Chapter 1

Risk Management

Episode 1.01

Episode title: **Defining Risk**

Objective: **1.5 Explain different threat actors, vectors, and intelligence sources.**

Risk Management

- Risk is the likelihood of a threat actor taking advantage of a vulnerability by using a threat against an IT asset

Threat Actors

- Hackers
- Hacktivists
- Script kiddies
- Insiders
- Competitors
- Shadow IT
- Criminal syndicates
- State actors
- Advanced persistent threat (APT)

Quick Review

- Risk is the likelihood of a threat actor taking advantage of a vulnerability by using a threat against an IT asset
- An asset is any part of an IT infrastructure that has value
- Likelihood is the probability of assets being damaged over time
- A threat actor is anyone or anything with the motive and resources to attack another's IT infrastructure
- A vulnerability is a weakness in an asset
- A threat is an action that a threat actor can use against a vulnerability to cause harm

Episode 1.02

Episode title: **Threats and Vulnerabilities**

Objective: **1.5 Explain different threat actors, vectors, and intelligence sources.**

Vulnerability and Threat

- Vulnerability
  - A weakness inherent in an asset that leaves it open to a threat
- Threat
  - An attack (exploit) that a malicious actor will use against an asset

Threat Actors

- Individuals or organizations who perpetrate attacks against vulnerabilities
- Example: script kiddies

Attack Vectors

- Pathways to gain access to infrastructure
  - Weak configurations
  - Open firewall ports
  - Lack of user security awareness
  - Lack of multifactor authentication
  - Missing patches
    - Equifax hack
  - Infected USB thumb drives
    - Stuxnet worm

Attack Vectors

- Supply-chain attack
  - Manufacturers
  - Contractors
  - Implementers
  - Outsourced software development
    - Right-to-audit clause

Quick Review

- Vulnerabilities are weaknesses of an asset in an IT system
- Exploits take advantage of vulnerabilities
- Threat actors are the sources of threats
- Attack vectors are pathways to gain access to restricted systems

Episode 1.03

Episode title: **Threat Intelligence**

Objective: **1.5 Explain different threat actors, vectors, and intelligence sources.**

Threat Intelligence Sources

- Facilitate risk management
- Hardening can reduce incident response time
- Provide cybersecurity insight
  - Adversary tactics, techniques, and procedures (TTP)
  - Threat maps
    - Example: geographical representations of malware outbreaks

Threat Intelligence Sources

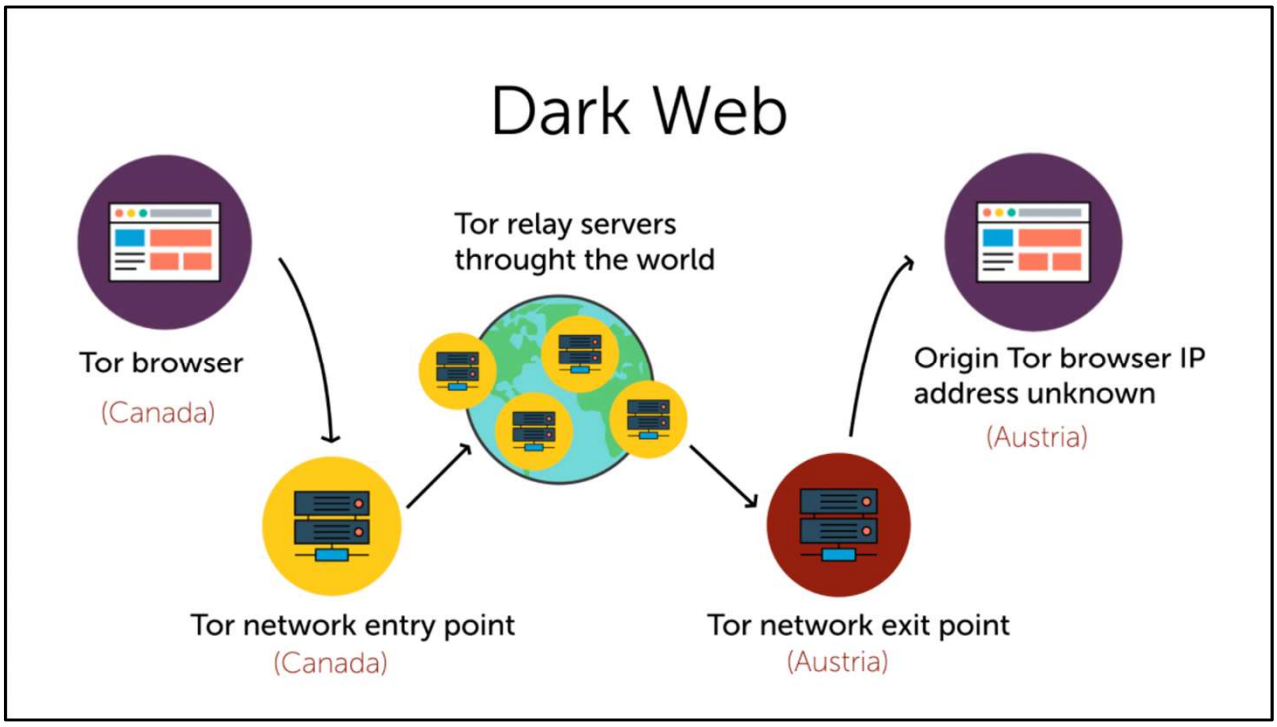
- Closed/proprietary
- OSINT (open-source intelligence)
  - Government reports
  - Media
  - Academic papers

