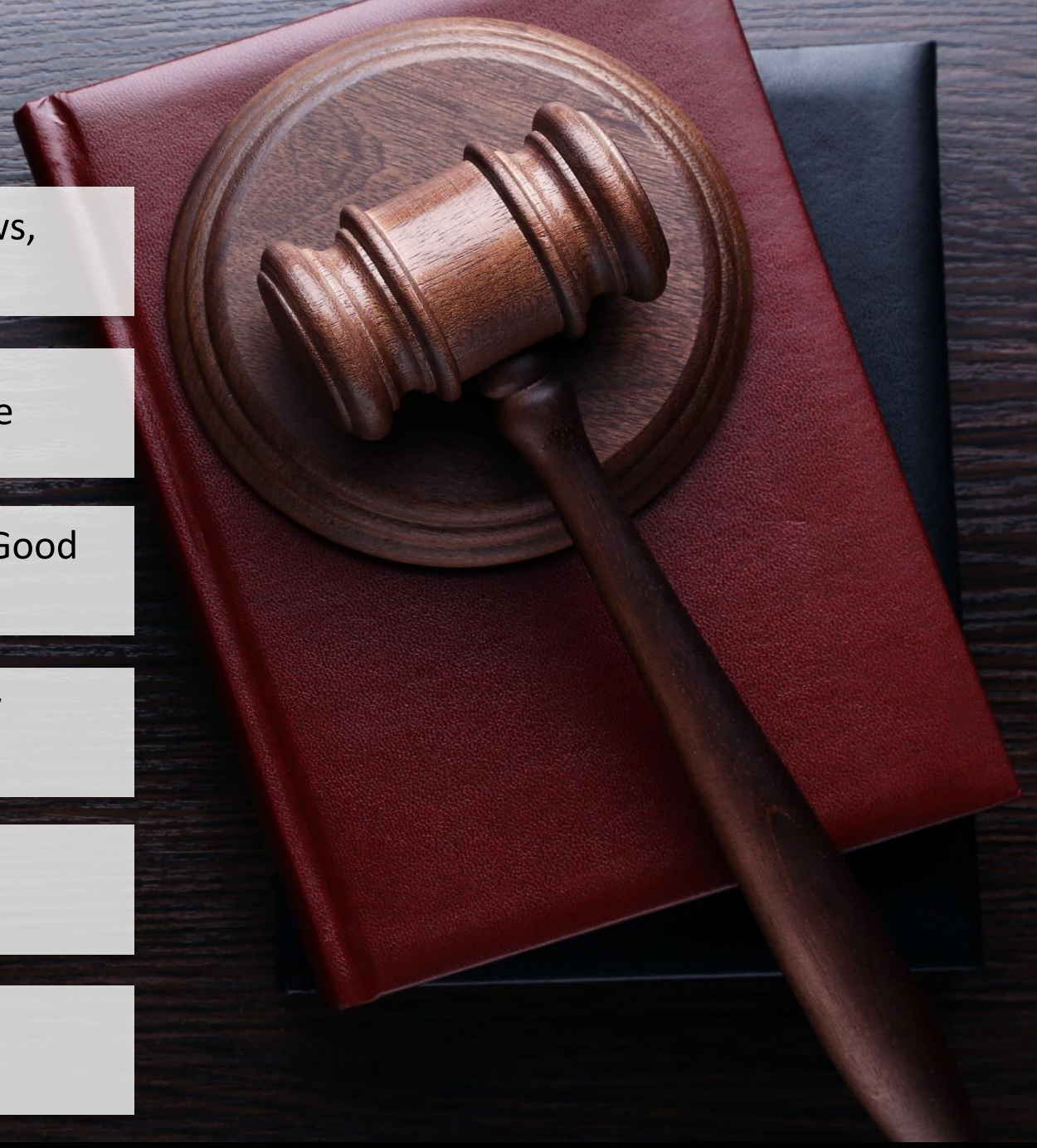

N|DE
Network Defense Essentials
Module 03
Network Security Controls - Administrative Controls

Module Objectives

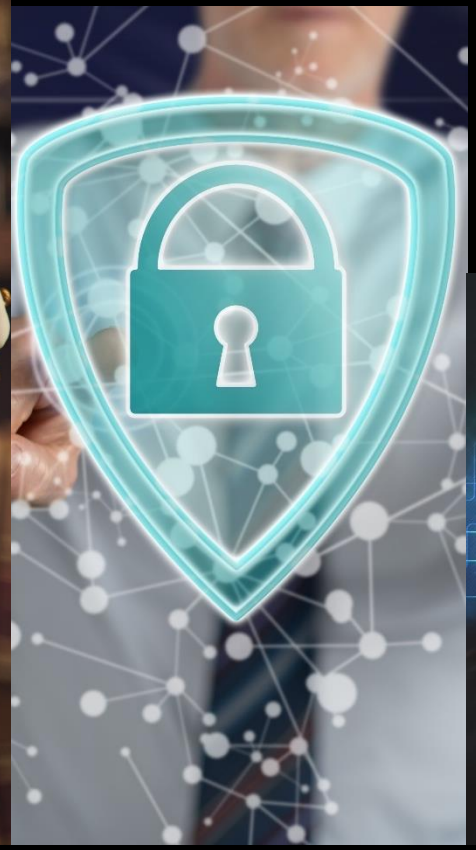
1. Understanding Various Regulatory Frameworks, Laws, and Acts
2. Understanding Why Organizations Need Compliance
3. Understanding the Need for and Characteristics of Good Security Policy
4. Understanding How to Design and Develop Security Policies
5. Overview of Different Types of Security Policies
6. Understanding the Different Types of Security and Awareness Training



