Security Compliance Frameworks

Requirements from

- Government regulations.
- Organizations' activities processing (not only financial and personal) information.
- Management policies, business conduct and processes.

Specifications developed by

- Government.
- Private/independent organizations.

Government laws

- US
  - SOX Section 404
  - HIPAA/HITECH
  - GLBA/FSRR
  - FISMA
  - CMVP
- PH
  - BSP - MORB, Sections 176/705

US Federal Regulatory Agencies' privacy form model

- Makes it easier for consumers to understand how financial institutions collect and share their information.
- Notify consumers of their information-sharing practices and
- Inform consumers of their right to opt out of certain sharing practices.
- Allows consumers to easily compare the privacy practices of different financial institutions.
- Developed jointly by the Board of Governors of the Federal Reserve System, Commodity Futures Trading Commission, Federal Deposit Insurance Corporation, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, and Securities and Exchange Commission.

US cybersecurity efforts

- Cybersecurity Frameworks
- Computer Security Resource Center Special Publications

Standardization

- Any organization whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise producing technical standards that are intended to address the needs of some relatively wide base of affected adopters.
- Most standards are voluntary in the sense that they are offered for adoption by people or industry without being mandated in law.
- Some standards become mandatory when they are adopted by regulators as legal requirements in particular domains.

Formal standard

- Refers specifically to a specification that has been approved by a standards setting organization.

De jure standard

- Refers to a standard mandated by legal requirements or refers generally to any formal standard.

De facto standard

- Refers to a specification (or protocol or technology) that has achieved widespread use and acceptance – often without being approved by any standards organization (or receiving such approval only after it already has achieved widespread use).

International (developing) standardization bodies

- WSC
  - ITU
  - IEC
  - ISO
- IETF
- W3C

Regional standards organizations

- European Committee for Standardization (CEN)
- European Committee for Electrotechnical Standardization (CENELEC)
- European Telecommunications Standards Institute (ETSI)
- Institute for Reference Materials and Measurements (IRMM) in Europe
- Pacific Area Standards Congress (PASC)
- Pan American Standards Commission (COPANT)
- African Organization for Standardization (ARSO)
- Arabic industrial development and mining organization (AIDMO)

National standardization representatives

- US: ANSI, NIST
- UK: BSI
- AU: SAI
- NZ: SNZ
- PH: BPS

Standards developing organizations

- IEEE
- ANSI
- JISC

Standards development process

- When an organization develops standards that may be used openly, it is common to have formal rules published regarding the process.
- This may include:
  - Who is allowed to vote and provide input on new or revised standards,
  - What is the formal step-by-step process,
  - How are bias and commercial interests handled,
  - How negative votes or ballots are handled,
  - What type of consensus is required.

Standards compliance

- PCI DSS
- ISO 27001

Advance intelligence compasses

"One hacker, plus one modem causes an enemy damage and losses almost equal to those of a war. Because it has the breadth and secrecy of trans-level combat, this method of individual combat very easily achieves results on the strategic and even war policy levels." -- *Qiao Liang and Wang Xiangsui*

- INFOCON, NIST-NVD (USG)
- THREATCON (Symantec)
- ATLAS (Arbor)
- CVE (Mitre, US-NCSD funded)