Security Frameworks

Robert M. Slade, MSc, CISSP
rmslade@shaw.ca, rslade@vcn.bc.ca,
rslade@computercrime.org

http://victoria.tc.ca/techrev/rms.htm

Security frameworks

- Guidelines
- Principles
- Standards
- Frameworks/breakdowns/structures
- Checklists
- Software
- “Best Practice”
- Audit guidelines/outlines
- Legislation
- Reporting standards
- Product evaluation

Security frameworks

- Financial reporting instructions
  - Sarbanes-Oxley/Sarbox/SOX, COSO, Turnbull, Basel II
  - Reliability of reported finances
    - Information systems source of reports
  - Internal controls
    - Information system controls
    - Insider attack, fraud?

Security framework types

- Governance
  - Breakdowns/frameworks
- Checklists
  - Controls lists
- Risk management
  - Infosec, business, and banking
  - Process oriented
- Audit and assurance

	Deterrent	Preventive	Detective	Corrective	Recovery	Compensating
Administrative	Policy	User registration procedure	Review violation reports	Termination	DR plan	Supervision, Job rotation
Technical	Warning banner	Password based login, IPS	Logs, IDS	Unplug, Isolate, Terminate connection, Checkpoint restart	Tape backups, fault tolerance, RAID	Diskless workstations, thin clients
Physical	Beware of dog sign	Fence	Sentry, CCTV	Fire Extinguisher	Reconstruction, Rebuild	Layered defense

Weaknesses

- Content limitations
- Define “Secure”
- “Best Practice”

BS 7799/ISO 27000 family

- BS 7799 Part 1
  - ISO 17799, ISO 27002
  - code of practice
    - 133 controls, 500+ detailed controls
- BS 7799 Part 2
  - ISO 27001
  - Information Security Management System (ISMS)
- ISO 27000
  - ISMS fundamentals and vocabulary, umbrella
  - 27003 ISMS implementation guide, 27004 ISM metrics, 27005 infosec ris k

    management, 27006 certification agencies, 27007 audit

COBIT

- ISACA (formerly I n formation Systems Audit and Control Association)
- Four phases/domains:
  - Planning and Organization
  - Acquisition and Implementation
  - Delivery and Support
  - Monitoring

Common Criteria (CC)

- Common Crite r ia for Information Technology Security Evaluation
- ISO 15408
  - not a security framework
  - not even evaluation standard
- Framework for specification of evaluation
  - Protection Profile (PP)
  - Evaluation Assurance Level (EAL 1-7)

FISMA

- Federal Information Systems Management Act – US
  - National Information
    A
    s
    surance Certification and Accreditation Process (NIACAP)
  - National Institute of Standards and Technology outline,
  - Defense Information
    Technology
    S
    y
    stems Certification and Accreditation Process (DITSCAP)
  - Director of Central Intelligence Directive 6/3

Information Security Forum (ISF)

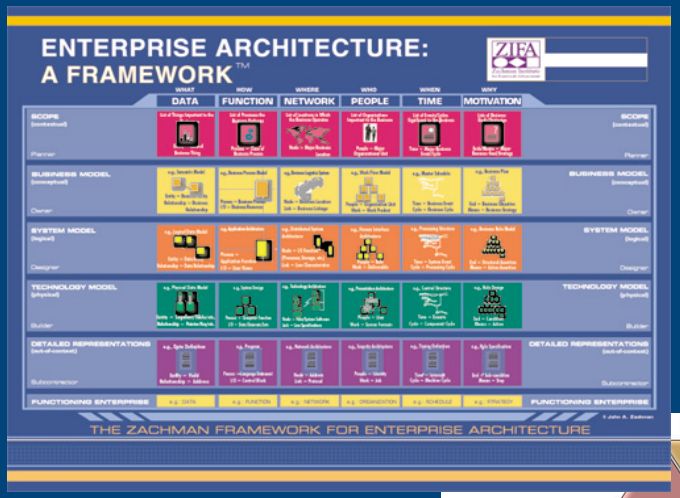
- Standard of Good Practice for Information Security
- 5 "aspects"
  - Security Management
  - Critical Business Applications
  - Computer Installations
  - Networks
  - Systems Development
- broken out into 30 "areas," and 135 "sections"
- www.securityforum.org
- http://www.isfsecuritystandard.com/pdf/standard.pdf

