# Toolkit E

## References to International Standards

As also discussed in Principle 4, there are a number of international standards and regulatory bodies that deal with security of information and the systems that handle and process it. This is by no means to be an exhaustive list and represent for the most part the primary references. Other references to authoritative guidance may be cited earlier in this document.

The NIST Cyber Security Framework was designed with the intent that individual businesses and other organisations use an assessment of the business risks they face to guide their use of the framework in a cost-effective way. The framework is divided into three parts: The Framework Core, Framework Implementation Tiers and Framework Profiles:

- The Framework Core is a set of activities, outcomes and references that detail approaches to aspects of cyber security. The core comprises five functions, which are subdivided into 22 categories (groups of cyber security outcomes) and 98 subcategories (security controls).
- Framework Implementation Tiers are used by an organisation to clarify for itself and its partners how it views cyber security risk and the degree of sophistication of its management approach.
- A Framework Profile is a list of outcomes that an organisation has chosen from the categories and subcategories, based on its business needs and individual risk assessments.

**Core functions, categories, subcategories and informative references**

The five Framework core functions are:

- Identify – Develop the organisational understanding to manage cyber security risk to systems, assets, data and capabilities.
- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cyber security event.
- Respond – Develop and implement the appropriate activities to take action regarding a detected cyber security event.
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired because of a cyber security event.

Each function is divided into categories – groups of cyber security outcomes that relate to particular activities. Examples include: Asset Management, Access Control and Detection Processes.

Subcategories further divide a category into specific outcomes of technical and/or management activities (security controls). Examples include: External information systems are catalogued, Data-at-rest is protected, and Notifications from detection systems are investigated.

**ISO-International Organisations for Standardisation**

- **ISO 27000** series to address standards that enable organisations to implement processes and controls that support the principles of information security.
- **ISO/IEC 27001 (2013)** is the international standard for information security management. It is a rigorous and comprehensive specification for protecting and preserving the confidentiality, integrity and availability of an organisation's information assets. The Standard offers a set of 114 best-practice security controls that can be applied based on the risks you face, and implemented as part of a broad organisational structure to achieve externally assessed and certified compliance.
- **ISO 17799 (2005)** a Code of Practice for Information Security management, is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce.

**OECD Guidelines for the Security of Information Systems (2002)**
The Organisation for Economic Co-operations and Development's (OECD's) *Guidelines for the Security of Information Systems* is designed to assist countries and enterprises to construct a framework for security of information systems.

**COBIT® - Control Objectives for Information and related Technology**, developed and promoted by the IT Governance Institute (ITGI)

- **COBIT® 4.0 (2005)** starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives. In addition to promoting process focus and process ownership, COBIT looks at fiduciary, quality and security needs of enterprises and provides seven information criteria that can be used to generically define what the business requires from IT: effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance.

  COBIT further divides IT into 34 processes belonging to four domains (Plan and Organise [PO], Acquire and Implement [AI], Deliver and Support [DS], and Monitor and Evaluate [ME]). The COBIT framework addresses information security issues of concern in more than 20 processes. However, the four processes that are most directly related to information security are:

  - PO6—Communicate management aims and directions.
  - PO9—Assess and manage IT risks.
  - DS4—Ensure continuous service.
  - DS5—Ensure systems security.

  For each process, a high-level control objective is defined: Identifying which information criteria are most important in that IT process; Listing which resources will usually be leveraged; Providing considerations on what is important for controlling that IT process.

  COBIT further provides more than 200 detailed control objectives for management and IT practitioners who are looking for best practices in control implementation, as well as management guidelines and maturity models building on these objectives.

COBIT includes a management and governance layer, providing management with:

- Performance measurement elements (outcome measures and performance drivers for all IT processes)
- A list of key activities that provides succinct, non-technical best practices for each IT process
- A maturity model to assist in benchmarking and decision making for control over IT

- **COBIT Security Baseline (2004)**
  Also published by ITGI, it addresses security in addition to the risks of the use of IT. Using the COBIT framework, the guidance focuses on the specific risks of IT security useful for all users—home, small to medium enterprises, and executives and board members of larger organisations.

**National Association of Corporate Directors (NACD) (U.S.)**
**NACD Director's Handbook on Cyber-Risk Oversight**
The NACD Director's Handbook on Cyber-Risk Oversight is built around five core principles that are applicable to board members of public companies, private companies, and nonprofit organisations of all sizes and in every industry sector. The Handbook was the first non-government resource to be featured on the U.S. Department of Homeland Security's US-CERT C3 Voluntary Programme website.

**European Banking Association**
**Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)**
These Guidelines are addressed to competent authorities and are intended to promote common procedures and methodologies for the assessment of the Information and Communication Technology (ICT) risk under the supervisory review and evaluation process (SREP), referred to in Article 97 of Directive 2013/36/EU1, as regards the banking sector.
In particular, these Guidelines drawn up pursuant to Article 107(3) of Directive 2013/36/EU, supplement and further specify criteria for the assessment of ICT risk as part of operational risk put forward in the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)2 (from here on 'EBA SREP Guidelines').

**ISA- ANSI Integrated Approach to Managing Cyber Risk**
One of the first multi-stakeholder models developed was created by the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI) in their joint 2008 publication The Financial Management of Cyber Risk: *50 Questions Every CFO Should Ask*.

**Standard of Good Practice for Information Security (2005)**
The Information Security Forum's (ISF's) *Standard of Good Practice for Information Security* is based on research and practical experience of members. 'The standard addresses information security from a business perspective, providing a practical basis for assessing an organisation's information security arrangements. It focuses on the arrangements that should be made by leading organisations to keep the business risks associated with critical information systems under control'. Each area is broken down into a number of detailed sections, totaling 135 appropriate controls.