Domain 2: Security and Compliance – Components and Resources

This presentation explores the essential components and resources for establishing a robust security and compliance framework. We'll examine key principles, domains, controls, and technologies that form the foundation of effective information security management.

Security Principles and Policies

Core Security Principles

The principle of least privilege ensures users have only the access needed for their role. Defense in depth implements multiple security layers. Secure-by-design integrates security from the beginning of development.

Documented Security Policies

Comprehensive written security policies provide consistent guidelines for protecting systems and data. They establish clear responsibilities and procedures for maintaining security across the organization.

Strategic Alignment

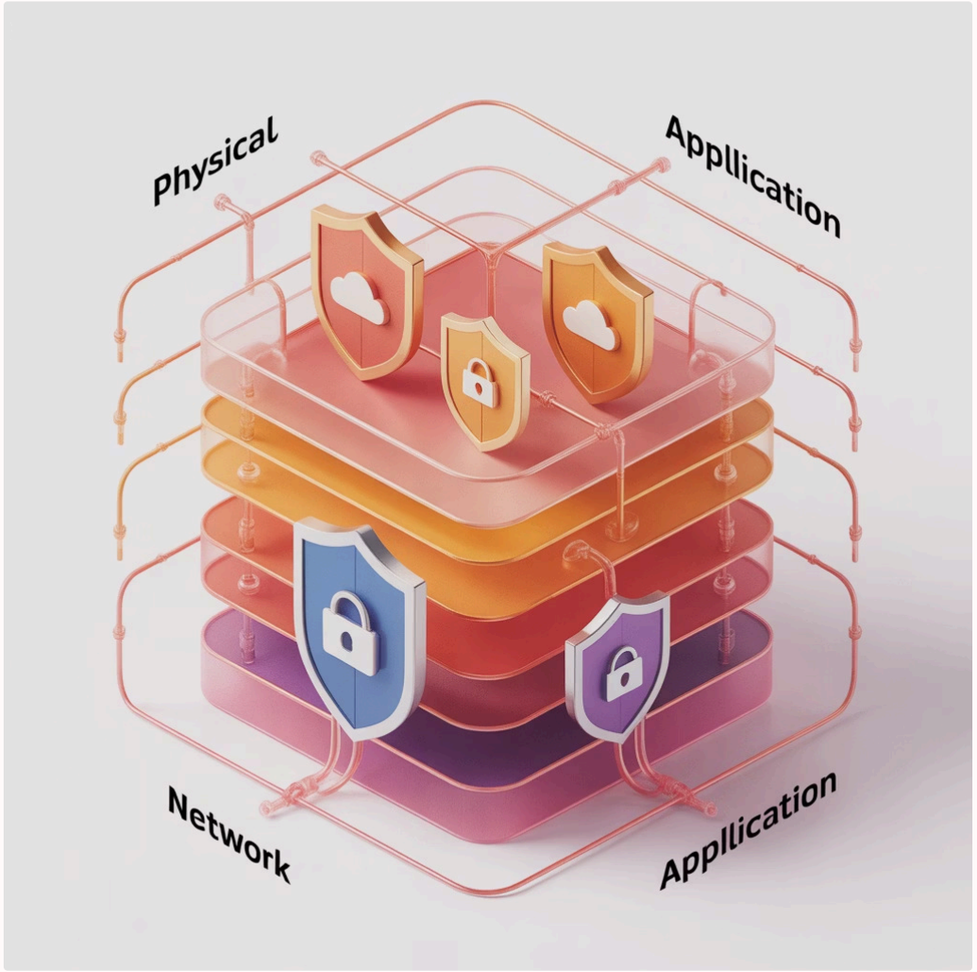
Effective security policies align with business objectives while ensuring compliance with legal and regulatory requirements. This balance enables security to support rather than hinder business operations.

Security Domains and Layers

Core Security Domains

- Network Security: Protects infrastructure and connections
- Application Security: Ensures software is developed and maintained securely
- Data Security: Safeguards information at rest, in transit, and in use
- Endpoint Security: Protects devices accessing corporate resources
- Cloud Security: Secures cloud-based systems, applications, and data

Architecture Layers



Segmenting security into distinct domains helps organizations target protective measures and allocate resources effectively, ensuring comprehensive coverage of all critical assets.

Security Controls and Frameworks

Preventive Controls

Multi-factor authentication verifies user identity through multiple methods. Access management systems enforce permissions based on roles. Next-generation firewalls filter traffic based on applications and content, not just ports.

