIA*plus* Skills

Framework » Category » Subcategory	Skill
V5.0 » Strategy and architecture » Information strategy	Information security

Skill Description

The management of, and provision of expert advice on, the selection, design, justification, implementation and operation of information security controls and management strategies to maintain the confidentiality, integrity, availability, accountability and relevant compliance of information systems with legislation, regulation and relevant standards.

Task Description

Provides leadership and guidelines on information assurance security expertise for the organisation, working effectively with strategic organisational functions such as legal experts and technical support to provide authoritative advice and guidance on the requirements for security controls. Provides for restoration of information systems by ensuring that protection, detection, and reaction capabilities are incorporated.

Framework » Category » Subcategory	Skill
V5.0 » Strategy and architecture » Information strategy	Information assurance

Skill Description

The leadership and oversight of information assurance, setting high level strategy and policy, to ensure stakeholder confidence that risk to the integrity of information in storage and transit is managed pragmatically, appropriately and in a cost effective manner.

Task Description

Develops corporate Information security policy, standards and guidelines. Prepares and maintains organisational strategies that address the evolving business risk and information control requirements. Operates as a focus for Information assurance governance expertise for the organisation, working effectively with strategic organisational functions such as legal experts and technical support to provide authoritative advice and guidance on the requirements for security controls. Ensures architectural principles are applied during design to reduce risk, and advances assurance standards through ensuring rigorous security testing.

Task Level Description

Autonomy
Has defined authority and responsibility for a significant area of work, including technical, financial and quality aspects. Establishes organisational objectives and delegates responsibilities. Is accountable for actions and decisions taken by self and subordinates.

Influence
Influences policy formation on the contribution of own specialism to business objectives. Influences a significant part of own organisation. Develops influential relationships with internal and external customers/suppliers/partners at senior management level, including industry leaders. Makes decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance.

Complexity
Performs highly complex work activities covering technical, financial and quality aspects. Contributes to the formulation and implementation of IT strategy. Creatively applies a wide range of technical and/or management principles.

Business Skills
Absorbs complex technical information and communicates effectively at all levels to both technical and non-technical audiences. Assesses and evaluates risk. Understands the implications of new technologies. Demonstrates clear leadership and the ability to influence and persuade. Has a broad understanding of all aspects of IT and deep understanding of own specialism(s). Understands and communicates the role and impact of IT in the employing organisation and promotes compliance with relevant legislation. Takes the initiative to keep both own and subordinates' skills up to date and to maintain an awareness of developments in the IT industry.

Work Activities

SFIA*plus* Work Activity Components	
Details	**Code**
Carries out risk assessment within a defined functional or technical area of business. Uses consistent processes for identifying potential risk events, quantifying and documenting probability of occurrence and impact on the business.	BURM501
Monitors status of risks, and reports status and need for action to senior management.	BURM504
Advises on the evaluation of identified risks (including probability/frequency of occurrence, impact, and severity).	BURM604
Advises on appropriate action, including contingency planning, and countermeasures.	BURM605
Working with the appropriate level of management in the organisation, uses security risk analysis methods, tools and techniques to identify potential exposures of all logical, physical and procedural components of information systems which support critical business processes e.g. single points of failure, lack of effective countermeasures or lack of tested, up-to-date recovery plans. Defines prioritised actions to address the potential exposures to a level approved by the organisation's senior management.	COPL502
Recommends organisational policies and prioritised actions to address the potential exposures to systems supporting higher criticality processes. Co-ordinates and monitors actions to meet agreed time and quality targets for the creation, testing and maintenance of business functions' information systems recovery plans.	COPL504
Working with organisation's management, defines and obtains agreement to strategies for testing and execution of recovery plans to ensure that effective recovery exists for all information systems that support processes critical to the organisation's continued existence.	COPL507
Is familiar with the relevant international standards for information governance and the principles embedded within them.	GOVN502
Reports issues and non-compliances, and proposes and monitors action for resolution.	GOVN503
Maintains awareness of good practice frameworks, within the sphere of Business and IT - capability and maturity models, and relevant standards.	GOVN504
Engages with the implementation of business systems and IT controls to measure performance, manage risk and ensure that IT and the business work together.	GOVN505
Protects and defends information and information systems by defining policies to ensure their availability, integrity, authentication, confidentiality, and non-repudiation. Ensures that policies permit individuals to access only information and	INAS601