Threat Intelligence Sources

- Closed/proprietary
- File/code repositories
  - Example: GitHub
- Vulnerability databases
  - Common Vulnerabilities and Exposures (CVEs)

Threat Intelligence Sources

- Dark Web/dark net
  - Tor network, Tor Web browser
  - Encrypted anonymous connections
  - Not indexed by search engines
  - Tor encryption and anonymity
    - Journalists
    - Law enforcement
    - Government informants


Dark Web
Tor relay servers throught the world
Tor browser
(Canada)
Origin Tor browser IP address unknown
(Austria)
Tor network entry point
(Canada)
Tor network exit point
(Austria)

Threat Intelligence Sharing

- Automated Indicator Sharing (AIS)
  - Exchange of cybersecurity intelligence (CI) between entities
- Structured Threat Information eXpression (STIX)
  - A form of AIS
  - Data exchange format for cybersecurity intelligence

Threat Intelligence Sharing

- Trusted Automated eXchange of Intelligence Information (TAXII)
  - Like RSS feed for threats
  - Consists of TAXII servers and clients
  - Real-time cyber intelligence feeds

Quick Review

- OSINT (open-source intelligence) refers to public cybersecurity intelligence sources
- The Common Vulnerabilities and Exposures (CVE) database is an example of OSINT
- The Dark Web is an encrypted and anonymized Internet access mechanism allowing access to unindexed content
- STIX is a cybersecurity intelligence (CI) sharing format; TAXII exchanges CI

Episode 1.04

Episode title: **Risk Management Concepts**

Objective: **5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.**

Risk Vector

- Mission-critical IT systems
  - Payment processing
  - Human resources
  - Emergency
- Sensitive data
  - Do we know what we have and where it is?
- Third-party access

Physical Risk Vectors

- Access control vestibules (mantraps)
- Server room access
- Limit USB bootable devices

Risk Management Frameworks (RMFs)

- Center for Internet Security (CIS)
  - Cybersecurity best practices
- NIST Risk Management Framework (RMF)/Cybersecurity Framework (CSF)
  - Cybersecurity risk management

Risk Management Frameworks (RMFs)

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC)
  - 27001/27002/27701/ 31000
    - IT system and information security

Financial RMFs

- Statement on Standards for Attestation Engagements System and Organization Controls (SSAE SOC 2)
  - Financial statement integrity
  - Internal controls
  - Type I and Type II

RMFs

- NIST Special Publication (SP) 800-30, Rev. 1
  - "Guide for Conducting Risk Assessments"
  - https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Data Privacy Regulations and Standards

- General Data Protection Regulation (GDPR)
  - Protects EU citizens' private data
- Health Insurance Portability and Accountability Act (HIPAA)
  - Protect American patient medical information

Data Privacy Regulations and Standards

- Payment Card Industry Data Security Standard (PCI DSS)
  - Protect cardholder information
  - https://www.pcicomplianceguide.org/faq/

Types of Security Policies

- Acceptable use policy (AUP)
  - E-mail, social media, Web browsing
- Resource access policies
  - App or file access
- Account policies
  - Account hardening

Types of Security Policies

- Data retention policies
  - Often dictated by regulations
- Change control policies
- Asset management policies

Quick Review

- Risk management frameworks (RMFs) provide guidance on identifying and managing risk
- Security regulations and standards such as GDPR, HIPAA, and PCI DSS are designed to protect sensitive data
- Organization security policies are designed to protect assets

