Security Governance: Fundamentals and Best Practices

Instructor Name

School/College Name

March 12, 2025

Introduction to Security Governance: Protecting What Matters

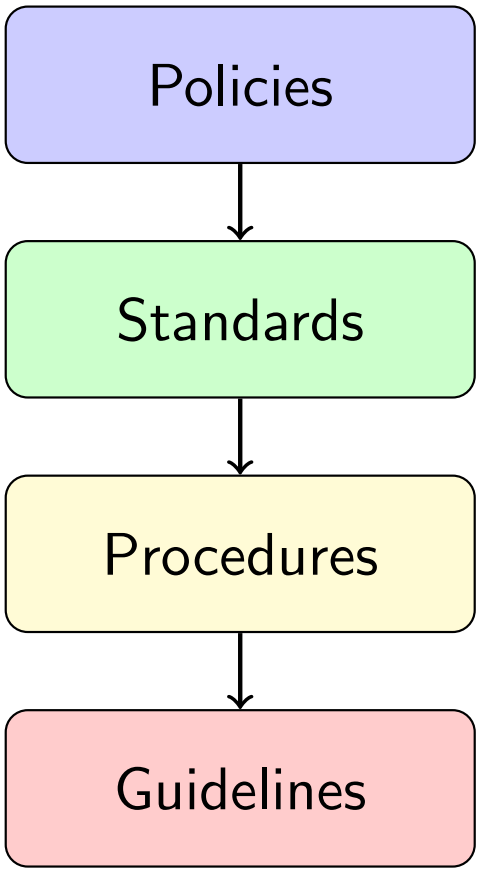
- **Security governance** is the framework of rules, processes, and practices that ensure an organization protects its information assets.
- Effective security governance aligns security practices with business objectives and stakeholder expectations.
- Security governance establishes accountability and clear lines of responsibility for protecting systems and data.
- Security governance reduces risks by providing structure and consistency to security efforts across an organization.

Why Security Governance Matters

Without proper governance, security efforts become fragmented, inconsistent, and ineffective, leaving organizations vulnerable to threats.

The Security Governance Framework: An Overview

- A security governance framework provides the structure that guides all security decisions and activities.
- The framework includes guidelines, policies, standards, and procedures that work together to protect assets.
- Effective frameworks balance security needs with usability to avoid creating barriers to legitimate work.
- Frameworks must adapt to changing threats, technologies, and regulatory requirements.



Security Guidelines: Setting the Foundation

- **Security guidelines** are recommendations that suggest how security should be implemented without mandating specific actions.
- Guidelines provide flexibility for different departments or situations while still promoting security best practices.
- Guidelines often serve as the starting point for developing more specific security policies and standards.
- Well-crafted guidelines help staff understand the reasoning behind security requirements.

Example Guideline

"Users should create passwords that are difficult for others to guess while still being memorable to themselves."

Policy Development: Creating Clear Security Direction

- **Security policies** are formal documents that define required behaviors, responsibilities, and consequences for non-compliance.
- Effective policies clearly state what must be done rather than how it should be accomplished.
- Policies should be written in clear, understandable language that avoids technical jargon when possible.
- All security policies should be regularly reviewed and updated to address emerging threats and technologies.

Policy Development Process

1. Identify need and gather requirements
2. Draft policy with stakeholder input
3. Review and obtain approval
4. Communicate and implement
5. Monitor, enforce, and revise

Acceptable Use Policies (AUP): Defining Proper Technology Use

- An **Acceptable Use Policy (AUP)** defines how employees may use company systems, networks, and data.
- AUPs outline prohibited activities such as accessing inappropriate content or installing unauthorized software.
- AUPs establish that company systems are primarily for business purposes and may be monitored.
- Effective AUPs balance necessary restrictions with reasonable allowances for limited personal use.

Typically Allowed	**Typically Prohibited**
Limited personal email	Installing unauthorized software
Brief web browsing during breaks	Accessing inappropriate content
Occasional personal calls	Sharing credentials
Using approved cloud storage	Circumventing security controls

Table: Common AUP Elements

Information Security Policies: Safeguarding Digital Assets

- **Information security policies** establish rules for protecting the confidentiality, integrity, and availability of data.
- These policies define data classification schemes that determine how different types of information should be handled.
- Information security policies specify access control requirements based on the principle of least privilege.
- They include requirements for data protection throughout its lifecycle, from creation to deletion.

