Information Security Risk Management Standard

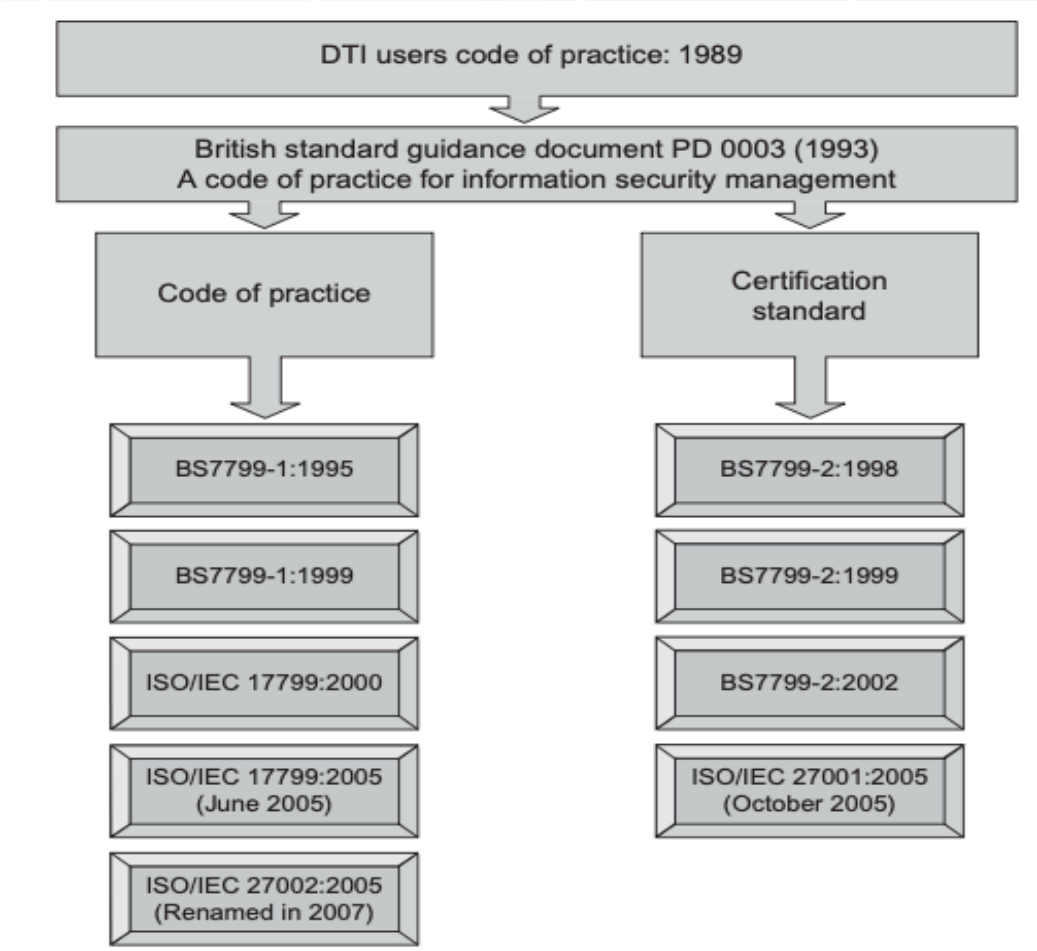
Dr. Muhammad Said Hasibuan
Materi diberikan Tgl 1 Mei 2021

5 Cakupan IT RISK

1. (Ongoing), Identification of threats, vulnerabilities, or (risk), event impacting the set of IT assets owned by the organization.
2. Risk assessment.
3. Risk mitigation planning
4. Risk mitigation implementation
5. Evaluation of the mitigations effectiveness

I.3

Timeline Leading to ISO code of practise



ISO/IEC 13335

- ISO 13335 (originally a set of technical reports) embodies a set of guidelines for the management of IT security.
  - ISO 13335-1:2004 : IT-Security Technique- Management of information and communications technology security.