Module Flow



1. **Discuss Various Regulatory Frameworks, Laws, and Acts**

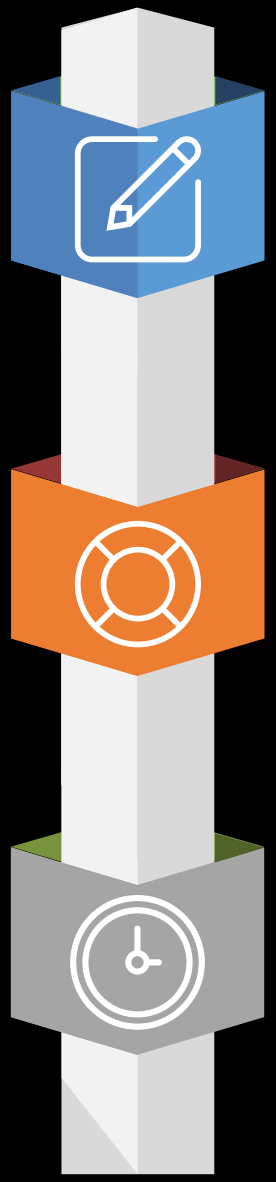


2. Learn to Design and Develop Security Policies



3. Learn to Conduct Different Types of Security and Awareness Training

Regulatory Frameworks Compliance



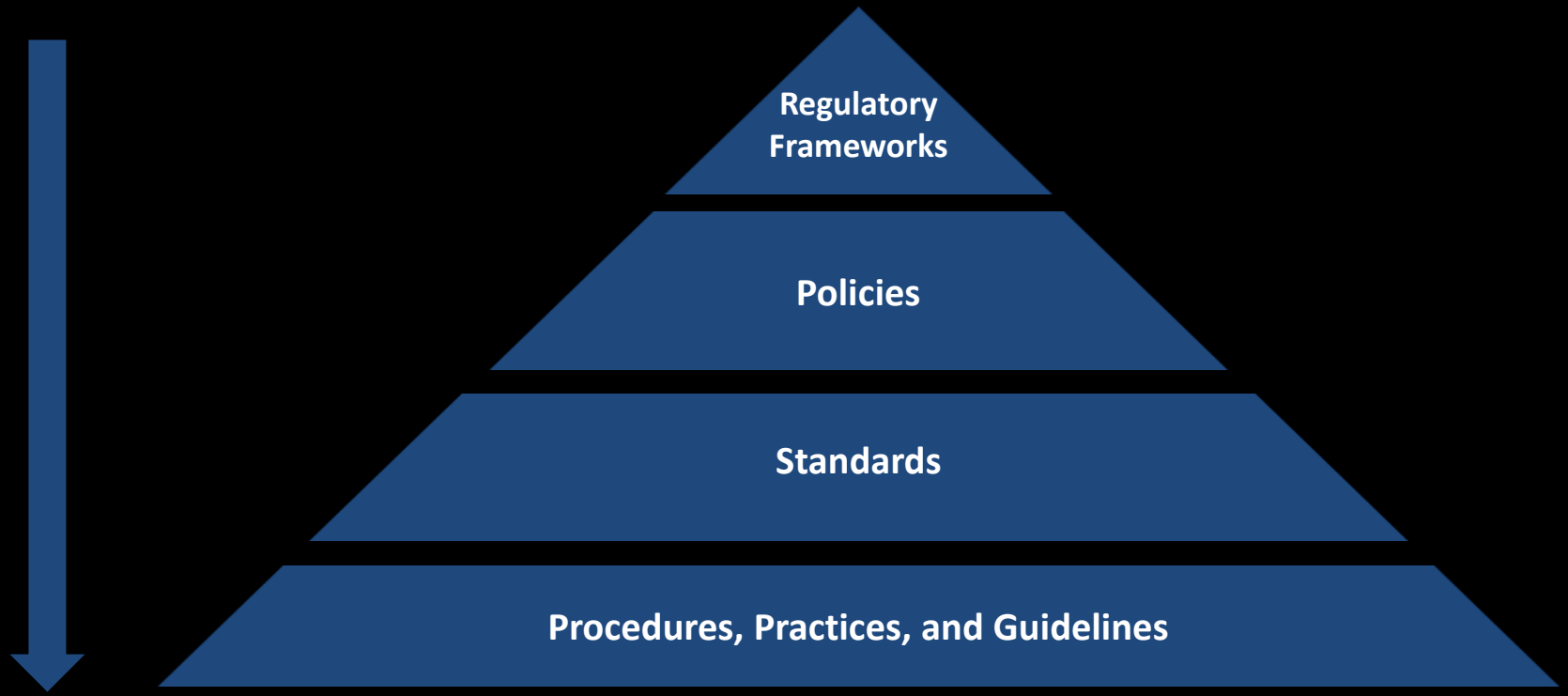
security regulation

collaborative effort
improvements

guidelines best practices

Regulatory Frameworks Compliance (Cont'd)

Role of Regulatory Frameworks Compliance in an Organization's Administrative Security



Why Organizations Need Compliance



Improves Security

- IT security **regulation** and **standards** improve overall security of an organization by meeting regulatory requirements

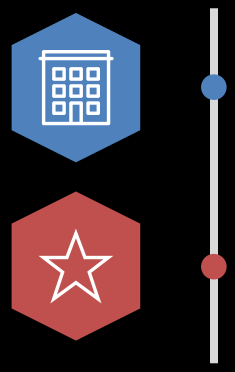
Minimize Losses

- Improved security, in turn, **prevents** security breaches, which can cost loss to company

