

Information Security

Prepared by Dr. Ahmed Omar

IT373
Information Security

Lecture 10



Lecture 10

Lecture 10

Prepared by
Dr. Ahmed Omar



Agenda

- ☐ **Introduction to Information Security Governance**
- ☐ **Risk Management and Security Frameworks**
- ☐ **Penetration Testing**
- ☐ **Cybersecurity Teams**

What is Information Security Governance?

- ❑ Information Security Governance is the system of direction and control that ensures information security aligns with **business objectives, manages risks effectively, and creates value** for stakeholders. It establishes *accountability, transparency, and strategic oversight* of an organization's information security program.

Key Components of Security Governance

The core components include ***strategic alignment, risk management, resource management, performance measurement, and value delivery.***

1. Strategic Alignment

- ❑ **Security objectives must support business goals** - *Security initiatives should directly contribute to achieving business objectives*
- ❑ **Integration with enterprise risk management** - *Security risks should be evaluated alongside other business risks*
- ❑ **Resource allocation based on business priorities** - *Security budgets should focus on protecting what matters most to the business*

Key Components of Security Governance

2. Risk Management

- ❑ **Identification and assessment of information risks** - *Understanding what threats could harm the organization and how likely they are*
- ❑ **Risk appetite and tolerance definition** - *Deciding how much risk the organization is willing to accept*
- ❑ **Treatment strategies and monitoring** - *Implementing controls to manage risks and tracking their effectiveness*

Key Components of Security Governance

3. Resource Management

- ❑ **Optimal allocation of security investments** - *Spending security budgets where they provide the most protection*
- ❑ **Skills and competency development** - *Ensuring staff have the right training and expertise*
- ❑ **Technology and infrastructure planning** - *Selecting and implementing security tools that meet current and future needs*

Key Components of Security Governance

4. Performance Measurement

- ❑ **Key performance indicators (KPIs) and metrics** - *Measuring security program effectiveness with specific, quantifiable measures*
- ❑ **Regular assessment and reporting** - *Providing ongoing visibility into security performance to management*
- ❑ **Continuous improvement processes** - *Using measurement results to identify and implement improvements*

Key Components of Security Governance

5. Value Delivery

- ☐ **Demonstrable return on security investments** - *Showing that security spending provides tangible benefits to the organization*
- ☐ **Business enablement through secure processes** - *Making security controls that help rather than hinder business operations*
- ☐ **Stakeholder satisfaction and confidence** - *Building trust with customers, partners, and regulators through effective security*

Governance Structure and Roles

A strong governance structure clearly defines who is responsible for security at every level.

- **Board of Directors/Executive Leadership:** Provides strategic oversight and sets the risk appetite. They approve budgets and receive regular security posture reports.
- **Chief Information Security Officer (CISO):** The senior executive responsible for developing and executing the security strategy, overseeing risk management, and coordinating incident response.
- **Security Steering Committee:** A cross-functional group that makes security decisions, approves policies, and prioritizes resources.
- **Security Operations Team:** The team responsible for day-to-day security operations, monitoring, and incident response.

Policy Development and Management

A clear **policy hierarchy** ensures that security guidance is consistent and enforceable throughout the organization.

- ❑ **Policies:** High-level, broad statements of management's intent (e.g., "All employees must use strong passwords").
- ❑ **Standards:** Mandatory rules and requirements that must be followed to comply with policies (e.g., "Passwords must be at least 12 characters long and include numbers, symbols, and letters").
- ❑ **Procedures:** Step-by-step implementation guidance for following standards (e.g., detailed instructions for setting up a new password in the system).
- ❑ **Guidelines:** Recommended practices and suggestions that support policies and standards but are not mandatory (e.g., "It is recommended to change your password every 90 days").

Policy Lifecycle

1. **Development and Review:** Create policies with input from affected stakeholders.
2. **Approval and Communication:** Get management approval and inform all employees.
3. **Implementation and Training:** Roll out the policies and train people on how to follow them.
4. **Monitoring and Compliance:** Check to see if people are following the policies.
5. **Review and Update:** Regularly update policies to keep them current and effective.

Risk Management and Security Frameworks

Security frameworks provide structured guidance for organizations to manage their information security. They are not one-size-fits-all, and a combination of frameworks is often used.