Episode 1.05

Episode title: **Security Controls**

Objective: **5.1 Compare and contrast various types of controls.**

Security Controls

- Solution that mitigates threat
- Example: Malware scanner mitigates malware infections
- Implemented differently based on platform/ vendor/user
  - Network infrastructure devices
    - Switches, routers, firewalls

Security Control Categories

- Managerial/administrative
  - What should be done?
  - Employee background checks
- Operational
  - How often must we do it?
  - Periodic review of security policies
- Technical
  - How exactly will we do it?
  - Firewall rule configuration

Security Control Types

- Physical
  - Access control vestibule (mantrap)
- Detective
  - Log analysis
- Corrective
  - Patching known vulnerabilities

Security Control Types

- Deterrent
  - Device logon warning banners
- Compensating
  - Network isolation for Internet of Things (IoT) devices
- https://www.shodan.io/

Cloud Security Control Documents

- Cloud Security Alliance (CSA)
  - Cloud Controls Matrix (CCM)

Security Control Documents

- Payment Card Industry Data Security Standard (PCI DSS)
  - Security controls must be in place to be compliant

Risk Example

- Risk
  - Theft of online banking credentials
- Attack vector
  - Spoofed e-mail message with link to spoofed Web site tricking an end user
- Mitigation through security controls
  - User security awareness
  - Antivirus software
  - Spam filters

Quick Review

- Security controls mitigate specific threats
- Managerial security controls include administrative functions such as background checks
- Operational security controls include policy reviews
- Technical controls relate to specific IT security solutions
- Security control types include physical, detective, corrective, preventive, deterrent, and compensating

Episode 1.06

Episode title: **Risk Assessments and Treatments**

Objective: **5.4 Summarize risk management processes and concepts.**

Risk Assessment

- Prioritization of threats against assets and determining what to do about it
- Applicable to
  - Entire organization
  - A single project or department
- Targets
  - Servers
  - Legacy systems
  - Intellectual property (IP)
  - Software licensing

Risk Assessment Process

- Risk awareness
  - Cybersecurity intelligence sources
- Evaluate security controls
  - Inherent (current) and residual risk
- Implement security controls
- Periodic review

Risk Types

- Environmental
  - Flood, hurricane
- Person-made
  - Riots, terrorism, sabotage
- Internal
  - Malicious insider, malware infections
- External
  - Distributed denial of service (DDoS)

Risk Treatments

- Mitigation/reduction
  - Security controls are proactively put in place before undertaking the risk
- Transference/sharing
  - Some risk is transferred to a third party in exchange for payment
  - Example: cybersecurity insurance

Risk Treatments

- Avoidance
  - Avoid an activity because the risks outweigh potential gains
- Acceptance
  - The current level of risk is acceptable
  - The risk falls within the organization's risk appetite

Quick Review

- A risk assessment strives to determine the likelihood and impact of threats
- Risk types include environmental, person-made, internal, and external
- Risk treatments (management) include acceptance, mitigation, transference, and avoidance

Episode 1.07

Episode title: **Quantitative Risk Assessments**

Objective: **5.4 Summarize risk management processes and concepts.**

Quantitative Risk Assessment

- Based on numeric values
- Asset value (AV)
- Exposure factor (EF)
  - Percentage of asset value loss when negative incident occurs

Single Loss Expectancy (SLE)

- How much loss is experienced during one negative incident?
- Multiply asset value (AV) by the exposure factor (EF)

Single Loss Expectancy (SLE)

- Asset value (AV) = $24,000
- Exposure factor (EF) = 12.5%
- $24,000 (AV) X 0.125 (EF) = $3,000 (SLE)

Calculate Single Loss Expectancy

SLE = Asset Value (AV) x Exposure Factor (EF)

Quantitative Risk Assessment

- Annualized rate of occurrence (ARO)
  - Expected number of yearly occurrences
  - Example: 2-3 times per year
- Annualized loss expectancy (ALE)
  - Total yearly cost of bad things happening
  - ALE = SLE X ARO

Annualized Loss Expectancy (ALE)

- ALE = single loss expectancy (SLE) x annualized rate of occurrence (ARO)
- Eg: $2,500 x 2 = $5,000
- Spending less than $5,000 yearly to protect the asset is worthwhile

Calculate Annualized Loss Expectancy

ALE = Single Loss Expectancy (SLE) x Annualized Rate of Ocurrence (ARO)