Maintain Trust

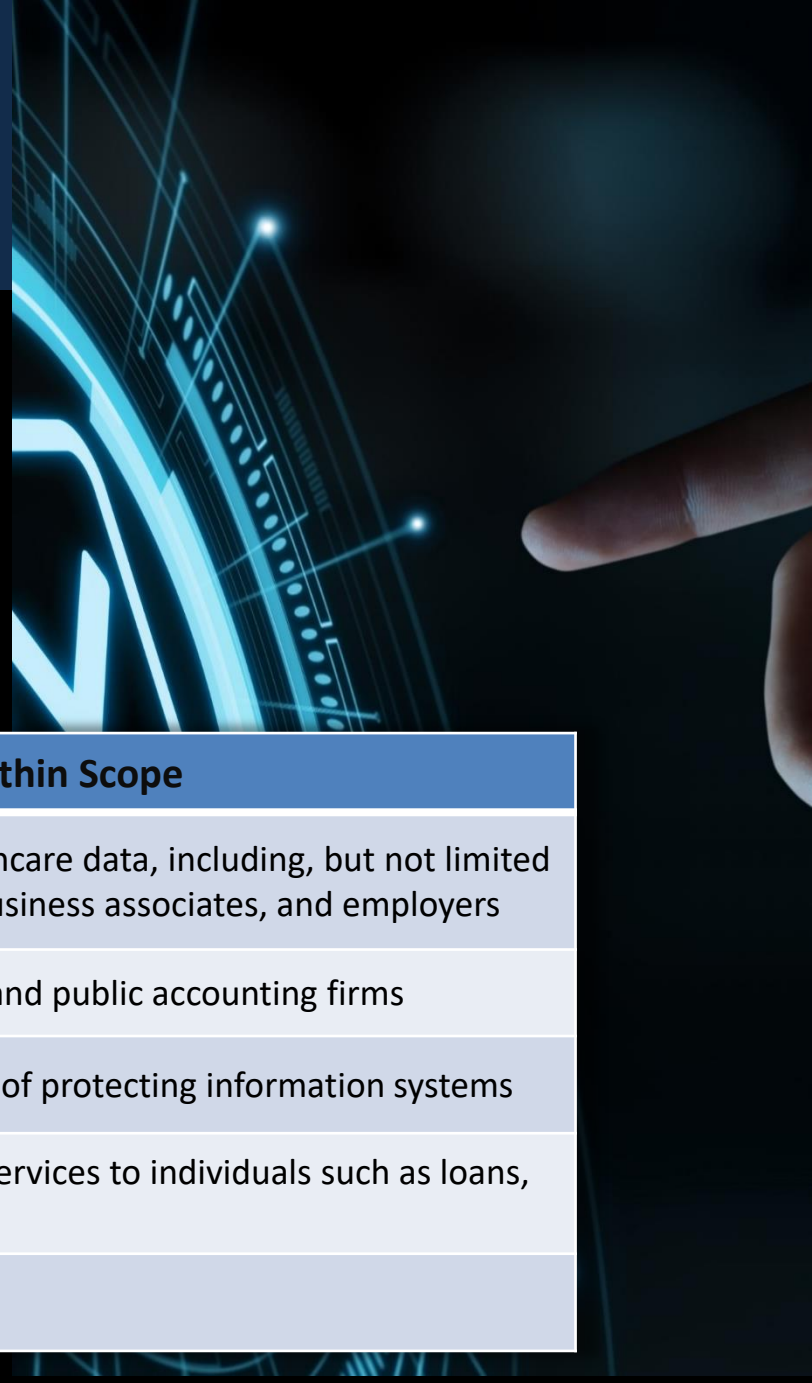
- Customer trusts the organization in belief that their information is **safe**

Identifying Which Regulatory Framework to Comply



assess

scope



Regulatory Framework	Organizations within Scope
Health Insurance Portability and Accountability Act (HIPAA)	Any company or office that deals with healthcare data, including, but not limited to, doctor's offices, insurance companies, business associates, and employers
Sarbanes Oxley Act	U.S. public company boards, management, and public accounting firms
Federal Information Security Management Act of 2002 (FISMA)	All federal agencies must develop a method of protecting information systems
Gramm Leach Bliley Act (GLBA)	Companies that offer financial products or services to individuals such as loans, financial or investment advice, or insurance
Payment Card Industry Data Security Standard (PCI-DSS)	Companies handling credit card information

Deciding on How to Comply to Regulatory Framework

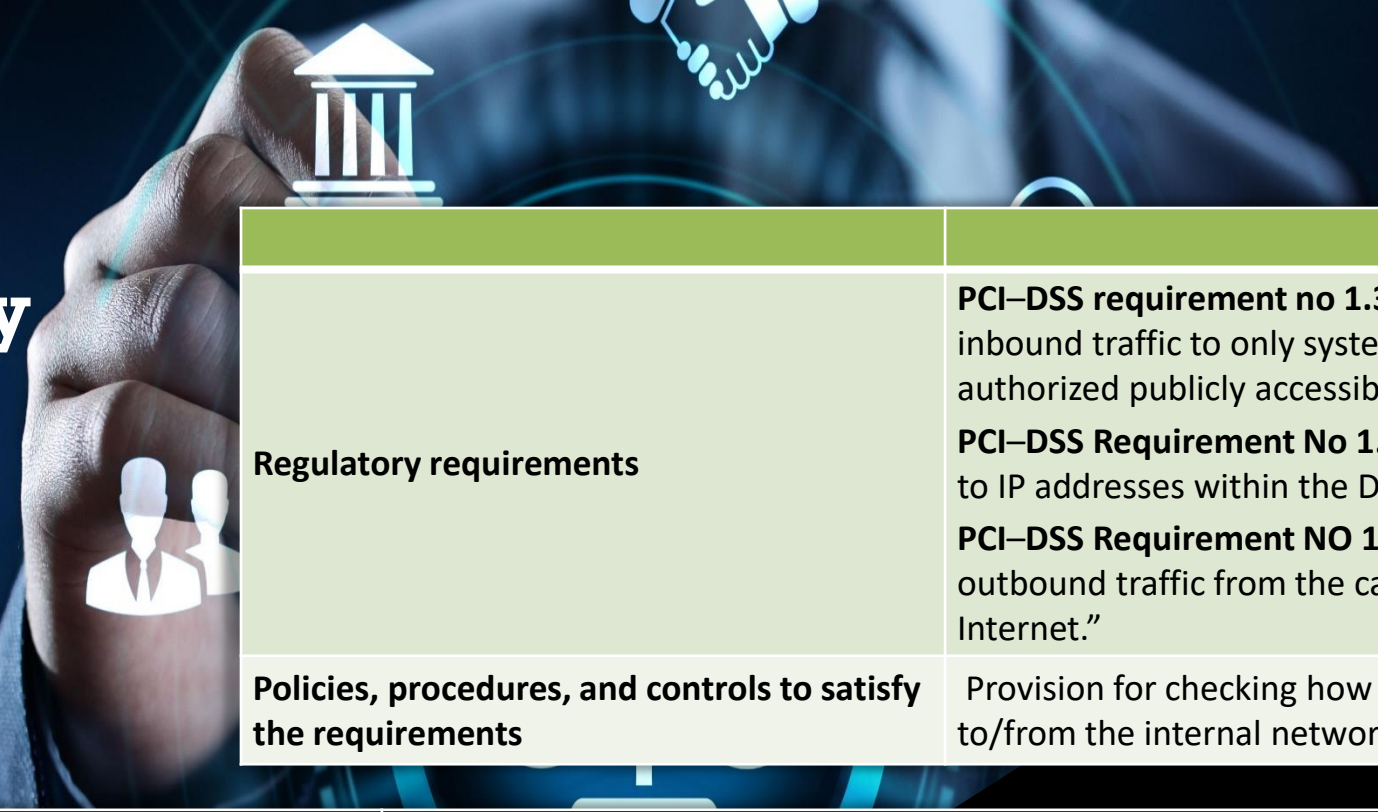
- When an organization falls within scope of certain regulatory framework, it needs to correctly **interpret** regulatory requirements in the regulator framework to be complied with
- Based on those regulatory requirements, an organization needs to establish **policies**, **procedures**, and **security controls** to manage and maintain compliance