    Concepts and models for information and communicaton technology security management.
  - ISO 13335-2: Management of Information and communications technology security.

    replace: 13335-3: 1998. 13335-4: 2000

ISO 13335

- ISO 13335-3:1998 : Technique for the management of IT Security.
  - Identification of assets.
  - Valuation of assets and establishment of dependencies between assets.
  - Threat and vulnerability assessment on assets within scope of the risk assessment
  - Identification of exiting or planned safeguards.
  - Assessment of risk exposures.

ISO 17799 (ISO 27002:2005)

- Biasanya ISO 17799 dibagi menjadi 2 yaitu: ISO 27002 dan ISO 27001 dengan spesifikasi untuk Information Security Management System (ISMS).

ISO 27000 Series

- Information Security
- Risk Management
- Management System

ISMS

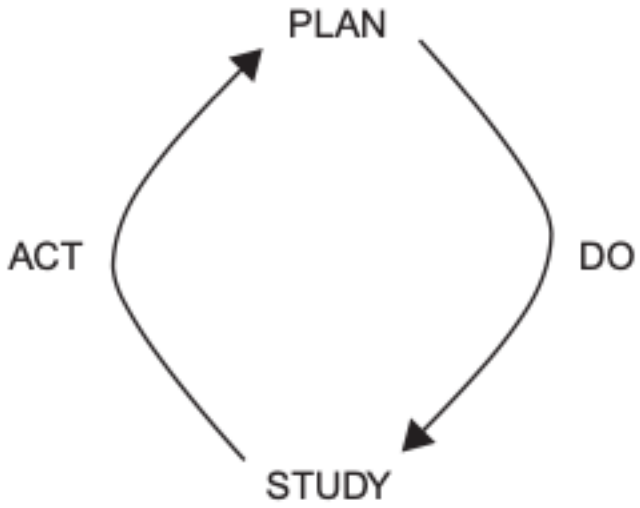
- ISMS aims at protecting the confidentially, Integrity, and avaibility.

TABLE 3.2. ISO/IEC 27000 Series of Standards

ISO/IEC 27000	(under development) Standard will provide an overview/ introduction to the ISO27k standards as a whole plus the specialist vocabulary used in ISO27k.
ISO/IEC 27001:2005	ISMS requirements specification used for the certification of an organization's ISMS.
ISO/IEC 27002:2005	Standard that encompasses the code of practice for information security management describing a set of information security control objectives and a set of generally accepted best practice security controls.
ISO/IEC 27003	(under development) Standard will provide implementation guidance for ISO/IEC 27001.
ISO/IEC 27004	(under development) Standard will be an information security management measurement standard recommending metrics to facilitate an improvement in the effectiveness of an ISMS.
ISO/IEC 27005:2008	A key information security risk management standard that provides advice on information security risk management.
ISO/IEC 27006:2007	A guide to the certification or registration process for accredited ISMS certification or registration bodies.
ISO/IEC 27007	(under development) Standard will be a guideline for auditing ISMSs.
ISO/IEC TR 27008	(under development) Standard will provide guidance on auditing information security controls.
ISO/IEC 27009	(under development) Standard will provide guidance on information security governance.
ISO/IEC 27010	(under development) Standard will provide guidance on information security management for sector-to-sector communications.
ISO/IEC 27011	(under development) Standard (also known as X.1051) will provide information security management guidelines for telecommunications.
ISO/IEC 27012	(under development) Standard will provide information security management systems guidance for e-government applications
ISO/IEC 27013	(under development) Standard will provide information security management systems guidance for financial services organizations

	continuity.
ISO/IEC 27032	(under development) Standard will provide guidelines for cybersecurity.
ISO/IEC 27033	(under development) Standard will replace the multi-part ISO/IEC 18028 standard on IT network security.
ISO/IEC 27034	(under development) Standard will provide guidelines for application security.
ISO/IEC 27035	(under development) Standard will replace ISO TR 18044 on security incident management.
ISO 27799	Recommendation that provides health sector specific ISMS implementation guidance.

PDSA



PLAN: Plan ahead for change. Analyze and predict the results.
DO: Execute the plan, taking small steps in controlled circumstances
STUDY: CHECK, study the results.
ACT: Take action to standardize or improve the process.

FIGURE 3.2 The Deming (PDCA) cycle

☺ Terima Kasih ☺