Key Information Security Policy Components

- Data classification (public, internal, confidential, restricted)
- Access control requirements
- Data handling procedures
- Security incident reporting

Business Continuity: Keeping Operations Running

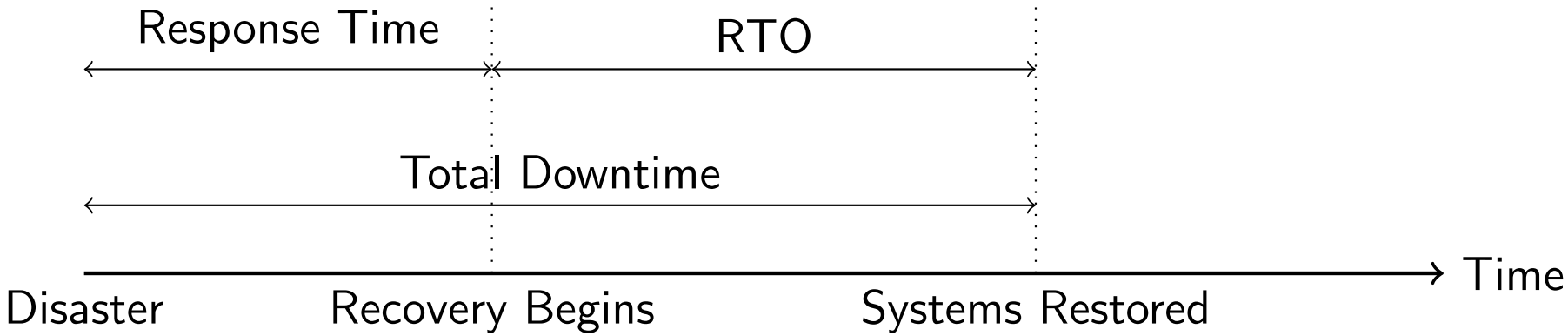
- **Business continuity** refers to maintaining essential functions during and after a disruptive event.
- Business continuity policies define how an organization will continue operating during disasters, outages, or other crises.
- These policies establish the maximum acceptable downtime for critical systems and processes.
- Business continuity planning includes identifying essential functions and creating alternate procedures when normal operations are disrupted.

Business Impact Analysis (BIA)

A BIA identifies critical business functions, determines the impact of disruptions, establishes recovery time objectives (RTOs), and informs resource allocation for continuity planning.

Disaster Recovery: Bouncing Back from Catastrophe

- **Disaster recovery** focuses specifically on restoring IT systems and infrastructure after a disruptive event.
- Disaster recovery policies define the methods, tools, and procedures for recovering damaged systems.
- These policies establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each system.
- Effective disaster recovery requires regular testing, updating, and training for all involved personnel.



Incident Response: Managing Security Breaches

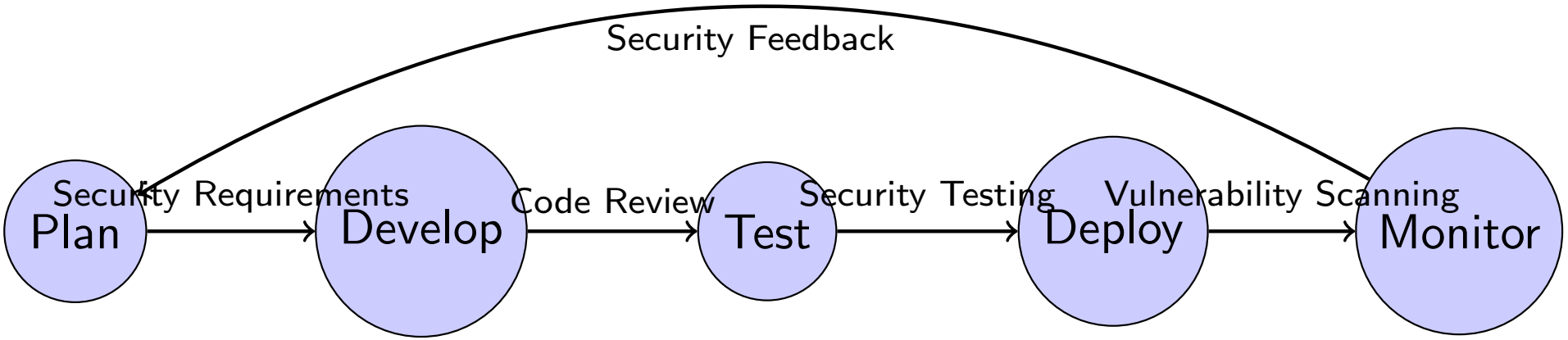
- **Incident response** is the organized approach to addressing and managing security breaches.
- Incident response policies define what constitutes a security incident and establish procedures for handling various types of incidents.
- These policies create a structured framework that enables quick and effective responses to minimize damage.
- Incident response requires clear communication protocols and defined roles for all team members.