For example, the following table shows some of the PCI–DSS regulatory requirements:

	PCI-DSS
Regulatory requirements	**PCI–DSS requirement No 1.1.1**: "A formal process for approving and testing all network connections and changes to the firewall and router configurations." **PCI–DSS Requirement No 1.2.1**: "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic."
Policies, procedures, and controls to satisfy the requirements	Provision for detecting all unauthorized network connections to/from an organization's IT assets

	PCI-DSS
Regulatory requirements	**PCI–DSS requirement no 1.1.6**: "Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure."
Policies, procedures, and controls to satisfy the requirements	Provision for looking insecure protocols and services running on systems

Deciding on How to Comply to Regulatory Framework (Cont'd)



	PCI-DSS
Regulatory requirements	**PCI–DSS requirement no 1.3.1:** "Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports." **PCI–DSS Requirement No 1.3.2:** "Limit inbound Internet traffic to IP addresses within the DMZ." **PCI–DSS Requirement NO 1.3.5:** "Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet."
Policies, procedures, and controls to satisfy the requirements	Provision for checking how traffic is flowing across the DMZ to/from the internal network

	PCI-DSS
Regulatory requirements	**PCI–DSS requirement no 5.1:** "Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)." **PCI–DSS requirement no 5.3:** "Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period."
Policies, procedures, and controls to satisfy the requirements	Provision for detecting malware infection when anti-virus protection is disabled on the machines



Regulatory Frameworks, Laws, and Acts

Payment Card Industry Data Security Standard (PCI–DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary **information security standard for organizations** that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards

PCI DSS **applies to all entities involved in payment card processing** — including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data

PCI Data Security Standard — High Level Overview

- **Build and Maintain a Secure Network**
- **Maintain a Vulnerability Management Program**
- **Regularly Monitor and Test Networks**
- **Protect Cardholder Data**
- **Implement Strong Access Control Measures**
- **Maintain an Information Security Policy**

Failure to meet the PCI DSS requirements may result in fines or the termination of payment card processing privileges

Health Insurance Portability and Accountability Act (HIPAA)



HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Set Standards

Requires every provider who does business electronically to **use the same health care transactions**, **code sets**, and **identifiers**

Privacy Rule

Provides **federal protections for the personal health information** held by covered entities and gives patients an array of rights with respect to that information

Security Rule

Specifies a series of administrative, physical, and technical safeguards for covered entities to use to ensure the **confidentiality**, **integrity**, and **availability of electronically protected health information**

National Identifier Requirements

Requires that health care providers, health plans, and employers have standard national numbers that identify them attached to **standard transactions**

Enforcement Rule

Provides the standards for enforcing all the **Administration Simplification Rules**

https://www.hhs.gov

Sarbanes Oxley Act (SOX)



- Enacted in 2002, the Sarbanes-Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures
- The key requirements and provisions of SOX are organized into **11 titles**:

Title I

Public Company Accounting Oversight Board (PCAOB) provides independent oversight of public accounting firms providing audit services ("auditors")

Title II

Auditor Independence establishes the standards for external auditor independence, intended to limit conflicts of interest and address new auditor approval requirements, audit partner rotation, and auditor reporting requirements

Title III

Corporate Responsibility mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports

https://www.sec.gov

Sarbanes Oxley Act (SOX) (Cont'd)



Title IV

Enhanced Financial Disclosures describe enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers

Title V

Analyst Conflicts of Interest consist of measures designed to help restore investor confidence in the reporting of securities analysts

Title VI

Commission Resources and Authority defines practices to restore investor confidence in securities analysts

Title VII

Studies and Reports includes the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing, or others to manipulate earnings and obfuscate true financial conditions

Sarbanes Oxley Act (SOX) (Cont'd)

Title VIII

Corporate and Criminal Fraud Accountability describes specific criminal penalties for fraud by the manipulation, destruction, or alteration of financial records, or other interference with investigations while providing certain protections for whistle-blowers

Title X

White Collar Crime Penalty Enhancement increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds the failure to certify corporate financial reports as a criminal offense

Title IX

Corporate Tax Returns states that the Chief Executive Officer should sign the company tax return

