THIS PAPER SHOWS HOW THE ISACA CERTIFICATIONS, CISA AND CISM, RELATE TO SFIA

ISACA

ISACA is a non-profit, global membership association with 95,000 constituents in 160 countries. It is a leading provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, ISACA hosts international conferences, publishes the ISACA® Journal, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems.

ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

ISACA also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

Further information about ISACA is available at www.isaca.org

MAPPING

The mapping is arranged under ISACA Certifications. For each relevant SFIA skill, the overall description is shown, together with the skill levels that are appropriate. Where the ISACA qualification does not require all aspect of the SFIA skill a subset has been quoted, with a lower level rating.

The full SFIA framework is available in more than one format, including spreadsheet, at www.sfia.org.uk.

Mapping to SFIA

In the text below, the various components of SFIA are represented thus:

CATEGORY

Subcategory

Skill **Skills code** **Relevant Levels**

Overall description of the skill. [To see the differential definitions of a skills at each of its levels, please refer to the full SFIA framework. at www.sfia.org.uk]

Certified Information Security Manager (CISM)

STRATEGY & ARCHITECTURE

Information strategy

Corporate governance of IT **GOVN** **6-7**

The planning and implementation of initiatives and procedures to ensure that the IT services used by an organisation, and the technology which supports them, deliver value, are efficient in use of resources, and are compliant with all relevant legislation and regulations. The implementation of systems and IT controls to measure performance, manage risk and ensure that IT and the business work together to support the business purpose.

Information management **IRMG** **4-7**

The overall management of the use of all types of information, structured and unstructured, whether produced internally or externally, to support decision-making and business processes. Encompasses development and promotion of the strategy and policies covering the design of information structures and taxonomies, the setting of policies for the sourcing and maintenance of the data content, and the development of policies, procedures, working practices and training to promote compliance with legislation regulating the management of records, and all aspects of holding, use and disclosure of data.

Information security **SCTY** **4-7**

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

Information assurance **INAS** **5-7**

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.

Business/IT strategy and planning

Business risk management **BURM** **5-6**

The planning and implementation of organisation-wide processes and procedures for the management of operational risk arising from any aspect of the use of information technology, including that arising from reduction or non-availability of energy supply or inappropriate disposal of materials, hardware or data.

SOLUTION DEVELOPMENT AND IMPLEMENTATION

Systems development

Systems development management **DLMG** **5-7**

The management of resources in order to plan, estimate and carry out programmes of systems development work to time, budget and quality targets and in accordance with appropriate standards.

SERVICE MANAGEMENT

Service transition

Asset management **ASMG** **4-6**

The management of the lifecycle for service assets (hardware, software, knowledge, warranties etc) including inventory, compliance, usage and disposal, aiming to optimise the total cost of ownership and sustainability by minimising operating costs, improving investment decisions and capitalising on potential opportunities. Knowledge and use of international standards such as ISO/IEC 19770-1 for software asset management and close integration with change and configuration management are examples of enhanced asset management development.

Service operation

Security administration	**SCAD**	**3-6**

The authorisation and monitoring of access to IT facilities or infrastructure in accordance with established organisational policy. Includes investigation of unauthorised access, compliance with relevant legislation and the performance of other administrative duties relating to security management.

Service desk and incident management	**USUP**	**1-6**

The processing and coordination of appropriate and timely responses to incident reports, including channelling requests for help to appropriate functions for resolution, monitoring resolution activity, and keeping clients appraised of progress.

Certified Information Systems Auditor (CISA)

STRATEGY & ARCHITECTURE

Information strategy

Corporate governance of IT	**GOVN**	**3-4**

The planning and implementation of initiatives and procedures to ensure that the IT services used by an organisation, and the technology which supports them, deliver value, are efficient in use of resources, and are compliant with all relevant legislation and regulations. The implementation of systems and IT controls to measure performance, manage risk and ensure that IT and the business work together to support the business purpose.

Information management	**IRMG**	**3**

The development of policies, procedures, working practices and training to promote compliance with legislation regulating the holding, use and disclosure of personal data.

Information security	**SCTY**	**3**

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

Information assurance **INAS** **3-5**

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.

Information analysis **INAN** **3**

The ability to discover and quantify patterns in data of any kind, including numbers, symbols, text, sound and image. The relevant techniques include statistical and data mining or machine learning methods such as rule induction, artificial neural networks, genetic algorithms and automated precis systems.

Business/IT strategy and planning

Business risk management **BURM** **3-4**

The planning and implementation of organisation-wide processes and procedures for the management of operational risk arising from any aspect of the use of information technology, including that arising from reduction or non-availability of energy supply or inappropriate disposal of materials, hardware or data.

Technical strategy and planning

Continuity management **COPL** **3-4**

The provision of service continuity planning and support. This includes the identification of information systems which support critical business processes, the assessment of risks to those systems' availability, integrity and confidentiality and the co-ordination of planning, designing, testing and maintenance procedures and contingency plans to address exposures and maintain agreed levels of continuity. This function should be performed as part of, or in close cooperation with, the function which plans business continuity for the whole organisation.

SOLUTION DEVELOPMENT AND IMPLEMENTATION

Systems development

Systems development management **DLMG** **3-4**

The management of resources in order to plan, estimate and carry out programmes of systems development work to time, budget and quality targets and in accordance with appropriate standards.

Mapping to SFIA

SERVICE MANAGEMENT

Service strategy

IT management **ITMG** **3-4**

The management of the IT infrastructure and resources required to plan for, develop, deliver and support properly-engineered IT services and products to meet the needs of a business. The preparation for new or changed services, management of the change process and the maintenance of regulatory, legal and professional standards. The management of performance of systems and services in terms of their contribution to business performance and in relation to their financial costs and sustainability. The management of bought-in services including, for example, public network, virtual private network and outsourced services. The development of continual service improvement plans to ensure the IT infrastructure adequately supports business needs.

Service design

Capacity management **CPMG** **3-4**

The management of the capability, functionality and sustainability of service components (including hardware, software and network) to meet current and forecast needs in a cost effective manner. This includes dealing with both long-term changes and short-term variations in the level of demand.

Service transition

Change management **CHMG** **3-4**

The management of change to the service infrastructure including service assets, configuration items and associated documentation, be it via request for change (RFC), emergency changes, incidents and problems, so providing effective control and mitigation of risk to the availability, performance, security and compliance of the business services impacted.

Service operation

Security administration **SCAD** **3-4**

The authorisation and monitoring of access to IT facilities or infrastructure in accordance with established organisational policy. Includes investigation of unauthorised access, compliance with relevant legislation and the performance of other administrative duties relating to security management.

Problem management **PBMG** **3-4**

The resolution of incidents and problems throughout the information system lifecycle, including classification, prioritisation and initiation of action, documentation of root causes and implementation of remedies.

Mapping to SFIA

PROCUREMENT & MANAGEMENT SUPPORT

Quality management

Technology audit **TAUD** **3-6**

The independent, risk-based assessment of the adequacy and integrity of controls in information processing systems, including hardware, software solutions, information management systems, security systems and tools, and communications technologies - both web-based and physical. The structured analysis of the risks to achievement of business objectives, including the risk that the organisation fails to make effective use of new technology to improve delivery and internal effectiveness. Assessment of the extent to which effective use has been made of techniques and tools to achieve sustainability and business continuity.