- ❑ **NIST Cybersecurity Framework:** Developed by the **National Institute of Standards and Technology**, this is a voluntary framework that helps organizations manage and reduce cybersecurity risk.
- ❑ **ISO 27001:** This is an international standard for an Information Security Management System (ISMS). It provides a structured, auditable approach to managing an organization's security risks and assets.
- ❑ **COBIT** is a broader framework that addresses the full lifecycle of IT, including governance, risk management, and compliance across the entire enterprise. It helps organizations align their IT goals with their business objectives and effectively manage IT risks.

Risk Management and Security Frameworks

Understanding Information Security Risk

Risk in information security context represents the potential for loss, damage, or destruction of assets as a result of a threat exploiting a vulnerability. *Risk occurs when something bad (threat) can take advantage of a weakness (vulnerability) to cause harm.* It's typically expressed as:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

Risk Management

Asset Identification

- ❑ **Information assets** (data, databases, files) - *The digital information that has value to the organization*
- ❑ **Physical assets** (hardware, facilities, media) - *Tangible items like servers, buildings, and storage devices*
- ❑ **Software assets** (applications, systems, utilities) - *Programs and systems that process or store information*
- ❑ **Human assets** (personnel, skills, knowledge) - *People and their expertise that are critical to operations*
- ❑ **Intangible assets** (reputation, intellectual property) - *Non-physical assets that have significant value*

Risk Management

Threat Identification

- ❑ **Natural threats:** Floods, earthquakes, fires, storms - *Environmental events that can damage systems and facilities*
- ❑ **Human threats:** Malicious insiders, external attackers, unintentional errors - *People who might cause harm either deliberately or accidentally*
- ❑ **Environmental threats:** Power failures, pollution, infrastructure failures - *Problems with utilities and supporting infrastructure*
- ❑ **Technical threats:** Hardware failures, software bugs, system crashes - *Technology-related problems that can disrupt operations*

Risk Management

Vulnerability Assessment, Find weaknesses in security controls, including:

- **Technical vulnerabilities:** Unpatched systems, weak configurations.
- **Physical vulnerabilities:** Inadequate access controls.
- **Administrative vulnerabilities:** Weak policies, insufficient training.

Risk Treatment Options

After assessing a risk, an organization can choose one of **four ways** to handle it.

- ☐ **Risk Acceptance:** Acknowledging the risk and deciding to take no further action. This is appropriate when the cost of mitigation is greater than the potential loss.
- ☐ **Risk Mitigation/Reduction:** Implementing controls to reduce the likelihood or impact of a risk. This is the most common approach and includes measures like firewalls, antivirus software, and training.
- ☐ **Risk Transfer:** Shifting the risk to another party. Examples include purchasing insurance or using service level agreements (SLAs) with a vendor.
- ☐ **Risk Avoidance:** Eliminating the risk entirely by removing the threat or vulnerability. This could mean discontinuing a risky business activity.

Penetration Testing

Penetration testing, often referred to as pen testing, is a simulated cyber attack against a computer system, network, or web application to check for exploitable **vulnerabilities**. It is a crucial part of a comprehensive security strategy, aiming to identify **weaknesses** before malicious actors can exploit them.

Penetration testing **methodologies** provide a **structured approach** to conducting these tests, ensuring consistency, thoroughness, and effectiveness.

Penetration Testing Methodologies

Several well-established methodologies guide penetration testers. These frameworks help define the **scope**, **phases**, and **techniques used** during a pen test. Some of the most prominent methodologies include:

1. **Open-Source Security Testing Methodology Manual (OSSTMM)**: A comprehensive methodology that provides a scientific approach to security testing, covering various aspects beyond just technical vulnerabilities, including human factors and physical security.

Penetration Testing Methodologies

2. Open Web Application Security Project (OWASP) Testing Guide: Specifically focuses on testing web applications, providing a detailed guide for identifying common web application vulnerabilities.

3. National Institute of Standards and Technology (NIST) Special Publication 800-115: Offers technical guidance for conducting information security tests and assessments, including penetration testing.

Penetration Testing Methodologies

4. Penetration Testing Execution Standard (PTES): A standard that outlines **seven** phases of a penetration test: *Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, and Reporting.*

5. Information System Security Assessment Framework (ISSAF): A structured approach to security assessments, including penetration testing, that covers various domains like *network, application, and physical security.*

Penetration Testing Steps

Regardless of the specific methodology chosen, most penetration tests follow a general set of phases:

1. **Reconnaissance/Information Gathering:** This initial phase involves collecting as much information as possible about the target system or network. This can include passive techniques (e.g., open-source intelligence gathering) and active techniques (e.g., network scanning).

