I. Common Principles and Approaches to Privacy

A. A Modern History of Privacy
   a. Descriptions, definitions and classes
   b. Historical and social origins

B. Types of Information
   a. Personal information
   b. Non-personal information
   c. General and organizational
      i. Financial
      ii. Human resources
      iii. Operational
      iv. Intellectual property (IP)
      v. 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
         1. Opt in and opt out

C. 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)

D. Modern Privacy Principles  
a. Foundational principles  
   i. U.S. fair information practices  
      1. Notice, access, choice, and consent  
      2. Scope and limitations of use  
   ii. The Organisation 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

II. Jurisdictions and Industries

A. Geography: Privacy and Data Protection Regulation  
a. Introduction  
b. Global perspectives overview  
   i. Countries with comprehensive data protection laws  
   ii. Countries with sectoral data protection laws  
   iii. The co-regulatory model  
   iv. The self-regulatory model  
c. United States  
   i. Federal privacy laws  
   ii. State privacy laws  
d. Canada  
   i. The Privacy Act of 1983  
   ii. The Personal Information Protection and Electronic Documents Act of 2000 (PIPEDA)  
e. 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 Principles  
      1. Program components  
      2. Privacy principles  
      3. Compliance and enforcement  
   f. Japan  
   i. The Law Concerning the Protection of Personal Information (2003)  
   ii. Data transfer requirements  
g. Australia  
   i. The Privacy Act of 2001  
h. Latin America  
   i. “Habeas data”  
i. India
j. Other Countries

B. Sectors of Privacy Law
   a. Introduction
   b. Healthcare
   c. Financial
   d. Telecommunications
   e. Online Privacy
   f. Government
   g. Marketing
   h. Energy
   i. Human Resources
   j. Other

III. 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
         1. Privacy vs. security
   b. Elements of information security
      i. Information security needs
      ii. Information security key principles
         1. Segregation of duties
         2. Access privileges
         3. Least privilege
   c. Information security standards
      i. ISO 27001
      ii. ISO 27002
         1. Security clauses
   d. Information security threats and vulnerabilities
      i. Determining risk
      ii. Threat agents and origins
      iii. Security risks and vulnerabilities
      iv. Malware
      v. Phishing
      vi. Social engineering

B. Information Security Management
   a. Building an information security framework
      i. Process components
      ii. Industry standards
      iii. Organizational policy
   b. Information security 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)

vii. 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
Vendor management
1. Due diligence and qualification
2. Contract management

IV. 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)
   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
   ii. Layered notice
   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. Internet searches
   k. Online marketing and advertising
   i. Search engine marketing (SEM)
   ii. Online behavioral marketing (OBM)
   l. Online social media
   i. Social networking services
   ii. Instant messaging
   m. Online assurance
   i. Trust seal and dispute resolution programs
   ii. Self-regulatory frameworks
   n. Cloud computing
   o. Mobile online privacy
   i. Location data