The Incident Response Lifecycle

1. Preparation: Create plans and train teams
2. Detection & Analysis: Identify and assess the incident
3. Containment: Prevent the incident from spreading
4. Eradication: Remove the threat from systems
5. Recovery: Restore systems to normal operation
6. Lessons Learned: Improve future responses

SDLC Security: Building Safety into Software Development

- **Software Development Lifecycle (SDLC)** security integrates security practices throughout the entire development process.
- SDLC security policies establish requirements for secure coding, testing, and validation at each development phase.
- These policies mandate security reviews and testing before software can move to the next development stage.
- Effective SDLC security shifts the focus from fixing vulnerabilities after deployment to preventing them during development.



Change Management Policies: Controlling System Modifications

- **Change management policies** establish processes for making changes to IT systems in a controlled, documented manner.
- These policies require formal approval processes before changes can be implemented in production environments.
- Change management ensures that modifications are properly tested and do not negatively impact security or functionality.
- Effective change management includes rollback plans in case changes create unexpected problems.

Example Change Management Process

A system administrator wants to update server software. They must:

1. Submit a change request with details and justification
2. Obtain approval from the change advisory board
3. Schedule the change during an approved maintenance window
4. Test the change in a non-production environment first
5. Document results and follow rollback procedures if needed

Security Standards: Establishing Consistent Practices

- **Security standards** define specific, mandatory requirements for implementing security controls.
- Standards provide detailed technical specifications that support the broader objectives stated in security policies.
- Unlike guidelines, standards leave little room for interpretation and establish clear compliance requirements.
- Effective standards balance security needs with practicality to ensure they can be reasonably implemented.

Security Element	**Example Standard Requirement**
Passwords	Minimum 12 characters with complexity requirements
System Updates	Critical patches must be applied within 14 days
Data Encryption	All sensitive data must use AES-256 encryption
Access Reviews	Administrator access must be reviewed quarterly

Table: Example Security Standards

Password Standards: Creating Strong Authentication Rules

- **Password standards** define specific requirements for creating, managing, and protecting user credentials.
- These standards specify minimum password length, complexity requirements, and expiration periods.
- Password standards often include rules for password storage, such as requiring salted hashing rather than storing plaintext passwords.
- Effective standards balance security needs with usability to avoid encouraging risky workarounds like writing passwords down.

Modern Password Guidance

The National Institute of Standards and Technology (NIST) now recommends:

- Longer passwords (at least 12 characters)
- Checking new passwords against lists of commonly used or compromised passwords
- Eliminating arbitrary complexity requirements
- Removing periodic password change requirements

Access Control Standards: Managing Who Gets In

- **Access control standards** define requirements for granting, managing, and revoking access to systems and data.
- These standards implement the principle of least privilege, ensuring users have only the access necessary for their job functions.
- Access control standards require regular reviews of user permissions to identify and remove unnecessary access rights.
- Effective standards include special provisions for privileged accounts that have elevated system access.

Control Type	Examples
Preventive Controls	Authentication Authorization
Detective Controls	Access auditing Login monitoring
Corrective Controls	Account lockout Password reset
Compensating Controls	Multi-factor authentication Separation of duties

Table: Examples of Access Control Standards

Physical Security Standards: Protecting Tangible Assets

- **Physical security standards** establish requirements for protecting facilities, equipment, and physical information assets.
- These standards define access requirements for different security zones within facilities (e.g., lobbies, server rooms).
- Physical security standards include requirements for monitoring systems like cameras and intrusion detection.
- Effective standards consider both deliberate threats (theft, vandalism) and environmental risks (fire, flood, power loss).