Title XI

Corporate Fraud Accountability identifies corporate fraud and record tampering as criminal offenses and assigns them specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments



Gramm-Leach-Bliley Act (GLBA)



- The objective of the **Gramm–Leach–Bliley Act** was to ease the transfer of **financial** information between **institutions** and **banks** while making the rights of the individual more specific through **security** requirements

Key Points include:

personal financial

information

$10,000 for each violation

General Data Protection Regulation (GDPR)



- GDPR regulation was put into effect on May 25, 2018 and one of the **most stringent privacy and security laws globally**
- The GDPR will **levy harsh fines** against those who violate its privacy and security standards, with penalties reaching tens of millions of euros

GDPR Data Protection Principles



Data Protection Act 2018 (DPA)

- The DPA is an act to make provision for the regulation of the processing of information relating to **individuals**; to make provision in connection with the **Information Commissioner's functions** under specific regulations relating to information; to make provision for a direct **marketing code** of practice, and connected purposes

The DPA **protects individuals** concerning the processing of personal data, in particular by:

Requiring **personal data to be processed lawfully** and fairly, based on the data subject's consent or another specified basis,

Conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and

Conferring functions on the Commissioner, giving the holder of that office responsibility to monitor and enforce their provisions

https://www.legislation.gov.uk

ISO Information Security Standards

Sr. No.	Standards	Objective
1	ISO/IEC 27001	Formal ISMS specification
2	ISO/IEC 27002	Information security controls
3	ISO/IEC 27003	ISMS implementation guide
4	ISO/IEC 27004	Information security metrics
5	ISO/IEC 27005	Information security risk management
6	ISO/IEC 27006	ISMS certification guide
7	ISO/IEC 27007	Management system auditing
8	ISO/IEC TR 27008	Technical auditing
9	ISO/IEC 27010	For inter-organization communication
10	ISO/IEC 27011	Iso27k in telecoms
11	ISO/IEC 27013	ISMS & ITIL/service management
12	ISO/IEC 27014	Information security governance
13	ISO/IEC TR27015	Iso27k in financial services
14	ISO/IEC TR 27016	Information security economics
15	ISO/IEC 27017	Cloud security controls

Sr. No.	Standards	Objective
16	ISO/IEC 27018	Cloud privacy
17	ISO/IEC TR 27019	Process control in energy
18	ISO/IEC 27031	ICT business continuity
19	ISO/IEC 27032	Cybersecurity
20	ISO/IEC 27033-1 to -5	Network security
21	ISO/IEC 27034 -1 & -5	Application security
22	ISO/IEC 27035	Incident management
23	ISO/IEC 27036-1 -2 & -3	ICT supply chain
24	ISO/IEC 27037	Digital evidence [forensics]
25	ISO/IEC 27038	Document reduction
26	ISO/IEC 27039	Intrusion prevention
27	ISO/IEC 27040	Storage security
28	ISO/IEC 27041	Investigation assurance
29	ISO/IEC 27042	Analyzing digital evidence
30	ISO/IEC 27043	Incident investigation
31	ISO 27799 ISO27k	In healthcare

https://www.iso27001security.com

The Digital Millennium Copyright Act (DMCA)



- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO)
- It **defines the legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information

https://www.copyright.gov

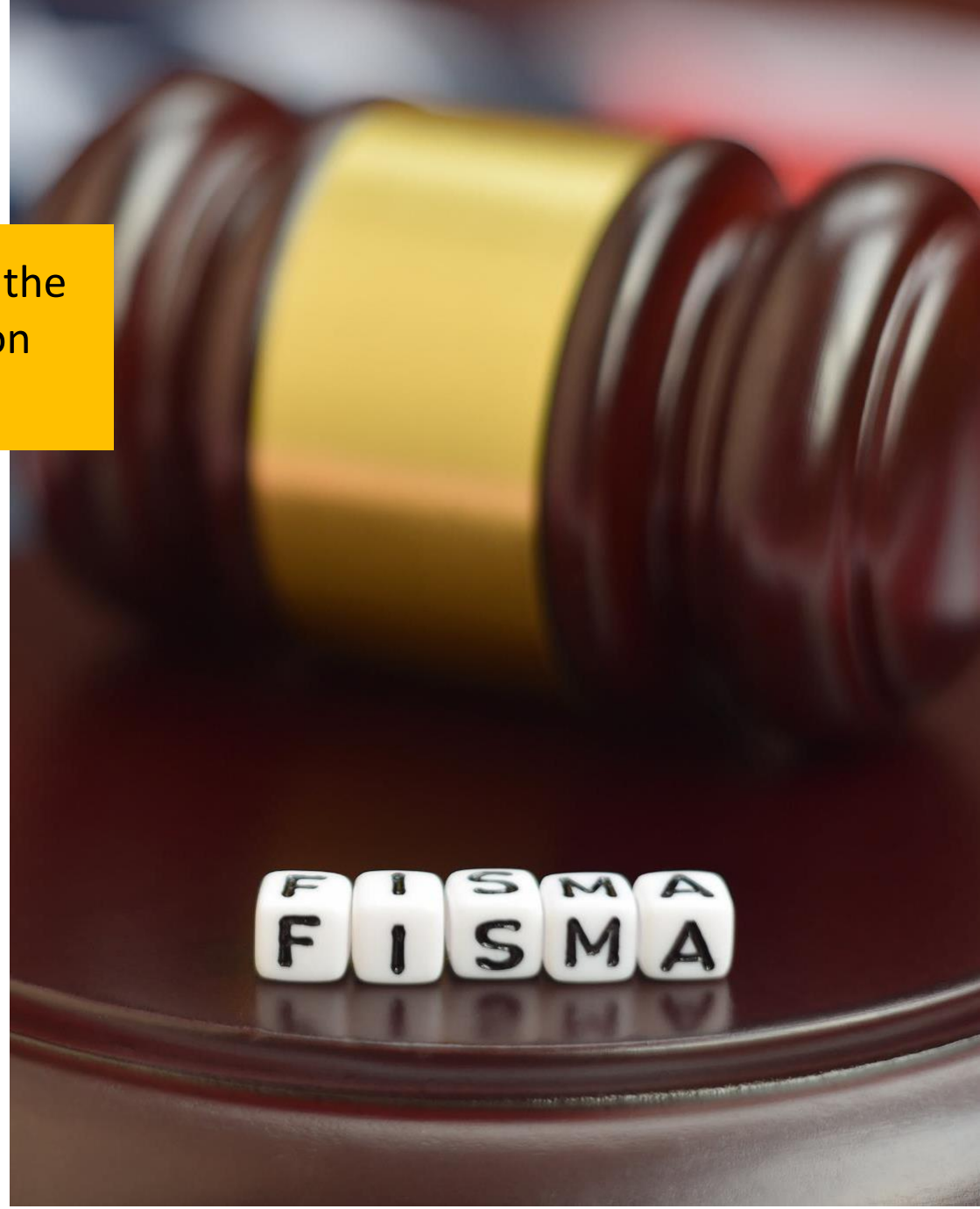
The Federal Information Security Management Act (FISMA)