Spending less than $6,000 anually to protect our ecommerce site is worthwhile

Quick Review

- The single loss expectancy (SLE) is calculated by multiplying the asset value (AV) by the exposure factor (EF)
- The annualized loss expectancy (ALE) is calculated by multiplying the annualized rate of occurrence (ARO) by the SLE

Episode 1.08

Episode title: **Qualitative Risk Assessments**

Objective: **5.4 Summarize risk management processes and concepts.**

Qualitative Risk Assessment

- Based on subjective opinions regarding:
  - Threat likelihood
  - Impact of realized threat
- Threats are given a severity rating

Risk Register

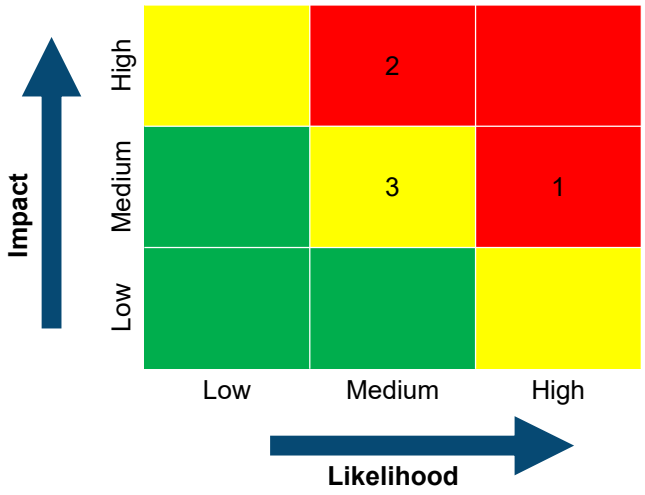
- Organizations should have one (or more)
- Centralized list of risks, severities, responsibilities, and mitigations
- Generally considered qualitative
  - Example: severity or impact ratings
  - Occasionally includes hard numbers (%, $)

Risk Register Example

Risk #	Date	Title	Likelihood	Impact	Severity	Owner	Mitigation
1	March 5	On-premises customer PII data exfiltration	High	Med	High	User1	Refer to IRP #425-1
2	June 3	Employees not attending security awareness training	Med	High	High	User2	Company-issued devices, VPN
3	March 6	Employees using BYOD smartphones	Med	Med	Med	User2	Company-issued devices, VPN

Risk Heat Map

- Take risk severity levels and map visually by color



Risk Matrix

- Table of risk details
- Similar to a heat map but without colors

Quick Review

- A qualitative risk assessment is based on subjective risk severity levels
- A risk register is an up-to-date centralized list of risks and their relative severities and mitigations
- Risk heat maps and risk matrices are used to plot and chart risk severity levels

Episode 1.09

Episode title: **Business Impact Analysis**

Objective:

5.4 Summarize risk management processes and concepts.

5.5 Explain privacy and sensitive data concepts in relation to security.

Business Impact Analysis (BIA)

- Prioritize mission-critical processes
  - Payment processing systems
  - Customer/patient records
- Assess risk
  - Identify sensitive data
  - Identify single points of failure
  - Identify security controls and compliance

Business Impact

- Financial
  - Fines
  - Loss of contracts
- Reputation
- Data loss
  - Breach notification
  - Escalation requirements
  - Exfiltration

Failed Component Impact

- Mean time between failures (MTBF)
  - Average time between repairable component failures
  - Software patching
- Mean time to failure (MTTF)
  - Average time between NON-repairable component failures
  - Hard disks, switches, routers
- Mean time to repair (MTTR)
  - Time required to repair a failed component

Locating Critical Resources

- Data discovery and classification
  - Where is our sensitive data?
  - Privacy threshold assessment (PTA)
    - First step before implementing solutions related to sensitive data
- Impact on sensitive data
  - Privacy impact assessment (PIA)
  - Regulatory compliance

Business Impact

- Recovery point objective (RPO)
  - Maximum tolerable amount of data loss
  - Directly related to backup frequency
- Recovery time objective (RTO)
  - Maximum tolerable amount of downtime
  - Return systems and data to usable state

Quick Review

- A business impact analysis (BIA) identifies how negative incidents will impact business processes and sensitive data
- MTBF, MTTF, and MTTR are related to the impact of failed components
- The recovery time objective (RTO) defines the maximum tolerable amount of downtime
- The recovery point objective (RPO) defines the maximum tolerable amount of data loss