Example: Server Room Requirements

- Access limited to authorized IT personnel via card readers with PIN
- 24/7 video surveillance with 90-day retention
- Environmental monitoring for temperature, humidity, and water
- Fire suppression system specific to electronic equipment

Encryption Standards: Securing Data Transmission and Storage

- **Encryption standards** define requirements for protecting data confidentiality through cryptographic methods.
- These standards specify which encryption algorithms and key lengths must be used for different types of data.
- Encryption standards establish requirements for key management, including generation, storage, and rotation practices.
- Effective standards address both data at rest (stored) and data in transit (being transmitted).

Data Type	Encryption Method	Key Management
Data at rest	AES-256	Keys stored in secure hardware
Data in transit	TLS 1.3	Certificates rotated annually
Emails	S/MIME or PGP	Key pairs for each user
Backups	AES-256	Offline key storage

Table: Example Encryption Standards

Security Procedures: Implementing Day-to-Day Practices

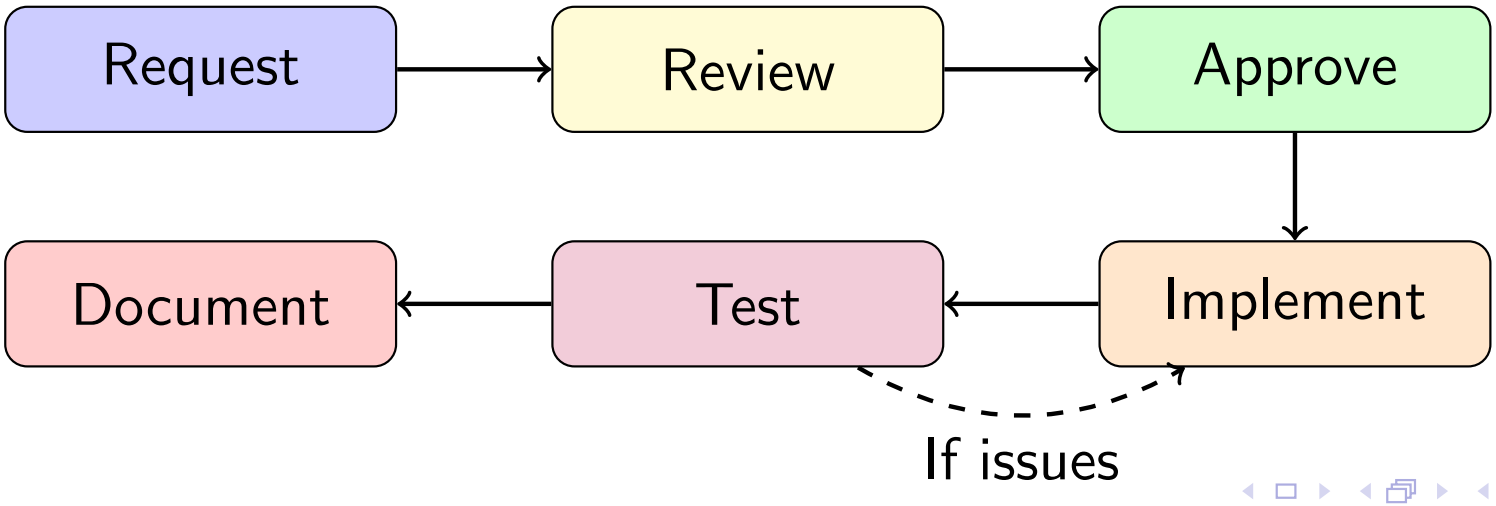
- **Security procedures** are detailed, step-by-step instructions for performing specific security-related tasks.
- Procedures translate high-level policies and standards into practical, actionable steps for implementation.
- Well-written procedures reduce human error by providing clear guidance for complex or infrequent tasks.
- Effective procedures include verification steps to confirm proper completion and documentation requirements.

