I. Introduction to Privacy: Common Principles and Approaches

A. A Modern History of Privacy
   a. Descriptions and definitions
   b. Historical and social origins
   c. Information types
      i. Personal and non-personal
      ii. General and organizational
         1. Financial
         2. Human resources
         3. Operational
         4. Intellectual property (IP)
         5. Information products and services
   d. Elements of personal information
      i. Data subjects
      ii. Personal data (EU)
      iii. Personally identifiable information (U.S.)
      iv. Sensitive personal information
   e. Processing of personal data
      i. Data controller
      ii. Data processor
      iii. Data protection authority (DPA)
   f. Privacy policy and notice
      i. Consent and choice

B. Information Risk Management
   a. Privacy’s impact on organizational risk
      i. Main drivers and challenges
      ii. Common processes
      iii. Potential outcomes
   b. Information lifecycle principles
      i. Collection
      ii. Use and retention
      iii. Disclosure
      iv. Management and administration
      v. Monitoring and enforcement
   c. Privacy impact assessments (PIA)
C. Modern Privacy Principles
   a. Foundational principles
      i. U.S. fair information practices
      ii. The Organization of Economic Cooperation and Development (OECD) "Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data" (1980)
      iii. The Asia Pacific Economic Cooperation (APEC) privacy principles
   b. Historical timeline of principles frameworks
   c. Common themes among principles frameworks

D. Privacy and Data Protection Regulation
   a. Global perspectives
      i. Countries with national data protection laws in force
      ii. Countries with emerging privacy or data protection laws
      iii. Sector-based and contextual privacy laws
      iv. Contrast in regulatory approaches: EU and U.S.
   b. United States
      i. Federal privacy laws
      ii. State privacy laws
   c. Europe
      i. The European Union (EU) Data Protection Directive (95/46/EC)
         1. Applicability
         2. Core principles
         3. Data processing
         4. Data transfers
            a. "Adequacy"
            b. Binding corporate rules (BCRs)
            c. Model contracts
      ii. The EU ePrivacy Directive (2002/58/EC)
      iii. The Article 29 Working Party
      iv. Employment data
      v. EU-U.S. safe harbor agreement
         1. Program components
         2. Privacy principles
         3. Compliance and enforcement
   d. Other national data protection regimes
      i. Canada
         1. The Privacy Act of 1983
         2. The Personal Information Protection and Electronic Documents Act of 2000 (PIPEDA)
      ii. Asia Pacific region
         1. Japan
            b. Data transfer requirements
      2. Australia
         a. The Privacy Act of 2001
      iii. Latin America
         1. “Habeas data”
II. Information Security: Safeguarding Personal Information

A. Introduction to Information Security

a. Privacy and information security in context
   i. Definitions
   ii. Confidentiality, integrity and availability
   iii. Common issues and challenges
b. Information security needs and principles
   i. Segregation of duties
   ii. Access privileges
c. Information security standards
   i. ISO 27001
   ii. ISO 27002
      1. Security clauses
d. Information security threats and vulnerabilities
   i. Threat agents and origins
   ii. SysAdmin Audit and Network Security (SANS) Top 20 Security Risks
   iii. Malware
   iv. Phishing
   v. Social engineering

B. Information Security Management

a. Building an infosecurity framework
   i. Process components
   ii. Industry standards
   iii. Organizational policy
b. Infosecurity compliance
   i. Legal requirements
c. Common information security controls
   i. Access control policy and responsibility
   ii. Access control types
      1. Preventative
      2. Detective
      3. Corrective
   iii. Access control placement
      1. Network
      2. Operating system
      3. Application layer
      4. Mobile computing and teleworking
   iv. Cryptography
      1. General concepts of shared and public key cryptography
         a. Public key infrastructure (PKI)
      2. Encryption
      3. Decryption
      4. Non-repudiation
      5. Other uses
         a. Digital signatures
         b. Certifications
   v. Identity and access management (IAM)
      1. Authentication
      2. Authorization
vi. Other controls
   1. Networks
      a. Firewalls
      b. Intrusion detection systems (IDS)
      c. Intrusion prevention systems (IPS)
      d. Data loss and data leakage protection
   2. Financial transactions
      a. Payment Card Industry (PCI) Data Security Standard (DSS)

d. Information security governance
   i. Internal to organization
   ii. External parties
   iii. Asset management
      1. Inventory of assets
      2. Information classification

iv. Human resources security
   1. Pre-employment
   2. Change of employment

v. Physical and environmental security
   1. Securing facilities
   2. Equipment safety

vi. Communications and operations management
   1. Management of third party service delivery
   2. System monitoring
      a. System and end user
   3. Back up media
      a. Handling
      b. Transfer of information
   4. Online security and monitoring

vii. Incident management
   1. Reporting events and weaknesses
   2. Managing incidents and improvements
   3. Business continuity

viii. The information security program
   1. The information security management system (ISMS)
   2. Program improvement
   3. Management review
   4. Program assessments
      a. Internal audits
      b. External/third-party audits

ix. Vendor management
   1. Due diligence and qualification
   2. Contract management
III. Online Privacy: Using Personal Information on Websites and with Other Internet-related Technologies

A. The Web as a Platform
   a. Standard Web protocols
      i. Internet Protocol (IP)
      ii. Hypertext Transfer Protocol (HTTP) and secure-HTTP
      iii. Hypertext Transfer Protocol-Secure (HTTPS)
      iv. Internet proxies and caches
      v. Web server logs
      vi. Transport layer security (TLS)
      vii. Secure Sockets Layer (SSL)

B. Privacy Considerations for Sensitive Online Information
   a. Threats to online privacy
      i. Cross-site scripting (XSS)
   b. Online privacy notices and methods for communication
      i. Website privacy statement
         1. Location at /link from all points of data collection
         2. Sample language
         3. Machine-readable policy formats
            a. Platform for Privacy Preferences Project (P3P)
   c. Data subject access and redress
   d. Online security
   e. Website user authentication
   f. Children’s online privacy
   g. Active versus passive data collection
      i. Web forms
   h. Online identification mechanisms
      i. Cookies
         1. First party and third party
         2. Common use cases
         3. Industry best practices
      ii. Web beacons
   i. Privacy and electronic mail
      i. Commercial e-mail
         1. Best practices and standards for privacy protection
         2. Unsolicited commercial e-mail (“spam”)
   j. Online marketing and advertising
      i. Search engine marketing (SEM)
      ii. Online behavioral marketing (OBM)
   k. Online social media
      i. Social networking services
      ii. Instant messaging
   l. Online assurance
      i. Trust seal and dispute resolution programs
      ii. Self-regulatory frameworks