



## Security is about Risk Mitigation

***Risk*** is function of the ***likelihood*** of a given ***threat***-source's exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event of the organizations.

NIST SP 800-30

---

# Legal Issues in Technology

Data Security, Consumer Privacy & Identity Theft



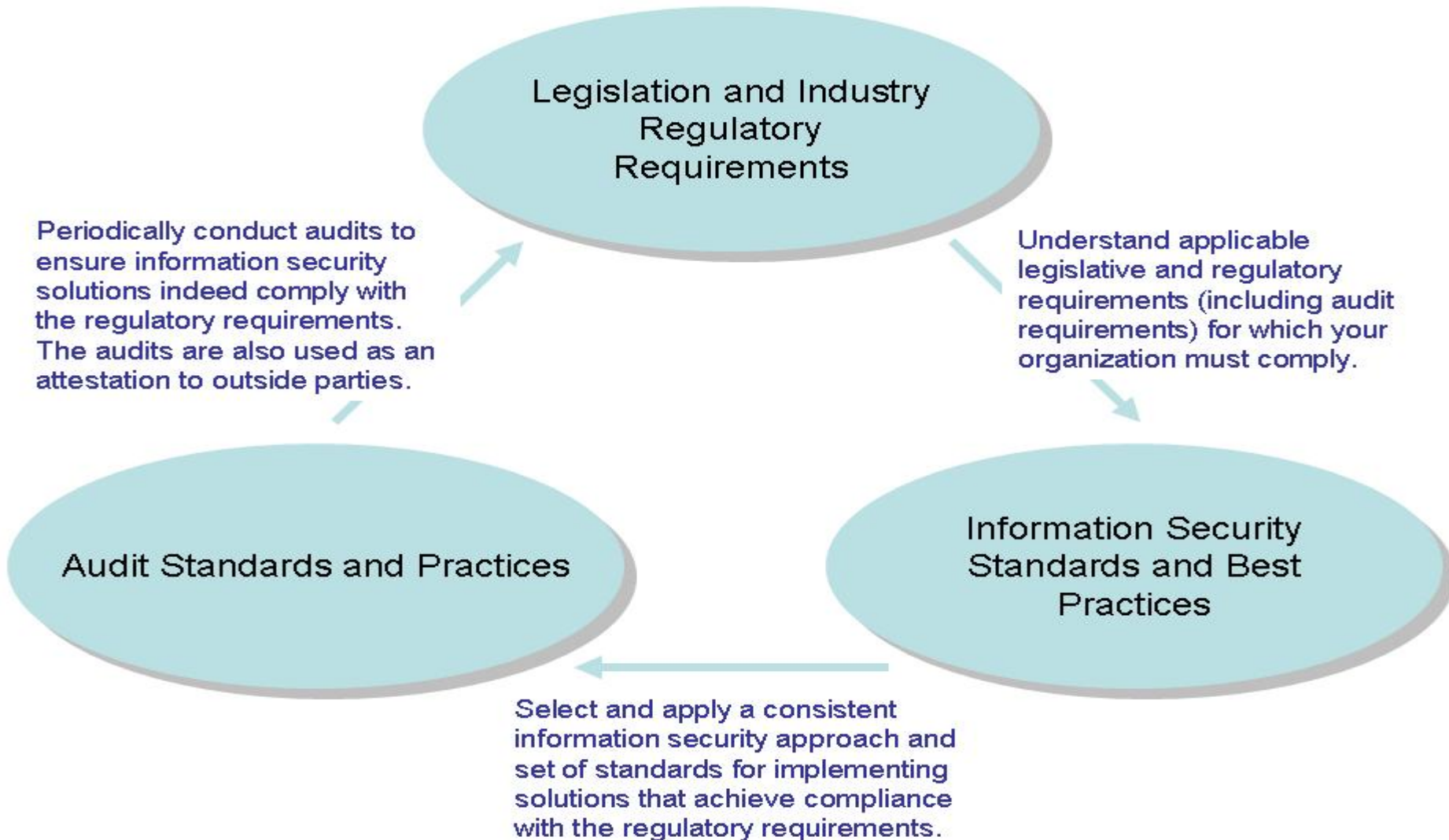
<b>Threat</b>	<b>Vulnerability</b>	<b>Risk</b>
Rogue Consumer	Poor Authentication	Mortgage entity may divulge PI to a person who is posing as a legitimate consumer.
	Minimal Event Logging	Mortgage entity is unaware of masquerader's tactics in collecting PI.
Hacker	Collecting Unnecessary PI	Hacker gains access to additional PI that is not even needed by mortgage entity.
	Poor Authentication	Hacker gains access to computing systems (consumer and mortgage entity) containing PI.
	Minimal Security (Mortgage Entity)	Hacker gains access to mortgage entity networks and computing systems containing PI.
	Minimal Security (Consumer)	Hacker gains access to consumer computing environment containing PI (e.g., cached data).
	Minimal Event Logging	Hacker's activities in collecting PI go unnoticed by mortgage entity.
Eavesdropper	Minimal Security	Eavesdropper is capable of intercepting PI that is poorly protected, or not protected at all (e.g., weak cryptography, insecure protocols).