ITIL

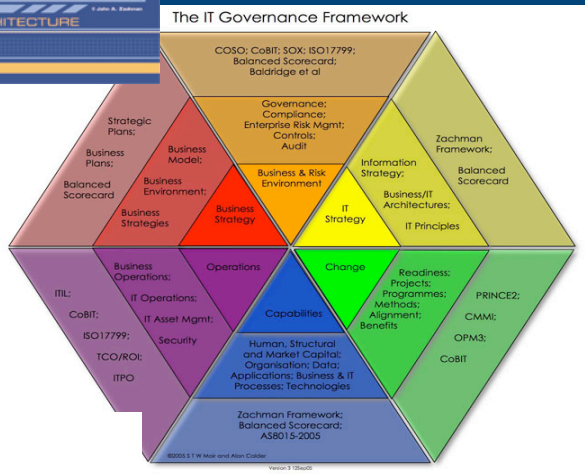
- Information Technology Infrastructure Library
  - management guidelines
    - Incident response
    - Problem management
    - Change management
    - Release management
    - Configuration management
    - Service desk management
    - Service level management
    - Availability
    - Capacity management
    - Service continuity
    - IT financials
    - IT workforce/HR management
  - security removed in recent revision
  - influenced BS 15000, ISO 20000

Management frameworks

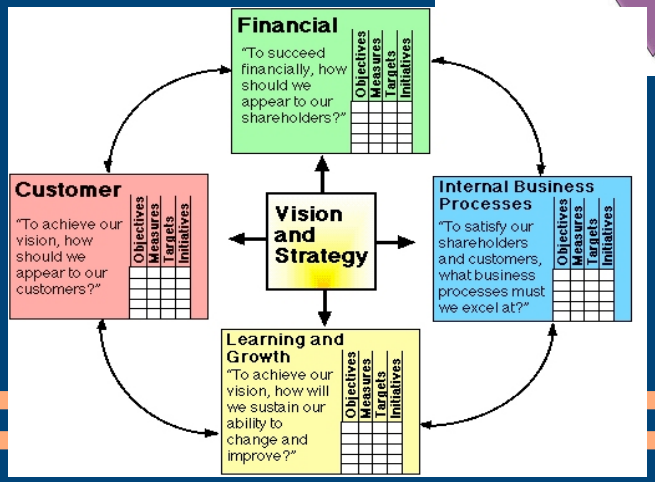
- Zachman Framework



- Calder-Moir Framework



- Balanced Scorecard



NIST

- library of freely available resources
  - http://csrc.nist.gov
    - Information Security Handbook: A Guide for Managers 800-100
    - Recommended Security Controls for Federal Info Systems 800-53
    - Guide to Information Technology Security Services 800-35
    - Risk Management Guide for Information Technology Systems 800-30
    - Engineering Principles for Information Technology Security 800-27
    - Guide for Developing Security Plans for Federal Info Systems 800-18
    - Generally Accepted Principles and Practices for Securing Information Technology Systems 800-14
    - An Introduction to Computer Security: The NIST Handbook 800-12
- Security Self-Assessment Guide for Information Technology Systems 800-26

OCTAVE

- Operationally Critical Threat, Asset, and Vulnerability Evaluation
- Carnegie Mellon University
- risk management

Quality

- TQM
  - Deming and PDCA
- Six Sigma
- ISO 9000

Securities and Financial

- Basel II
  - bank solvency
  - “operational risk”
- COSO
  - Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management Integrated Framework
  - internal controls
- SOX

COSO

- 3-D grid
  - scope
  - range
  - activities
- 128 “areas”

PCI

- Payment Card Industry Data Security Stand
  a
  rds (PCI DSS, generally referred to simply as PCI)
- 6 Control Objectives
- 12 Requirements

PCI Control Objectives

- build and maintain a secure network 1,2
- protect cardholder data 3,4
- maintain vulnerability management 5,6
- implement strong access control 7, 8, 9
- monitor and test networks 10, 11
- maintain inforsec policy 12

PCI Requirements

- 1 - maintain firewall configuration to protect card data
- 2 - no vendor default password etc.
- 3 - protect stored data
- 4 - encrypt transmitted data on public net
- 5 - use and maintain AV
- 6 - develop secure apps and systems
- 7 - access by need to know
- 8 - assign unique ID
- 9 - restrict physical access
- 10 - monitor access to resources and data
- 11 - test security
- 12 - maintain security policy

Security Governance

- part of “CISO Toolkit” (Fred Cohen)
- structured
  accord
  i
  ng to business concepts, rather than security topics
  - easier for businesspeople to understand
- checklist in book form
  - 900 checks

SSE-CMM

- Syst
  e
  m
  s Security Engineering Capability Maturity Model
  - Basic (chaotic/informal)
  - Planned and verified
  - Well defined and coordinated
  - Measurable and quantitatively controlled
  - Constantly improving (optimizing)

Unified Compliance Framework

- Compares most checklist frameworks
- 12 areas
- 2-300 controls
  - HTML version free online
  - Spreadsheets $1,000 - $10,000
- http://www.unifiedcompliance.com/

Which one?

- no framework best for all
  - no one-size-fits-all in security
- no framework sole source for any enterprise
  - multiple frameworks, multiple perspectives
- Which one addresses a viewpoint you haven't used?

Security Frameworks

Robert M. Slade, MSc, CISSP
rmslade@shaw.ca, rslade@vcn.bc.ca,
rslade@computercrime.org

http://victoria.tc.ca/techrev/rms.htm