5.0 Security Program Management and Oversight

CompTIA Security+ SY0-701

Topics

- Elements of Effective Security Governance
- Elements of the Risk Management Process
- Third-party Risk Assessment and Management
- Effective Security Compliance
- Audits and Assessments
- Security Awareness Practices

Elements of Effective Security Governance

- IT Governance
- IT Management
- Guidelines, Policies, Standards, Procedures
- External Considerations
- Monitoring and Revision
- Roles and Responsibilities for Systems and Data

What is IT Governance?

- A sub-discipline of organizational governance
- A formal way (provides structure) to align IT & business strategy
- ensure that IT investments support business objectives
- Typically adopt one or more well-known frameworks such as:
    - COBIT, COSO, FAIR (risk management)
    - ITIL (streamline service and operations)
    - CMMI (software and hardware development, purchasing, and service delivery)

Types of IT Governance Structures

Boards	• Provide strategic direction • Responsible for IT strategy oversight, technology systems, IT financing, and risk management within the organization • The IT Governance Board is typically a committee of the organization’s board of directors
Committees	• Handle specific tasks or initiatives • Conduct research to make recommendations • Once recommendations are approved, committees execute plans, monitor progress, and ensure successful implementation
Government entities	• Governments are realizing that in order to mount a proper national cyber defense, their role should expand from just securing public networks to helping to secure both public and private networks • There are numerous government initiatives to share information and provide guidelines to the public
Centralized/decentralized	• Depending on need, IT governance and operations can be run centrally or locally by business unit or location

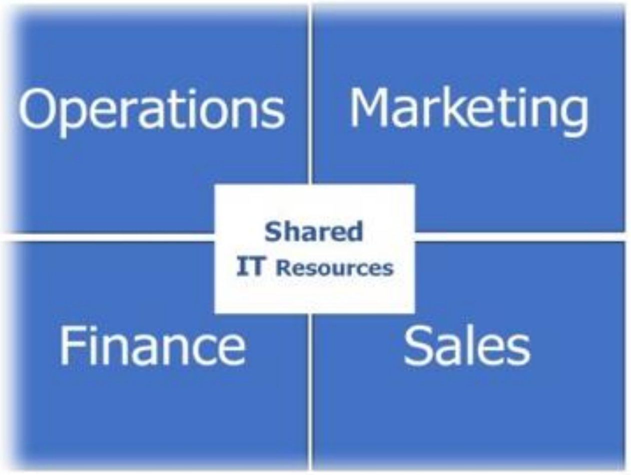
Centralized IT Management

- Lower overall expenses
- Usually easier to meet specific industry regulations
- Can improve IT staff productivity
- Usually easier to share information throughout the organization
- Reduced hacking vulnerabilities
- Fewer successful cyber incidents
- Can facilitate continual improvement
- Requires excellent network connectivity

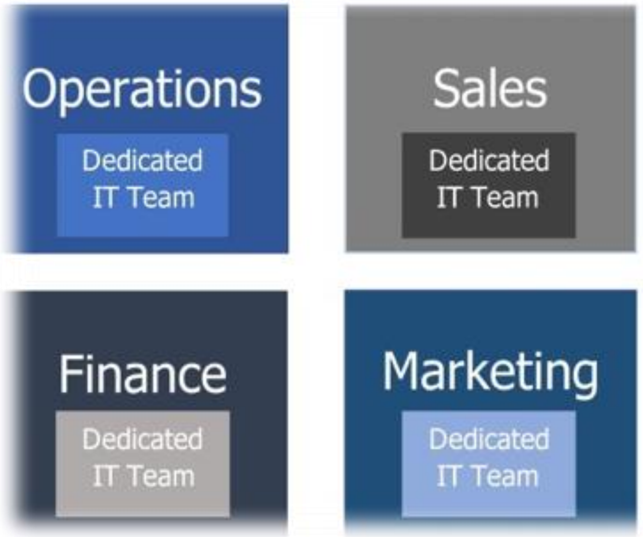
De-centralized IT Management

- Specialized and dedicated to the unique needs of each business unit or region
- Leads to highly flexible and configurable networks
- Makes it easier to adapt to new technology
- Makes the company's IT network more resilient
- Can lead to an increased sense of empowerment and responsibility from IT employees

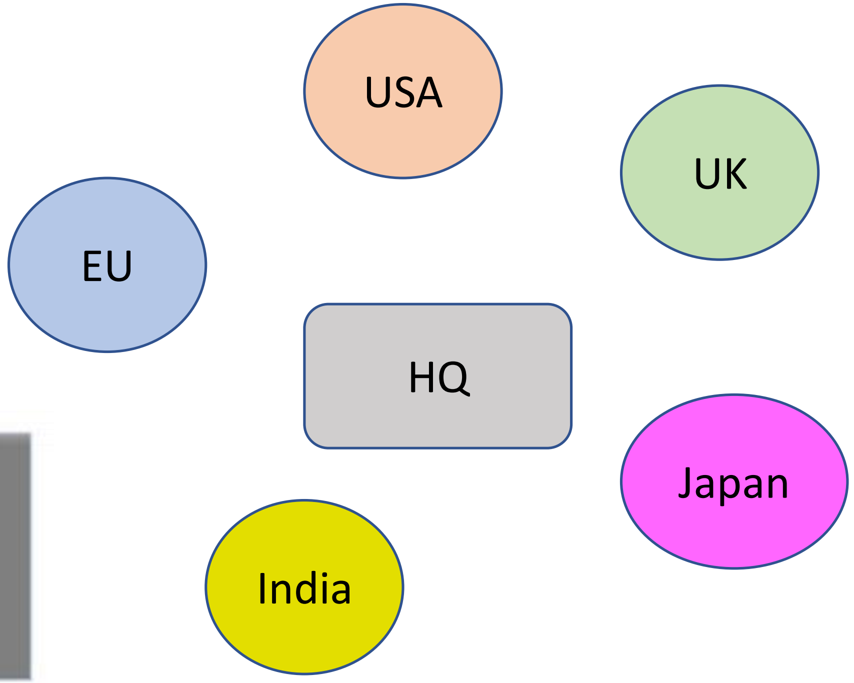
Centralized vs Decentralized IT Management Examples



