Security +

Laws, Standards, and Organizations

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

Types of Standards

Regulatory
- Based on laws and regulations

Non-regulatory
- Common standards and best practices that organizations can follow

National vs international
- Some standards are international in scope and some are national

Industry specific
- Implemented by a vendor or group of vendors related to an industry

Vendor specific guidelines
- Manuals and guidelines from software / hardware vendors

Laws

Health Insurance Portability and Accountability Act (HIPAA)
- Purpose is to protect PII (personal identifiable information)

Sarbanes Oxley (SOX)
- Purpose is to maintain legal regulation of maintaining financial records for a certain number of years

Gram-Leach Bliley Act Financial Services Modernization Act (GBLA)
- Includes a financial privacy rule
- Requires financial institutions to provide consumers with a privacy notice explaining what information they collect

Organizations Quick List

ISO - International Organization for Standards (international)
IEC - International Electrochemical Commissions (US national)
IEEE - Institute for Electronics and Electrical Engineers
IETF - Internet Engineering Task Force
ANSI - American National Standards Institute
ONC - National Coordinator for Health Information Technology
HHS - US Department of Health and Human Services
OCR - Office for Civil Rights
HIPAA Security Risk Assessment SRA
MITRE Corporation
- Maintains CVE Common Vulnerability and Exposures

NIST - National Institutes for Science and Technology
SANS - SysAdmin, Audit, Network and Security
US DOD - US Department of Defence
The Open Group
TCG - The Trusted Computing Group
DISA - Defence Information System Agency
- Combat support agency of the Department of Defence

Organizations Detailed List

NIST National Institute for Science and Technology
- **NIST SP 800-30** Guide for Conducing Risk Assessments
- **NIST SP 800-47** Security Guide for Interconnecting Information Technology Systems
- **NIST SP 800-52** Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- **NIST SP 800-53** Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-61** Computer Security Incident Handling Guide
- **NIST SP 800-78** Cryptographic Algorithms and Key Sizes
- **NIST SP 800-88** Guidelines for Media Sanitization
- **NIST SP 800-94** Guide to Intrusion Detection and Prevention Systems
- **NIST SP 800-115** Technical Guide to Information Security Testing and Assessment
- **NIST SP 800-122** Guide to Protecting The Confidentiality of Personally Identifiable Information (PII)
- **NIST SP 800-124** Guidelines for Managing the Security of Mobile Devices in the Enterprise
- **NIST SP 800-162** Guide to Attribute Based Access Control (ABAC)

FIPS Federal Information Processing Standard
- FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

IETF Internet Engineering Task Force

ITU-T
- International Telecommunications Union’s Standardization sector

ISACA The Risk IT Framework

Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
- International standard for computer security certification
- Allows vendors to make claims about the security attributes of their products

    - The criteria for an OS to be considered a trusted OS.
    - Common Criteria uses:
        - Target of evaluation (**TOE**)
        - Protection Profile (**PP**)
        - Security Target (**ST**)
        - Produces a Security Functional Requirement (**SFR**)
        - The result post-testing is a security assurance requirements (**SAR**) which describes the measures during development and evaluation of a product to assure compliance with the claimed security functionality

ITU Telecommunication Standardization Sector

- Coordinates standards for telecommunications and Information Communication Technology such as X.509, Y.3172, and H.264/MPEG-4 AVC

IANA The Internet Assigned Numbers Authority

- Responsible for coordinating some of the key elements that keep the Internet running smoothly
- Domain names
- IP and ASN (Autonomous System Number) number resources
- Protocol Assignments

US Department of Defence

- Cloud Computing Security Requirements Guide
- Trusted Computer System Evaluation Criteria (TCSEC)

EISA: Enterprise Information Security Architecture:

- Analyzes security systems in place and includes industry-standard frameworks such as:
    - NIST RMF, and includes regulatory and non-regulatory influences (national and international laws, standards, best-practices, standard operating procedures)

Other Industry Standards and Frameworks

PCI-DSS Payment Card Industry Data Security Standard

FCRA Fair Credit Reporting Act

- Requires employers to obtain written permission from prospective employee before conducting a credit check

OWASP Cheatsheet series

- Preventing XSS attacks
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.htm

O-TTPS Open Trusted Technology Provider Standard (ISO/IEC 20243)

- Provides organizations the tools to create best practices for supply chain security using commercial off the shelf (COTS) and information and

communication technology (ICT)

CVE Common Vulnerability and Exposures

NVD National Vulnerability Database

SCAP Security Content Automation Protocol

- A multi-purpose framework of specifications that supports automation of:
  - Configuration
  - Vulnerability and patch checking
  - Technical control compliance activities
  - Security measurement
- Also includes the risk scores for CVE

COBIT Control Objectives for Information and Related Technologies

OWASP Web Application Security Project

OSINT Open source Intelligence

ISO 73:2009 - ??? Risk management Framework

Projects In Controlled Environments (PRINCE2)

ITSEC Information Technology Security Evaluation Criteria

- Introduced in 1990 in Europe
- Largely replaced by **Common Criteria**

Secure Electronic Transaction SET

- https://en.wikipedia.org/wiki/Secure_Electronic_Transaction
  - Developed in 1996 by SET Consortium (VISA, MasterCard, IBM, Netscape, RSA, VeriSign, and others)
  - Not used anymore - failed to gain attraction in the market
  - A communications protocol standard for securing credit card transactions over networks, specifically, the Internet
  - Supported initially by MasterCard, Visa, Microsoft, Netscape, and others