network facilities for which they are authorised.	
Assesses legal and best practice issues, and promotes awareness of national and international laws, including those relating to confidentiality, privacy, and copyright.	INAS602
Develops strategies for information assurance, as part of corporate IT governance, including guidelines for information and network users.	INAS603
Ensures architectural principles are applied during design to reduce risk, and advances assurance standards through ensuring rigorous security testing.	INAS604
Determines appropriate and practical performance measures, to ensure that information assurance priorities set by the business can be effectively monitored.	INAS605
In the context of Business Continuity, assesses protection, detection, and reaction capabilities, to determine whether they are sufficient to support restoration of information systems in a secure manner.	INAS606
Guides, encourages, leads, and develops junior colleagues, in the disciplines of Information assurance.	INAS607
Takes overall responsibility for establishing and managing Information assurance strategy and policies in accordance with the ISO/IEC 27000 series of standards.	INAS701
Ensures that the organisation implements processes to take forward the Information assurance strategy and policies.	INAS703
Leads and guides provision of Information assurance requirements across all the organisation’s information and information systems.	INAS704
Drafts and maintains the policy, standards and procedures for compliance with organisational policies and procedures, overall information management strategy, and relevant legislation.	IRMG502
Initiates procedures to improve relations and open communications with and between stakeholders.	RLMT605
Contributes to the definition of an organisation governance framework, which may be under the oversight and/or direction of a project/programme management office.	RLMT608
Develops implementation approach, taking account of current best practice, legislation and regulation. Ensures implementation of information security strategy in automated systems and ensures operations of security systems. Analyses results of investigations into complex, or highly sensitive security violations, to determine whether standards are fit for purpose, are current and are correctly implemented.	SCAD601
Ensures that procedures are in place for investigation of system access enquiries referred by support staff and for handling all enquiries relating to information security, contingency planning as they affect the activities of the organisation, function or department. Authorises implementation of procedures to satisfy new access requirements, or provide effective interfaces between users and service	SCAD603

providers.	
Devises new or revised procedures relating to security control of all IT environments, systems, products or services in order to demonstrate continual improvement in control including creation of auditable records, user documentation and security awareness literature.	SCAD604
Authorises and initiates the provision of training, guidance and support to other security administrators and their agents within the employing organisation, in all aspects of security policy and control.	SCAD605
Reviews new business proposals and planned technical changes and provides specialist guidance on security issues and implications.	SCAD606
Conducts business risk and vulnerability assessments and business impact analysis for well-defined business applications or IT installations.	SCTY402
Conducts security control reviews across a full range of control types and techniques, for business applications and computer installations. Seeks guidance from more experienced or specialised practitioners as required. Recommends appropriate action to management.	SCTY501
Identifies threats to the confidentiality, integrity, availability, accountability and relevant compliance of information systems. Conducts risk and vulnerability assessments of business applications and computer installations in the light of these threats and recommends appropriate action to management.	SCTY502
Conducts investigation, analysis and review following breaches of security controls, and manages security incidents. Prepares recommendations for appropriate control improvements, involving other professionals as required.	SCTY503
Provides authoritative advice and guidance on the application and operation of all types of security controls, including legislative or regulatory requirements such as data protection and software copyright law. Contributes to development of standards and guidelines.	SCTY504
Delivers and contributes to the design and development of specialist IT security education and training to IT and system user management and staff.	SCTY506
Develops information security policy, standards and guidelines appropriate to business, technology and legal requirements and in accordance with best professional and industry practice.	SCTY601
Prepares and maintains a business strategy and plan for information security work which addresses the evolving business risk and information control requirements, and is consistent with relevant IT and business plans, budgets, strategies, etc.	SCTY602
Manages assessment of threats to confidentiality, integrity, availability, accountability and relevant compliance. Takes ownership of security control reviews, business risk assessments, and reviews that follow significant breaches of security controls.	SCTY603

Operates as a focus for IT security expertise for the organisation, providing authoritative advice and guidance on the application and operation of all types of security control, including legislative or regulatory requirements such as data protection and software copyright law.	SCTY604
Keeps in close touch with and contributes to current developments in the technical specialism within employing organisation, own industry and professional and trade bodies. Is fluent at articulating best practice and is a recognised authority in the technical specialism.	TECH502
Promotes the application of the technical specialism within employing organisation and closely associated organisations, such as customers, suppliers and partners, and actively campaigns for appropriate action.	TECH504

Additional Information

The codes used are associated with the SFIA*plus* descriptions and reflect specific sections, for example “SURE” refers to “Supplier Relationship Management”. The specific numerical reference e.g. SURE501 identifies a particular component/element within SURE. Some descriptions have been amended to more accurately reflect the University environment.