

# Cybersecurity Skills

## Information security SCTY

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

### Level 3

Communicates information security risks and issues to business managers and others. Performs basic risk assessments for small information systems. Contributes to vulnerability assessments. Applies and maintains specific security controls as required by organisational policy and local risk assessments. Investigates suspected attacks. Responds to security breaches in line with security policy and records the incidents and action taken.

## Information governance IRMG

The overall governance of how all types of information, structured and unstructured, whether produced internally or externally, are used to support decision-making, business processes and digital services. 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 all aspects of holding, use and disclosure of data.

### Level 4

Ensures implementation of information and records management policies and standard practice. Ensures effective controls are in place for internal delegation, audit and control relating to information and records management. Assesses and manages risks around the use of information. Provides reports on the

consolidated status of information controls to inform effective decision making. Recommends remediation actions as required. Ensures that information is presented effectively.

## Penetration testing PENT

The assessment of organisational vulnerabilities through the design and execution of penetration tests that demonstrate how an adversary can either subvert the organisation's security goals or achieve specific adversarial objectives. Penetration testing may be a stand-alone activity or an aspect of acceptance testing prior to an approval to operate. The identification of deeper insights into the business risks of various vulnerabilities.

### Level 4

Maintains current knowledge of malware attacks, and other cyber security threats. Creates test cases using in-depth technical analysis of risks and typical vulnerabilities. Produces test scripts, materials and test packs to test new and existing software or services. Specifies requirements for environment, data, resources and tools. Interprets, executes and documents complex test scripts using agreed methods and standards. Records and analyses actions and results. Reviews test results and modifies tests if necessary. Provides reports on progress, anomalies, risks and issues associated with the overall project. Reports on system quality and collects metrics on test cases. Provides specialist advice to support others.

## Digital forensics DGFS

The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings including computer-related evidence in support of security vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

### Level 4

Contributes to digital forensic investigations. Processes and analyses evidence in line with policy, standards and guidelines and supports production of forensics findings and reports.

## Business risk management BURM

The planning and implementation of organisation-wide processes and procedures for the management of risk to the success or integrity of the business, especially those arising from the use of information technology, reduction or non-availability of energy supply or inappropriate disposal of materials, hardware or data.

### Level 4

Investigates and reports on hazards and potential risk events within a specific function or business area.

## Data management DATM

The management of practices and processes to ensure the security, quality, integrity, safety and availability of all forms of data and data structures that make up the organisation's information. The management of data and information in all its forms and the analysis of information structure (including logical analysis of taxonomies, data and metadata). The development of innovative ways of managing the information assets of the organisation.

### Level 4

Takes responsibility for the accessibility, retrievability, security, quality, retention and ethical handling of specific subsets of data. Assesses the integrity of data from multiple sources. Provides advice on the transformation of data/information from one format or medium to another. Maintains and implements information handling procedures. Enables the availability, integrity and searchability of information through the application of formal data and metadata structures and protection measures. Manipulates specific data from information services, to satisfy defined information needs.