Penetration Testing Steps

- 2. Scanning:** In this phase, testers use various tools to identify potential vulnerabilities in the target system. This includes port scanning, vulnerability scanning, and network mapping.
- 3. Vulnerability Analysis:** The gathered information and scan results are analyzed to identify potential weaknesses and determine their exploitability.
- 4. Exploitation:** This is the phase where testers attempt to exploit identified vulnerabilities to gain unauthorized access or achieve specific objectives. This is done in a controlled manner to avoid causing damage.

Penetration Testing Steps

5. Post-Exploitation: Once access is gained, testers assess the impact of the compromise, look for further vulnerabilities, and attempt to maintain access for a specified period to demonstrate persistence.

6. Reporting: The final and crucial phase involves documenting all findings, including exploited vulnerabilities, their impact, and recommendations for remediation. A clear and concise report is essential for the client to understand and address the security issues.

Penetration Testing Types

Penetration testing can also be categorized by the level of knowledge the tester has about the target system:

- ❑ **Black Box Testing:** The tester has no prior knowledge of the target system, simulating an external attacker.
- ❑ **White Box Testing:** The tester has full knowledge of the target system's internal structure, code, and configurations, simulating an insider threat or a developer with malicious intent.
- ❑ **Gray Box Testing:** The tester has some limited knowledge of the target system, such as user-level credentials or network diagrams.

Common Penetration Testing Tools

Penetration testers utilize a wide array of specialized tools to conduct their assessments. These tools range from *open-source* utilities to *commercial suites*, each designed to assist in different phases of the penetration testing process. Here are some of the most commonly used penetration testing tools:

- ❑ **Kali Linux:** A popular Debian-derived Linux distribution specifically designed for digital forensics and penetration testing. It comes pre-installed with hundreds of tools, making it a go-to operating system for security professionals.

Common Penetration Testing Tools

- ❑ **Nmap (Network Mapper):** A free and open-source utility for network discovery and security auditing. It is used to discover hosts and services on a computer network, thus creating a "map" of the network. Nmap can identify open ports, running services, operating systems, and device types.
- ❑ **Metasploit Framework:** A powerful open-source penetration testing framework that provides a platform for developing, testing, and executing exploits. It includes a vast database of exploits and payloads, making it invaluable for the exploitation phase of a pen test.

Common Penetration Testing Tools

- ❑ **Burp Suite:** A leading web vulnerability scanner and web proxy tool. It is widely used for web application penetration testing, allowing testers to intercept, inspect, and modify HTTP/S traffic, perform vulnerability scanning, and automate various attacks.
- ❑ **Wireshark:** A free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. In penetration testing, Wireshark helps in capturing and analyzing network traffic to identify sensitive information or unusual patterns.

Common Penetration Testing Tools

- ❑ **SQLmap:** An open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It supports a wide range of database management systems.
- ❑ **OWASP ZAP (Zed Attack Proxy):** A free and open-source web application security scanner. It is designed to be used by both those new to application security and professional penetration testers. It helps find vulnerabilities in web applications during the development and testing phases.

Ethical Considerations in Penetration Testing

- ❑ Penetration testing, while a crucial security practice, operates in a gray area between ethical hacking and malicious attacks. Therefore, a strong ethical framework is paramount to ensure that these tests are conducted responsibly, legally, and without causing unintended harm.

Ethical Considerations in Penetration Testing

- ❑ The following are key ethical considerations that every penetration tester and organization must adhere to:
- ❑ **Authorization and Consent:** This is the most fundamental ethical principle. Penetration testing must always be performed with the explicit, written consent of the organization that owns the system or network. The scope of the test, including the systems to be tested, the methods to be used, and the timeframe, must be clearly defined and agreed upon in a formal document, often called a "get out of jail free card."

Ethical Considerations in Penetration Testing

- ❑ **Legality and Compliance:** Penetration testers must be aware of and comply with all applicable laws and regulations. This includes national and international laws related to cybersecurity, data privacy (e.g., GDPR, HIPAA), and computer crime. Unauthorized access to computer systems is a criminal offense in most jurisdictions.
- ❑ **Confidentiality and Non-Disclosure:** During a penetration test, testers may gain access to sensitive and confidential information. They have a strict ethical and legal obligation to maintain the confidentiality of this information and not to disclose it to any unauthorized parties. A non-disclosure agreement (NDA) is typically signed as part of the engagement.