The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets

It includes

- Standards for categorizing information and information systems by mission impact
- Standards for minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems
- Guidance for assessing security controls in information systems and determining security control effectiveness
- Guidance for security authorization of information systems

https://csrc.nist.gov



Other Information Security Acts and Laws

1. USA Patriot Act 2001
2. Freedom of Information Act (FOIA)
3. The Electronic Communications Privacy Act
4. The Human Rights Act 1998
5. The Freedom of Information Act 2000
6. Computer Fraud and Abuse Act

Cyber Law in Different Countries



Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	*https://www.copyright.gov*
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	*https://www.uspto.gov*
	Foreign Intelligence Surveillance Act	*https://fas.org*
	Protect America Act of 2007	*https://www.justice.gov*
	Privacy Act of 1974	*https://www.justice.gov*
	National Information Infrastructure Protection Act of 1996	*https://www.nrotc.navy.mil*
	Computer Security Act of 1987	*https://csrc.nist.gov*
	Federal Identity Theft and Assumption Deterrence Act	*https://www.ftc.gov*

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	*https://www.legislation.gov.au*
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	*https://www.legislation.gov.uk*
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
	The Network and Information Systems Regulations 2018	
	Communications Act 2003	
	The Privacy and Electronic Communications (EC Directive) Regulations 2003	
	Investigatory Powers Act 2016	
	Regulation of Investigatory Powers Act 2000	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	*http://www.npc.gov.cn*
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	*http://www.ipindia.nic.in*
	Information Technology Act	*https://www.meity.gov.in*
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	*https://www.cybercrimelaw.net*



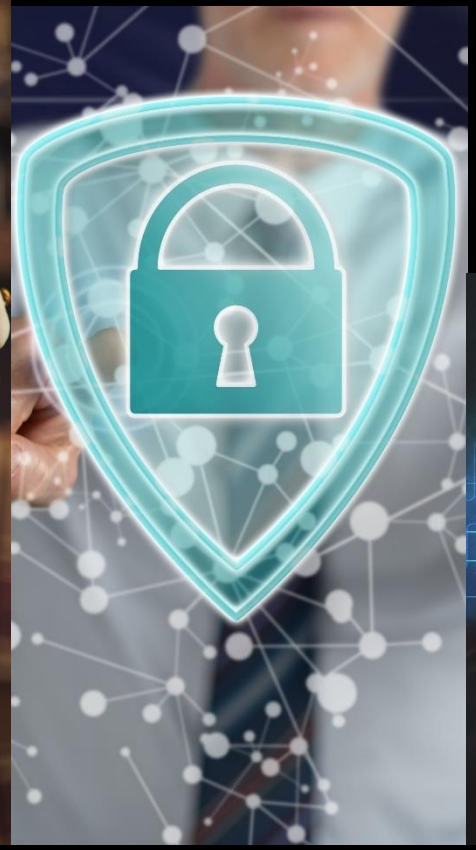
Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	*https://www.cybercrimelaw.net*
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	*https://www.iip.or.jp*
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	*https://laws-lois.justice.gc.ca*
Singapore	Computer Misuse Act	*https://sso.agc.gov.sg*
South Africa	Trademarks Act 194 of 1993	*http://www.cipc.co.za*
	Copyright Act of 1978	*https://www.nlsa.ac.za*
South Korea	Copyright Law Act No. 3916	*https://www.copyright.or.kr*
	Industrial Design Protection Act	*https://www.kipo.go.kr*
Belgium	Copyright Law, 30/06/1994	*https://www.wipo.int*
	Computer Hacking	*https://www.cybercrimelaw.net*
Brazil	Unauthorized modification or alteration of the information system	*https://www.domstol.no*
Hong Kong	Article 139 of the Basic Law	*https://www.basiclaw.gov.hk*

Module Flow



1. Discuss Various Regulatory Frameworks, Laws, and Acts



2. **Learn to Design and Develop Security Policies**



3. Learn to Conduct Different Types of Security and Awareness Training

What is Security Policy?