## Safeguards / Countermeasures

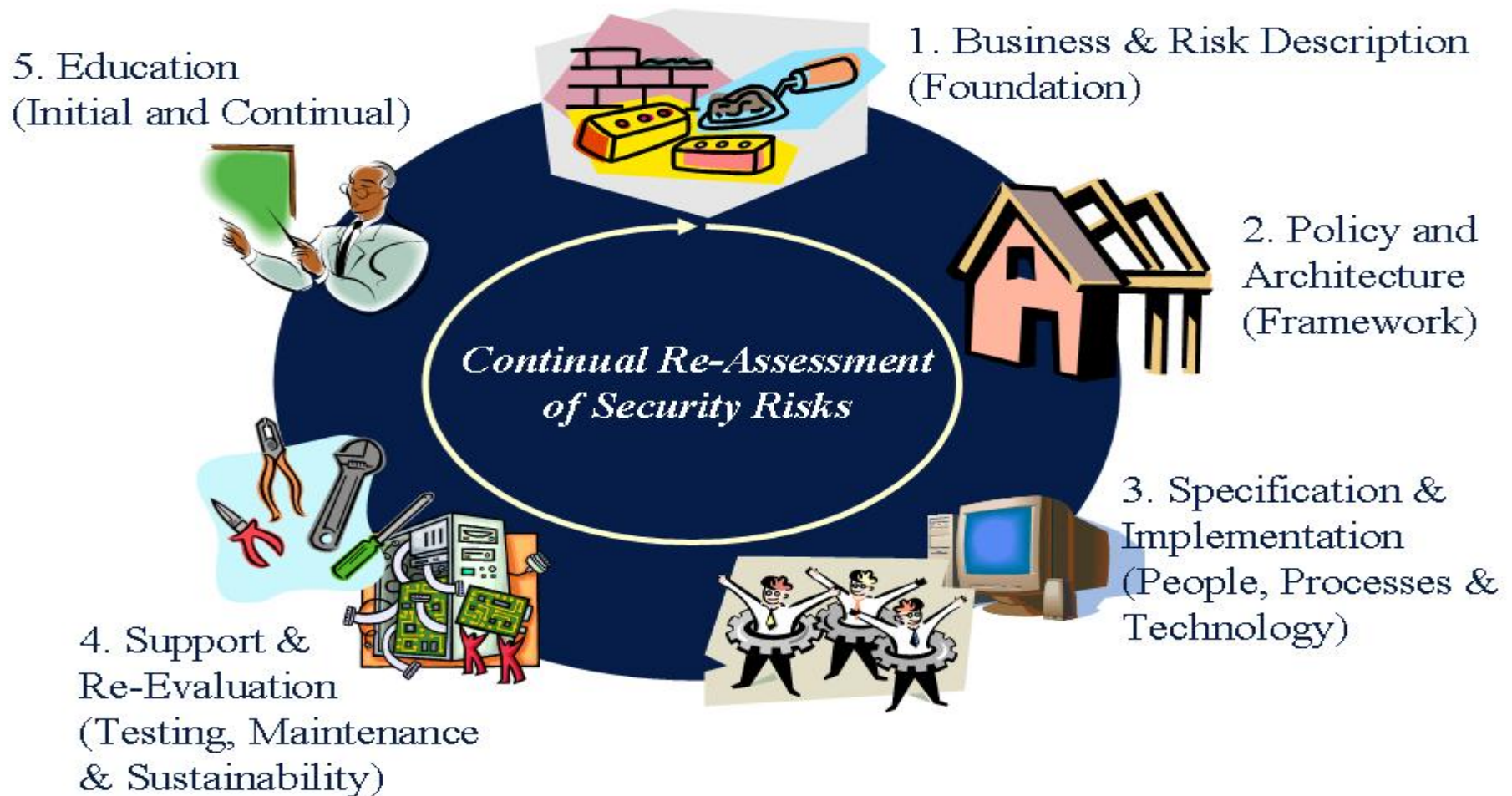
- ***Safeguards*** are practices, procedures or mechanisms that may protect against a ***threat***, reduce ***vulnerability***, limit the impact of an information security incident, detect incidents and facilitate recovery.
- Effective security usually requires a ***combination*** of different safeguards to provide ***layers*** of security to protect assets.