Episode 1.10

Episode title: **Data Types and Roles**

Objective: **5.5 Explain privacy and sensitive data concepts in relation to security.**

Data Classification

- Government/military classification
  - Top secret
  - Secret
  - Confidential

Data Classification

- Standard classification
  - PII (personally identifiable information)
  - PHI (protected health information)
  - Proprietary
  - Public/private
  - Critical
  - Financial

Data Privacy Standards

- Ensure data privacy and breach notification
- Levy fines
- Protect intellectual property (IP)
- Example: HIPAA (Health Insurance Portability and Accountability Act)

Data Privacy Standards

- PCI DSS (Payment Card Industry Data Security Standard)
  - Cardholder information
- GDPR (General Data Protection Regulation)
  - Protects EU citizens' data regardless of location

Data Classification Tools

- Any method of applying metadata
  - Example: cloud resource tagging

Data Roles and Responsibilities

- Owner
  - Legal data owner
  - Set policies on how data will be managed
- Controller
  - Ensure data complies with applicable regulations
- Processor
  - Handles data in accordance with privacy guidelines
- Custodian/steward
  - Responsible for managing data (permissions, backup) in alignment with data owner policies
- Data privacy officer (DPO)
  - Ensures data privacy regulation compliance such as with GDPR

Quick Review

- Data classification assigns labels to data to facilitate management
- Common data privacy standards include HIPAA, PCI DSS, and GDPR
- Data owners determine data management policies
- Data custodians apply data management policies

Episode 1.11

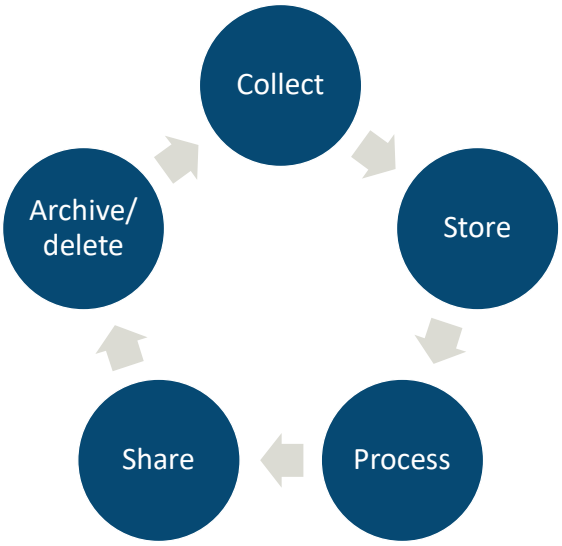
Episode title: **Security and the Information Life Cycle**

Objective: **5.5 Explain privacy and sensitive data concepts in relation to security.**

Information Life Cycle

- Security involved at every phase
- Data collection
  - Consent
- Implementation depends on regulations/ standards

Information Life Cycle



Personally Identifiable Information (PII)

- One or more pieces of sensitive information that can be traced back to an individual
  - Social security number
  - E-mail address
  - Credit card number
  - Home address
  - Web browser cookie containing sensitive session identifiers

Protected Health Information (PHI)

- One or more pieces of sensitive medical information that can be traced back to an individual
  - Health insurance plan number
  - Blood type
  - Patient medical ailments

Privacy-Enhancing Technologies

- Anonymization
- The GDPR allows anonymized data collection and use without user consent
- Anonymized data has limited marketing value

Anonymization Techniques

- Pseudo-anonymization
  - Replace PII with fake identifiers
- Data minimization
  - Limit stored/retained sensitive data
- Tokenization
  - A digital token authorizes access instead of the original credentials
- Data masking
  - Hide sensitive data from unauthorized users
  - Masked out credit card number digits on a receipt

Data Sovereignty

- Location of data and laws that apply to it
  - Where did the data originate?
  - Where does the data reside?
  - Which laws/regulations apply to the data?