Components of Effective Security Procedures

- Clear purpose and scope statement
- Required tools and prerequisites
- Detailed sequential steps with screenshots or diagrams
- Expected outcomes and verification methods
- Troubleshooting guidance for common issues

Change Management Procedures: Steps for Safe System Updates

- **Change management procedures** provide detailed instructions for implementing the change management policy.
- These procedures define the exact steps for requesting, approving, implementing, and documenting changes.
- Change management procedures include methods for categorizing changes based on risk and potential impact.
- Effective procedures establish different approval paths for routine, significant, and emergency changes.



Onboarding Procedures: Securely Adding New Users

- **Onboarding procedures** define the process for granting new employees appropriate access to systems and data.
- These procedures establish verification requirements to confirm user identity before access is granted.
- Onboarding procedures include security training requirements that must be completed before users receive full access.
- Effective onboarding creates a complete record of all access granted for future reference and auditing.

Sample Onboarding Procedure Steps

1. HR verifies employee identity and provides documented approval
2. IT creates accounts based on role-specific access templates
3. Employee completes security awareness training
4. Employee acknowledges acceptance of security policies
5. Manager confirms appropriate access levels
6. Access provisioning is documented in access management system

Offboarding Procedures: Safely Removing Access

- **Offboarding procedures** define the process for removing access when an employee leaves the organization.
- These procedures establish timelines for access removal based on the nature of the departure (e.g., immediate for terminations, phased for retirements).
- Offboarding procedures include steps to recover company equipment and data from departing employees.
- Effective offboarding requires coordination between HR, IT, facilities, and the employee's department.

Departure Type	Access Removal Timeline	Special Considerations
Voluntary resignation	End of last workday	Knowledge transfer period
Retirement	End of last workday	Phased transition period
Termination	Immediate	Monitor final access activities
Transfer	Based on new role start	Modify rather than remove

Table: Offboarding Timeline Examples

Security Playbooks: Standardized Response Actions

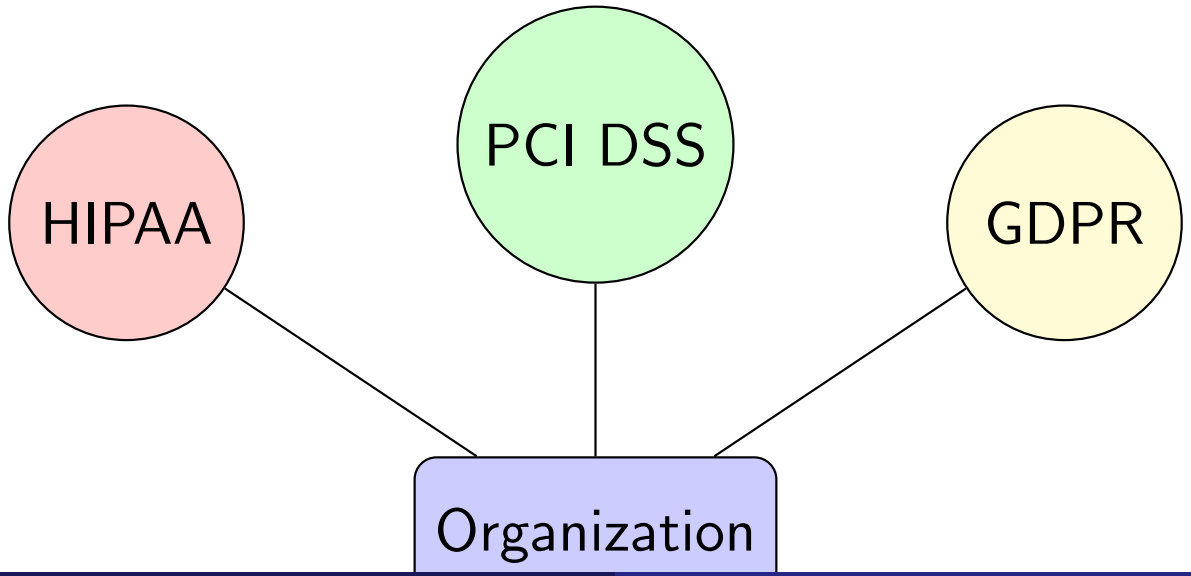
- **Security playbooks** are detailed action plans for responding to specific security incidents or scenarios.
- Playbooks provide step-by-step instructions that reduce decision-making burden during high-stress situations.
- Well-designed playbooks include decision trees to guide responders through different scenario variations.
- Effective playbooks assign clear responsibilities to specific roles rather than individuals to ensure coverage.

