BCS Foundation Certificate in Information Security Management Principles

ISO – International Standards Organisation / IEC - International Electrotechnical Commission References:

ISO 9001:2015 Quality management systems

ISO/IEC 27000:2016 Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems

ISO/IEC 27002:2013 Information technology – Security techniques – **Code of practice (CoP)** for information security controls

ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation

ISO/IEC 27005:2011 Information technology – Security techniques – **Information Security Risk Management**

ISO 31000:2009 Enterprise Risk management – Principles and guidelines

Comment: ISO 27000 is the overall series for Information Technology

ISO 27001 ISMS was previously called British Standards (BS) BS:7799, then evolved into ISO 27001: The **Statement of Applicability (SoA)** summarises your organisation's position on each of the 114 information security controls outlined in Annex A of ISO 27001: Annex A, outlines each control in one or two sentences, whereas ISO 27002 dedicates approx. of one page per control to augment the **policy**.

ISO/IEC 20000:2018 Information technology — Service management (ITIL)

The four components of the cycle are known as **PDCA or Plan, Do, Check or Study and Act:** Reales to ISO 27001 continual improvement (clause 10.2)

ISO 15408 Common Criteria

Comment: The Common Criteria provides a level of assurance against technology products on an **Evaluation Assurance Level (EAL1 through EAL7)**

The EAL levels are:

EAL1 - functionally tested *Weakest

EAL2 - structurally tested

EAL3 - methodically tested and checked

EAL4 - methodically designed, tested, and reviewed *Economic Benchmark

EAL5 - semi-formally designed and tested

EAL6 - semi-formally verified design and tested

EAL7 - formally verified design and tested *Strongest

Protection Profile (PP)	Target of Evaluation (ToE)	Security Target (ST)
Template used to define a standard set of security requirements for a particular class of related products. A protection profile serves as a reusable template of security requirements. Depending on the Target of Evaluation, multiple profiles may be used at once.	The device or system to be reviewed for CC certification	Explicitly stated set of requirements specific to the capabilities of the product under evaluation.

Cloud:

ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

---

ISO 15489 Information and documentation – Records management and retention of records

ISO 19011:2018 Guidelines for auditing management systems
Comment: Referred to within ISO 27xxx: Lead Auditing Courses

ISO 22301:2012 Societal security – Business continuity management systems – Requirements

ISO/IEC 27031:2011 Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity

ISO/IEC 17025 Testing and Calibration Laboratories (ISO 17025 is a **mandatory standard for Digital Forensics laboratories**)

ISO/IEC 27035 Information technology - Security techniques - Information security incident management

- ISO/IEC 27035-1:2016 Part 1: Principles of incident management
- ISO/IEC 27035-2:2016 Part 2: Guidelines to plan and prepare for incident response

Operational Technology / Industrial Controls Systems (ICS)

ISA99 Industrial Automation and Control Systems Security

ISA/IEC 62443 Series: Industrial automation and control systems