Quick Review

- The information life cycle includes data collection, storage, processing, sharing, and archiving then deletion
- Sensitive data can be anonymized through pseudo-anonymization, data minimization, data masking, and tokenization
- Data sovereignty refers to the origin and storage location of data related to applicable laws

Episode 1.12

Episode title: **Data Destruction**

Objective: **2.7 Explain the importance of physical security controls.**

Data Destruction

- Paper, film, magnetic tape
  - Burning
  - Pulping
  - Shredding (pulverizing)

Digital Data Destruction

- Failed or decommissioned storage devices
- Storage device end-of-life policies
  - Reuse? Donate? Destroy?
  - Update asset inventory

Digital Media Sanitization

- Data is still recoverable
  - Deleted files, repartitioned, or reformatted drives
- Disk wiping tools
  - SSD and HD
    - Multiple pass disk overwrites
  - HD only
    - Degaussing

Digital Media Sanitization

- Cryptographic erasure
  - Destroy storage media decryption key
  - Self-encrypting drives (SEDs)

Quick Review

- Data sanitization ensures sensitive data cannot be recovered
- Organizational policies define how physical and digital data is safely destroyed
- Data sanitization methods include burning, shredding, cryptographic erasure, disk wiping tools, and degaussing

Episode 1.13

Episode title: **Personnel Risk and Policies**

Objective: **5.3 Explain the importance of policies to organizational security.**

Personnel Management Policies

- Standard operating procedure (SOP)
  - Example: proper steps for sending sensitive data via e-mail
- Mandatory vacation, job rotation
  - Detection of irregularities
- Separation of duties (multi-person control)
  - Reduce likelihood of internal fraud
  - Does not prevent collusion

Employee/ Contractor Hiring

- Social media analysis
- Web search
- Background check
  - Criminal record
  - Unpaid fines
  - Credit check
  - Interviews with friends, family, colleagues

User Onboarding

- Non-disclosure agreement (NDA)
  - Proprietary secrets, PII/PHI
- Security policy awareness
  - User sign-off
- User account and resource access
- Issue security badge, smart card

User Habits

- Clean desk policies
- Physical and digital document shredding
  - Mitigates dumpster diving, data recovery
- Personally-owned devices
  - Mobile device management (MDM)
  - Bring your own device (BYOD)

User Training

- Ongoing, role-based
- Computer-based training (CBT)
- Gamification
  - Capture the flag contests
- Phishing campaigns/ simulations
  - Lunch and learn
  - Can be part of a penetration test

User Offboarding

- Termination letter
- Exit interview
- Return of equipment
- Knowledge transfer
- Account disablement vs. deletion

Quick Review

- Securing personnel management can be implemented with job rotation, mandatory vacations, and separation of duties
- Employee and contractor background checks help ensure trustworthiness
- User onboarding occurs after hiring and includes training and account provisioning
- Clean desk and secure data disposal policies reduce the risk of security breaches

Episode 1.14

Episode title: **Third-Party Risk Management**

Objective: **5.3 Explain the importance of policies to organizational security.**

Third-Party Risk Management

- Measurement systems analysis (MSA)
  - Quality assurance

Supply Chain Security Risks

- Hardware and software vendors
  - End-of-service life (EOL, EOSL) means no more patches or support
- Cloud service providers security compliance
- Contractors
  - Data privacy notices
- Company mergers and system linking
- Software developers using third-party components

Third-Party Risk Management

- Data Loss Prevention (DLP) systems
  - Reduce intentional/ unintentional sensitive data exfiltration

Quick Review

- A measurement systems analysis (MSA) can identify supply chain improvements
- Supply chain risks include unstable or insecure hardware, software, or contractors, or suppliers not meeting security standards
- Sensitive data stored in the public cloud presents a third-party risk
- The intentional/unintentional disclosure of sensitive data can be controlled with DLP

Episode 1.15

Episode title: **Agreement Types**

Objective: **5.3 Explain the importance of policies to organizational security.**

Agreement Types

- Interconnection security agreement (ISA)
  - Legal review, regulatory compliance
  - Linking companies, partners, agencies
  - Vulnerability scan results
  - Mandatory training/ certification
  - Input from IT security professionals
- Service level agreement (SLA)
  - Contractual document stating level of service
  - Guarantee service uptime
  - Consequences for not meeting requirements

Agreement Types

- Memorandum of understanding (MOU)
  - Broad terms of agreement between parties
- Memorandum of agreement (MOA)
  - Detailed terms between parties
- Business partnership agreement (BPA)
  - Legal document
  - Responsibilities, investment, decision-making
- Non-disclosure agreement (NDA)
  - Prevent sensitive data disclosure to third parties

Quick Review

- Interconnection security agreements (ISAs) apply when connecting different entities together
- Service level agreements (SLAs) detail expected service uptime from a provider
- Memorandums of understanding (MOUs) state broad agreement terms between parties, memorandums of agreement (MOAs) are more detailed
- Non-disclosure agreements (NDAs) prevent sensitive data disclosure to third parties