Common Security Playbook Elements

- Incident identification criteria and severity classifications
- Required tools and resources for response
- Communication templates and escalation paths
- Detailed containment and eradication steps
- Evidence collection and preservation procedures
- Recovery validation checkpoints

External Regulatory Considerations: Compliance Requirements

- **Regulatory compliance** involves adhering to laws, regulations, and standards established by external authorities.
- Security governance must account for industry-specific regulations that mandate certain security controls or practices.
- Non-compliance with regulations can result in significant financial penalties, legal liability, and reputational damage.
- Effective governance includes monitoring regulatory changes to ensure continued compliance as requirements evolve.



Legal Considerations in Security Governance

- Security governance must align with relevant laws regarding data protection, privacy, and breach notification.
- Legal considerations include liability for security failures that impact customers, partners, or the public.
- Security governance documentation may become legal evidence during investigations or litigation.
- Effective governance includes consultation with legal experts when developing policies for sensitive areas.

Legal Compliance Considerations

- Data breach notification requirements vary by jurisdiction
- Privacy laws restrict how personal data can be collected and used
- Contractual obligations may impose additional security requirements
- Intellectual property laws affect how proprietary information must be protected

Industry-Specific Security Standards

- **Industry-specific security standards** are frameworks tailored to address unique risks in particular sectors.
- These standards often develop through industry associations or specialized regulatory bodies.
- Industry standards may be voluntary but can become de facto requirements for doing business in certain sectors.
- Effective governance leverages these standards to establish baseline security controls relevant to the organization's industry.

Industry	**Standard**	**Focus Areas**
Healthcare	HIPAA	Patient data privacy and security
Financial	PCI DSS	Payment card processing security
Critical Infrastructure	NERC CIP	Power grid protection
Government	FedRAMP	Cloud service security

Table: Example Industry Standards

Local and Regional Security Regulations

- **Local and regional regulations** establish security and privacy requirements specific to geographic areas.
- These regulations can vary significantly between different cities, states, provinces, or regions.
- Organizations operating in multiple locations must ensure compliance with all applicable local requirements.
- Effective governance includes monitoring for new or changing local regulations that may impact security practices.

Examples of Regional Security Regulations

- California Consumer Privacy Act (CCPA) applies specifically to businesses operating in California
- New York SHIELD Act establishes specific data security requirements for companies with New York residents' data
- Illinois Biometric Information Privacy Act (BIPA) regulates collection and storage of biometric data
- Massachusetts 201 CMR 17.00 establishes specific technical security requirements for personal information

National Security Standards and Laws

- **National security standards** provide frameworks that apply to all organizations within a country.
- These standards establish baseline security expectations that may be further strengthened by industry regulations.
- National laws often include penalties for security breaches or failure to implement reasonable security measures.
- Effective governance ensures compliance with both mandatory requirements and voluntary national standards.

Country	Standard/Law	Primary Focus
United States	FISMA	Federal information security
United Kingdom	Data Protection Act	Personal data protection
Australia	Privacy Act	Data breach notification
Canada	PIPEDA	Consumer privacy

Table: National Security Standards Examples

Global Security Frameworks and Regulations

- **Global security frameworks** provide standardized approaches recognized across international boundaries.
- These frameworks help organizations establish security governance that satisfies requirements in multiple countries.
- Global regulations like GDPR may apply to organizations regardless of where they are physically located.
- Effective governance identifies which global frameworks best align with the organization's operations and compliance needs.

Key Global Security Frameworks

- **ISO 27001**: International standard for information security management systems
- **NIST Cybersecurity Framework**: Flexible framework for managing and reducing cybersecurity risk
- **CIS Controls**: Prioritized set of actions to protect critical systems and data
- **COBIT**: Framework for governance and management of enterprise information technology

Monitoring and Revising Security Governance

- **Security governance monitoring** involves regular assessment of how well policies and standards are being followed.
- Effective governance requires continuous review to address emerging threats, technologies, and regulatory changes.
- Revisions should be based on compliance data, incident response lessons, and security testing results.
- A formal review cycle ensures all governance documents remain relevant and effective over time.