- A security policy is a **well-documented** set of plans, processes, procedures, standards, and guidelines required to establish an ideal information security status of an organization
- Security policies are used to inform people on how to work in a safe and secure manner; they define and guide employee actions on how to deal with organization sensitive operation, data, or resources
- The security policy is an **integral** part of an information security management program for any organization



Need for a Security Policy

security principles

information security standards

exposure

secure environment



legal protection

impact

data breach

Advantages of Security Policies

- Enhanced Data and Network Security





- Better Network Performance

- Risk Mitigation





- Quick Response to Issues and Lower Downtime

- Monitored and Controlled Device Usage and Data Transfers





- Reduction in Management Stress Levels

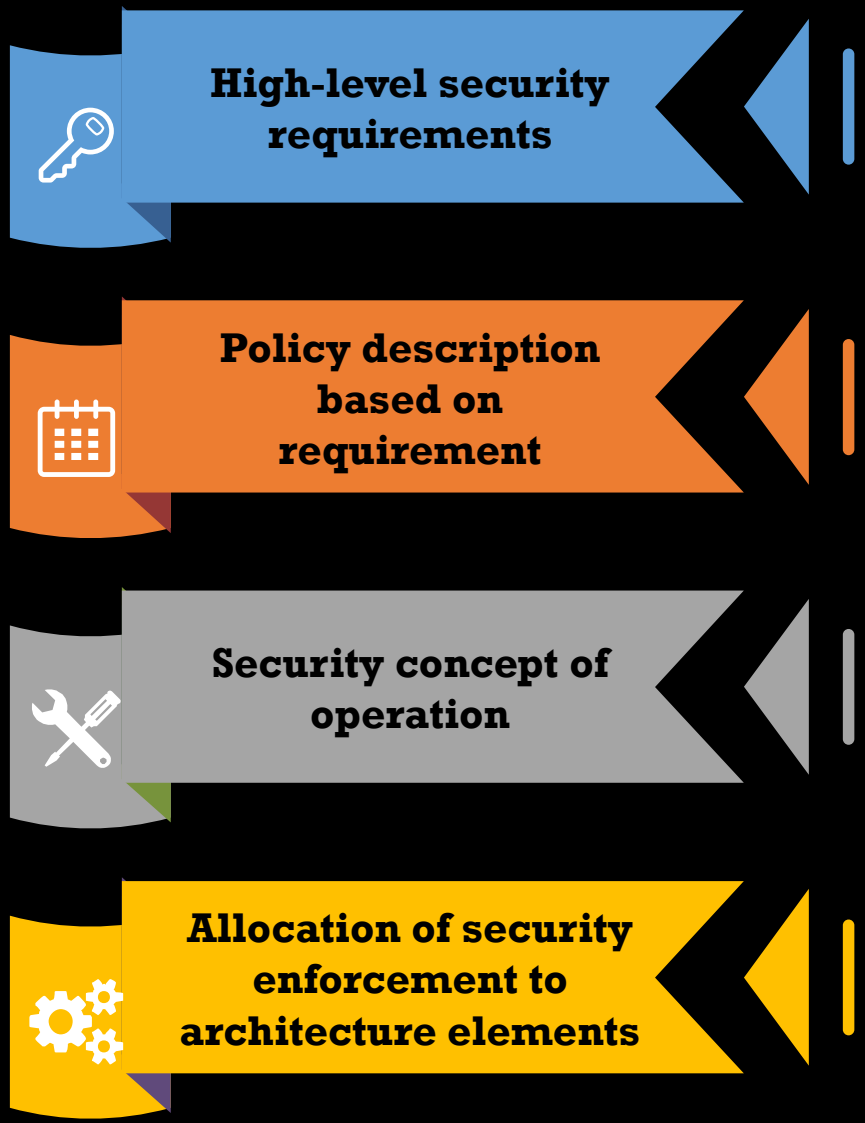
Characteristics of a Good Security Policy

- Concise and Clear
- Usable
- Economically Feasible
- Understandable
- Realistic
- Consistent
- Procedurally Tolerable
- Legal Compliance
- Based on Standards and Regulations

Key Elements of Security Policy



Contents of a Security Policy



requirements

safeguards

roles responsibilities functions

architecture allocation

Typical Policy Document Content



Types of Information Security Policies

Enterprise Information Security Policy (EISP)

- EISP drives an organization's scope and provides direction to their security policies

Examples of EISP:

- ✓ Application policy
- ✓ Network and network device security policy
- ✓ Back up and restore policy
- ✓ System security policy

Issue Specific Security Policy (ISSP)

- ISSP directs the audience on the usage of technology-based systems with the help of **guidelines**

Examples of ISSP:

- ✓ Remote access and wireless policies
- ✓ Incident response plan
- ✓ Password policies
- ✓ Policies for personal devices

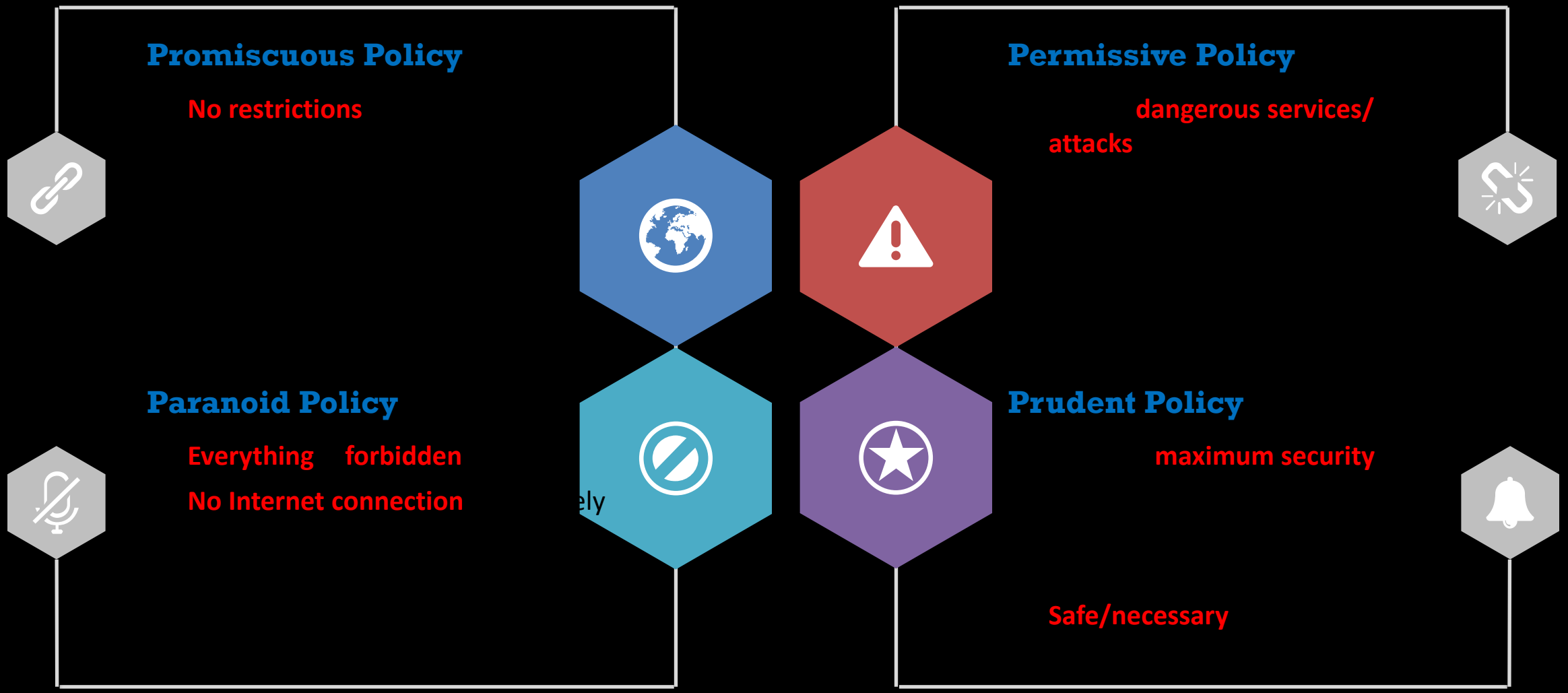
System Specific Security Policy (SSSP)