Detection & Response

SIEM systems aggregate and analyze security data from multiple sources. Advanced log monitoring identifies suspicious patterns. Endpoint Detection and Response (EDR) tools detect and contain threats at the device level.

Standard Frameworks

NIST Cybersecurity Framework provides flexible guidance for managing security risk. ISO 27001 offers an international standard for information security management. CIS Controls deliver prioritized security actions.

These frameworks provide structured approaches to implementing comprehensive security programs, helping organizations establish baseline controls and measure security maturity.

Security Tools and Technologies

Perimeter & Network Protection

Next-generation firewalls filter traffic based on applications. Intrusion Detection/Prevention Systems (IDS/IPS) identify and block suspicious network activities. Data encryption protects information integrity and confidentiality.

Monitoring & Analysis

SIEM platforms aggregate and correlate security events from multiple sources. EDR solutions monitor endpoints for suspicious activities and facilitate rapid response to threats.

Vulnerability Management

Scanning tools identify system weaknesses before attackers can exploit them. Vulnerability management platforms track remediation efforts and prioritize fixes based on risk.

People and Processes

Clear Security Roles

IT teams handle day-to-day security operations. Dedicated security teams develop strategies and respond to incidents. Governance committees establish policies and oversee compliance. Clear delineation of responsibilities prevents gaps in coverage.

Training & Awareness

Regular security awareness training educates staff about threats like phishing. Role-specific technical training ensures security personnel have necessary skills. Simulated attacks test effectiveness of training and identify improvement areas.

Incident Procedures

Documented incident response plans outline steps for containing and remediating security events. Clear escalation procedures ensure appropriate involvement of stakeholders based on incident severity. Regular drills validate procedures.

Risk and Threat Modeling

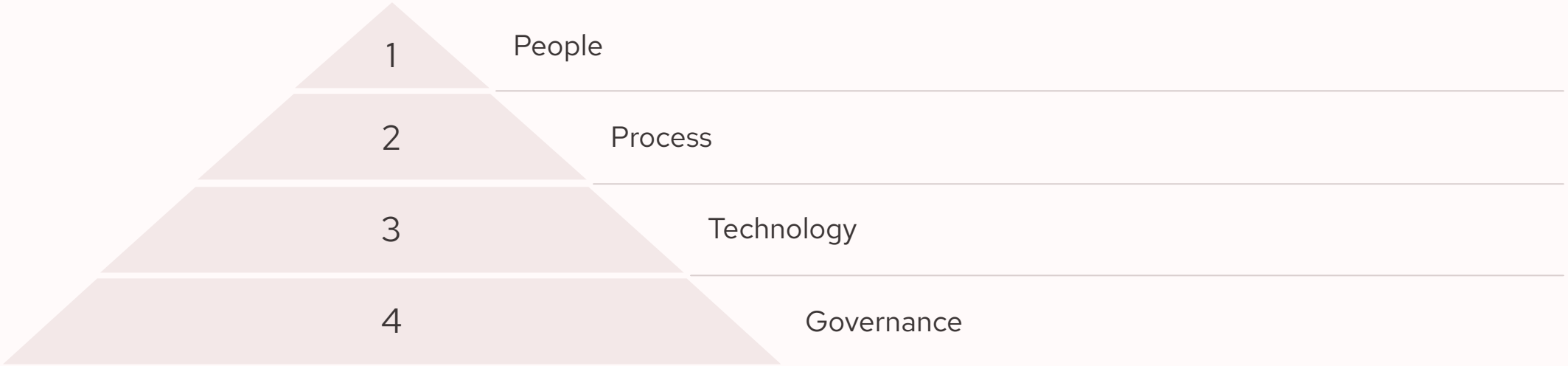
The Risk Assessment Process

1. Identify valuable assets and potential threats
2. Assess likelihood and potential impact of threats
3. Prioritize risks based on severity scores
4. Implement controls proportional to risk levels
5. Monitor effectiveness and adjust as needed

Threat intelligence feeds provide current information about emerging attack vectors and vulnerabilities, enabling proactive defense adjustments.

Regular risk assessments ensure security resources target the most significant threats to critical assets. This approach optimizes protection while managing security costs effectively.

Summary: Integrated Security Architecture



Effective security requires continuous monitoring and realignment as threats and business needs evolve. Regular assessment, testing, and improvement ensure controls remain effective against emerging threats.

A comprehensive security program integrates all components—from technical controls to human awareness—creating multiple layers of protection. This defense-in-depth approach ensures that if one security measure fails, others are in place to protect critical assets.