- 1) Legislation, Regulation and Advocacy
    - Government & Legal Affairs
  - 2) MBA Board of Directors Technology Steering Committee (BoDTech)
    - White papers, Research, and Analysis
  - 3) Education
    - CampusMBA & Conferences
  - 4) MISMO
    - Information Security Work Group
    - [www.mismo.org](http://www.mismo.org)
    - <http://www.mismo.org/files/mismo/InformationSecurityWhitepaper.pdf>
  - 5) Identity Management
    - Secure Identity Services Accreditation Corporation
    - [www.sisac.org](http://www.sisac.org)
-

- 2005 white paper on “Protecting Personal Information: The Good, Bad, and Ugly”
  - 2006 research on “Five-Step Information Assurance Model for the Mortgage Industry”
    - » Research and analysis of critical areas of information assurance
      - Legislative & Regulatory, Audit Practices and Security Standards & Framework
      - Achieving industry consensus in lieu of increased and additional regulations
      - [http://store.mortgagebankers.org/ProductDetail.aspx?product\\_code=EC5-400000-BK-P](http://store.mortgagebankers.org/ProductDetail.aspx?product_code=EC5-400000-BK-P)
-



## Five-Step Information Assurance Model



# Legal Issues in Technology

Data Security, Consumer Privacy & Identity Theft



Category	Legislation & Regulation	Audit Standards	Information Security Standards
Business & Risk Description	Reg AB, SOX, FFIEC, FTC	AICPA, BITS, FDIC, Federal Reserve, FFIEC, GAO, NCUA, CobiT, ISO 17799, ISO 27001, NIST	COSO, ISACA/CobiT, ISO 17799, ISO 27001, NIST 800-53,26,37, X9.99
Policy & Architecture	EU Privacy, GLBA, Japan Privacy	AICPA, BITS, FDIC, Federal Reserve, FFIEC, GAO, NCUA, CobiT, ISO 17799, ISO 27001, NIST	ISACA/CobiT, ISO 17799, ISO 27001, NIST 800-53,26,37, X9.99
Solution Specification & Implementation	AU Federal Privacy, PIPPEA, EU Privacy, FACT, FCRA, Japan Privacy, Reg AB, SOX, USA Patriot, FFIEC, FTC	AICPA, BITS, FDIC, Federal Reserve, FFIEC, GAO, NCUA, CobiT, ISO 17799, ISO 27001, NIST	COSO, ISACA/CobiT, ISO 17799, ISO 27001, NIST 800-53,26,37, X9.99
Solution Support & Re-evaluation	Japan Privacy, Reg AB, SOX, FFIEC, CA SB 1386, EU Privacy, GLBA, High-risk 3997, FTC	AICPA, BITS, Federal Reserve, FFIEC, GAO, NCUA, FDIC, CobiT, ISO 17799, ISO 27001, NIST	COSO, ISACA/CobiT, ISO 17799, ISO 27001, NIST 800-53,26,37, X9.99
Education	Japan Privacy, FTC	AICPA, BITS, FDIC, Federal Reserve, GAO, NCUA, CobiT, ISO 17799, ISO 27001, NIST	COSO, ISACA/CobiT, ISO 17799, ISO 27001, X9.99

1. Information Asset Identification
  2. Information Risk Assessment
  3. Information Security Policy
  4. Information Security Architecture
  5. Solution Specification: Technologies
  6. Solution Specification: Procedures
  7. Solution Specification: Personnel
  8. Solution Implementation Planning & Execution
  9. Information Security Maintenance Program
  10. Information Security Monitoring and Incident Response Program
  11. Business Continuity Planning & Testing
  12. Information Security Awareness and Education
-

- Comprehensive approach
  - Product or Services life-cycle
    - » No longer layer on at the end
  - Integrated team
    - » Legal, compliance, business analysis, IT/IS, etc.
  - Senior Management
    - » Critical to success
    - » Regulatory requirement (CIP, Red Flag, etc.)
  - Digital Rights management
    - » Review & authorize who has access to what
    - » Not all data for all eyes
  - More than just technology
    - » Beyond securing servers and encryption
    - » People & Processes
  - Assess & Re-assess
    - » Regulations, technology, practices, products, partners all change over time
-