- SSSP directs users while **configuring or maintaining** a system

Examples of SSSP:

- ✓ DMZ policy
- ✓ Encryption policy
- ✓ Policies for Intrusion detection and prevention
- ✓ Access control policy

Internet Access Policies



Password Policy

Password policy provides guidelines for using strong passwords for an organization's resources

Design Considerations

01 Password length and formation

02 Complexity of password

03 Password blacklists

04 Password duration

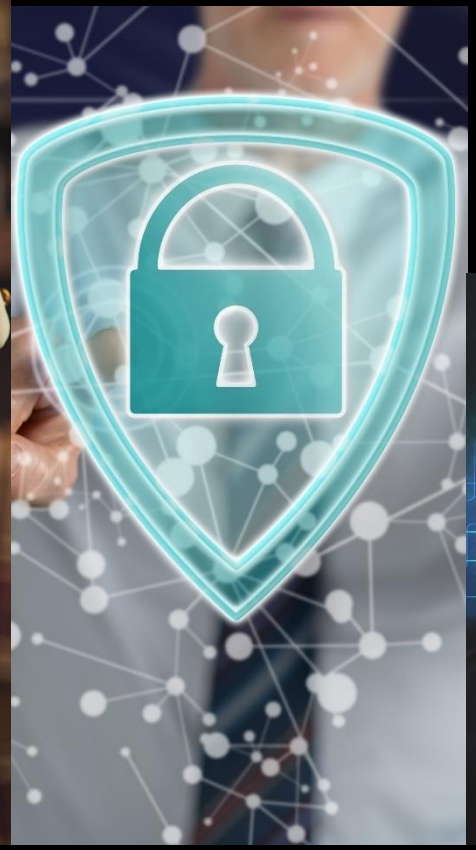
05 Common password practice



Module Flow



1. Discuss Various Regulatory Frameworks, Laws, and Acts



2. Learn to Design and Develop Security Policies



3. **Learn to Conduct Different Types of Security and Awareness Training**

Employee Awareness and Training

- An organization need to provide **formal security awareness training** for its employees when they join and periodically thereafter, so employees
  - Know **how to defend** themselves and the organization against threats
  - **Follow security policies** and procedures for working with IT
  - Know **whom to contact** if they discover a security threat
  - Can identify the **nature of the data** based on data classification
  - Protect physical and **informational assets** of that organization



Different methods to train employees are:



Employee Awareness and Training: Security Policy



perform

training

Advantages

Effective **implementation** of a security policy

Policies are followed and not just **enforced**

Creates **awareness** on compliance issues

Helps an organization **enhance** its network security

Employee Awareness and Training: Physical Security

educate employees

Training should educate employees about how to:



Employee Awareness and Training: Social Engineering



combat

But I must explain to you how all this mistaken idea

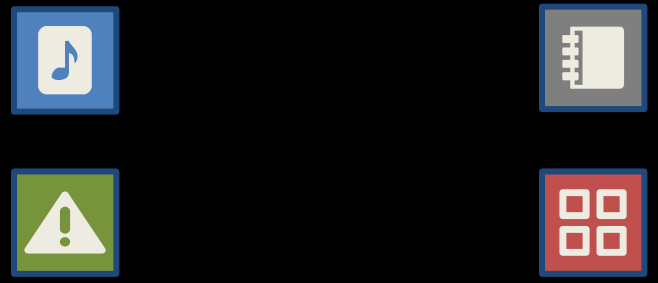
Areas of Risk	Attack Techniques	Train employee/Help Desk on:
Phone	Impersonation	• Not providing any confidential information, if this has occurred
Dumpsters	Dumpster Diving	• Not throwing sensitive documents in the trash • Shredding document before putting into the trash • Erasing magnetic data before putting into the trash
Email	Phishing, malicious attachment	• Differentiating between legitimate email and a targeted phishing email • Not downloading malicious attachment

Employee Training and Awareness: Data Classification

- Organization should train employees on how to tell if information is confidential

Areas of Risk	Attack Techniques	Train employee/Help Desk on
Office	Stealing sensitive information	How to classify and mark document-based classification levels and keep sensitive document in secured place

Typical Information classification levels:





- Security labels are used to mark the **security level requirements** for the information assets and controls access to it
- Organizations use security labels to manage access clearance to their information assets

Module Summary