Ethical Considerations in Penetration Testing

- ❑ **Integrity and Honesty:** Penetration testers must act with integrity and honesty throughout the engagement. This includes accurately reporting all findings, not exaggerating risks, and providing unbiased recommendations for remediation. They should not use their skills for personal gain or to cause harm.
- ❑ **Do No Harm:** The primary goal of a penetration test is to identify vulnerabilities, not to cause damage. Testers must take great care to avoid disrupting business operations, corrupting data, or causing system downtime. The principle of proportionality should be applied, meaning the actions taken should be proportionate to the identified risks.

Cybersecurity Teams

Cybersecurity teams are specialized groups that work together to protect an organization's digital assets and infrastructure from threats. Modern security operations require different teams with specialized skills to effectively combat evolving cyber threats.

- ❑ Teams are organized by offensive and defensive functions
- ❑ Collaboration between teams enhances overall security posture
- ❑ Each team requires specific certifications and expertise
- ❑ Continuous adaptation to emerging threats is essential

Red Team - Offensive Security

A Red Team is a group of cybersecurity professionals who simulate real-world attacks to identify vulnerabilities in an organization's security defenses.

Red Teams adopt an adversarial mindset to challenge existing security controls and identify weaknesses before malicious actors can exploit them.

RED

Raxis performs a simulated, realistic cyber attack with the goal of an actual data breach



AVOID DETECTION

STAGING / WEAPONIZE

LATERAL MOVEMENT

CAPTURE DATA

BUILD DOCUMENTATION

Red Team - Offensive Security

Key Activities:

- ☐ Penetration Testing
- ☐ Vulnerability Exploitation
- ☐ Social Engineering
- ☐ Web Application Scanning
- ☐ Physical Security Testing

RED

Raxis performs a simulated, realistic cyber attack with the goal of an actual data breach



AVOID DETECTION

STAGING / WEAPONIZE

LATERAL MOVEMENT

CAPTURE DATA

BUILD DOCUMENTATION

Blue Team - Defensive Security

A Blue Team is responsible for defending an organization's systems and networks against cyber threats, both simulated and real.

Blue Teams focus on detection, response, and recovery to maintain the security posture and protect critical assets from compromise.



Blue Team - Defensive Security

Key Activities:

- ☐ Security Monitoring
- ☐ Threat Detection
- ☐ Incident Response
- ☐ Security Controls Implementation
- ☐ Security Metrics & Reporting



Purple Team - Collaborative Security

A Purple Team is the integration of Red and Blue Team objectives, creating a collaborative approach to improve an organization's overall security posture.

Purple Teams focus on knowledge transfer and continuous improvement by combining offensive tactics with defensive strategies.

Benefits of Purple Team Approach:

- ☐ Real-time feedback between attackers and defenders
- ☐ Enhanced learning and skill development
- ☐ Targeted security improvements
- ☐ Measurable security posture enhancement

Zero Trust Architecture

"Never Trust, Always Verify"

- ☐ The traditional "**Castle and Moat**" security model assumes everything inside the network is safe. In a world of remote work and cloud apps, the perimeter has dissolved.
- ☐ **Zero Trust** assumes breach and verifies every request as if it originates from an open network, regardless of where the request comes from or what resource it accesses.

Three Core Principles



Verify Explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, and data classification.



Least Privilege Access

Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection to secure both data and productivity.



Assume Breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

The 5 Pillars of Zero Trust

- ✓ **Identity:** Continuous validation (MFA, behavioral analytics).
- ✓ **Devices:** Real-time health, patch status, and compliance.
- ✓ **Network:** Micro-segmentation, encryption, software-defined perimeters.
- ✓ **Applications:** Securing workloads, containers, and hypervisors.
- ✓ **Data:** Data tagging, classification, and encryption at rest/transit.

The Implementation Journey

Zero Trust is a **strategy**, not a product. It requires a phased evolution.

1

Traditional

Manual configurations, static security policies, broad network segmentation, proprietary solutions, dependency on perimeter ownership.

2

Advanced

Cross-pillar policy enforcement, centralized identity and visibility, some automation, response to pre-defined triggers.

3

Optimal

Fully automated, dynamic policies based on real-time risk, self-healing networks, continuous authorization, machine learning-driven analytics.

Summary

- ❑ Information Security Governance
- ❑ Risk Management and Security Frameworks
- ❑ Penetration Testing
- ❑ Cybersecurity Teams



Thank You