Operations
Marketing
Shared
IT Resources
Finance
Sales



Operations
Dedicated
IT Team
Sales
Dedicated
IT Team
Finance
Dedicated
IT Team
Marketing
Dedicated
IT Team



USA
UK
EU
HQ
Japan
India

Guidelines

- Voluntary
- Recommendations
- Based on best practice
- Typically industry-wide

Policies

- Organization-specific requirements
- Enforceable
- Common types include:
    - Acceptable use policy (AUP)
    - Information security policies
    - Business continuity
    - Disaster recovery
    - Incident response
    - Software development lifecycle (SDLC)
    - Change management

Standards

- Broadly-accepted specifications
- Designed to maximize interoperability
- Examples:
  - Password
  - Access control
  - Physical security
  - Encryption

Procedures

- Organization-specific
- Task-oriented
- Step-by-step
- Usually published as a Standard Operating Procedure (SOP)
- Examples:
  - Change management
  - Onboarding/offboarding
  - Playbooks/Run books

External Considerations

- IT governance ensures that organizations comply with relevant laws, regulations, and industry standards pertaining to IT operations
- IT governance includes policies and procedures to address data privacy, information security, intellectual property rights, and other legal and regulatory obligations
- In addition to your internal organizational policies, you must also ensure you are in compliance with external requirements including:
  - Industry-specific (health, financial, legal, public utilities)
  - Local/regional
  - National
  - Global
- Work with your legal department to ensure your organization stays in compliance

Monitoring and Revision

- Monitor evolving external requirements and update your own implementations as needed
- As a general rule, organizational policies and procedures should be reviewed every one to three years
  - Prefer one year if possible
- Schedule time into the corporate calendar to proactively review your policies and procedures

Roles and Responsibilities for Systems and Data

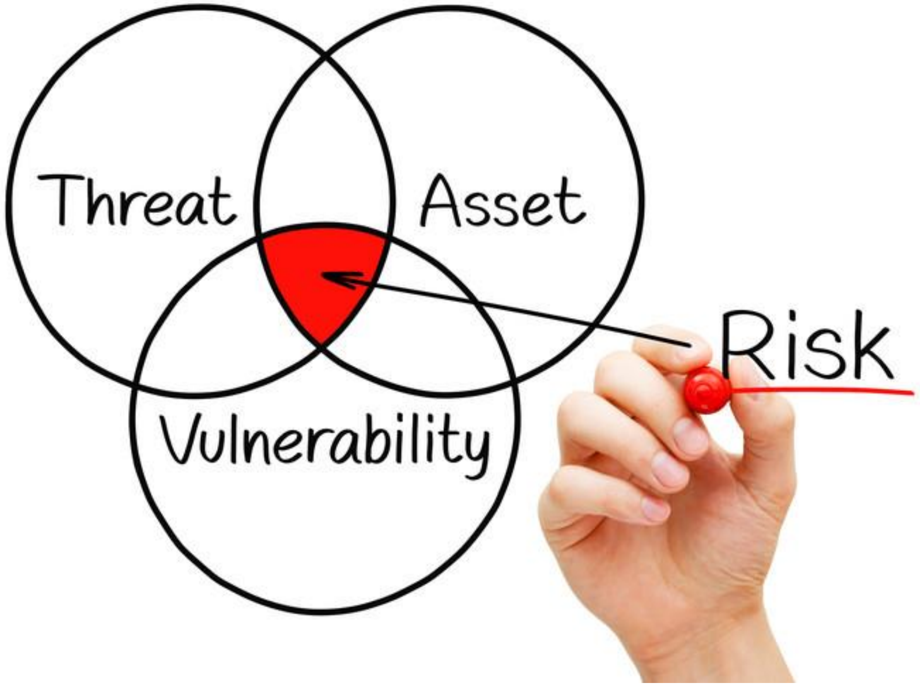
Owner	• Typically the head of the department that uses the data • Concerned with risk and appropriate access to data • Determines who can access data
Controller	• Determines the purpose of any personal data and the means of processing it • May be governed by statutory obligation
Processor	• Processes any data that the data controller gives them • Cannot change the purpose or means by which data is used
Custodian	• Manages the actual data • Implements access control per the owner’s requirements • Manages databases, servers, backups, and networks
Steward	• Concerned with the meaning of data and the correct usage of data • Doesn’t care who uses the data so long as they use it correctly

Elements of the Risk Management Process

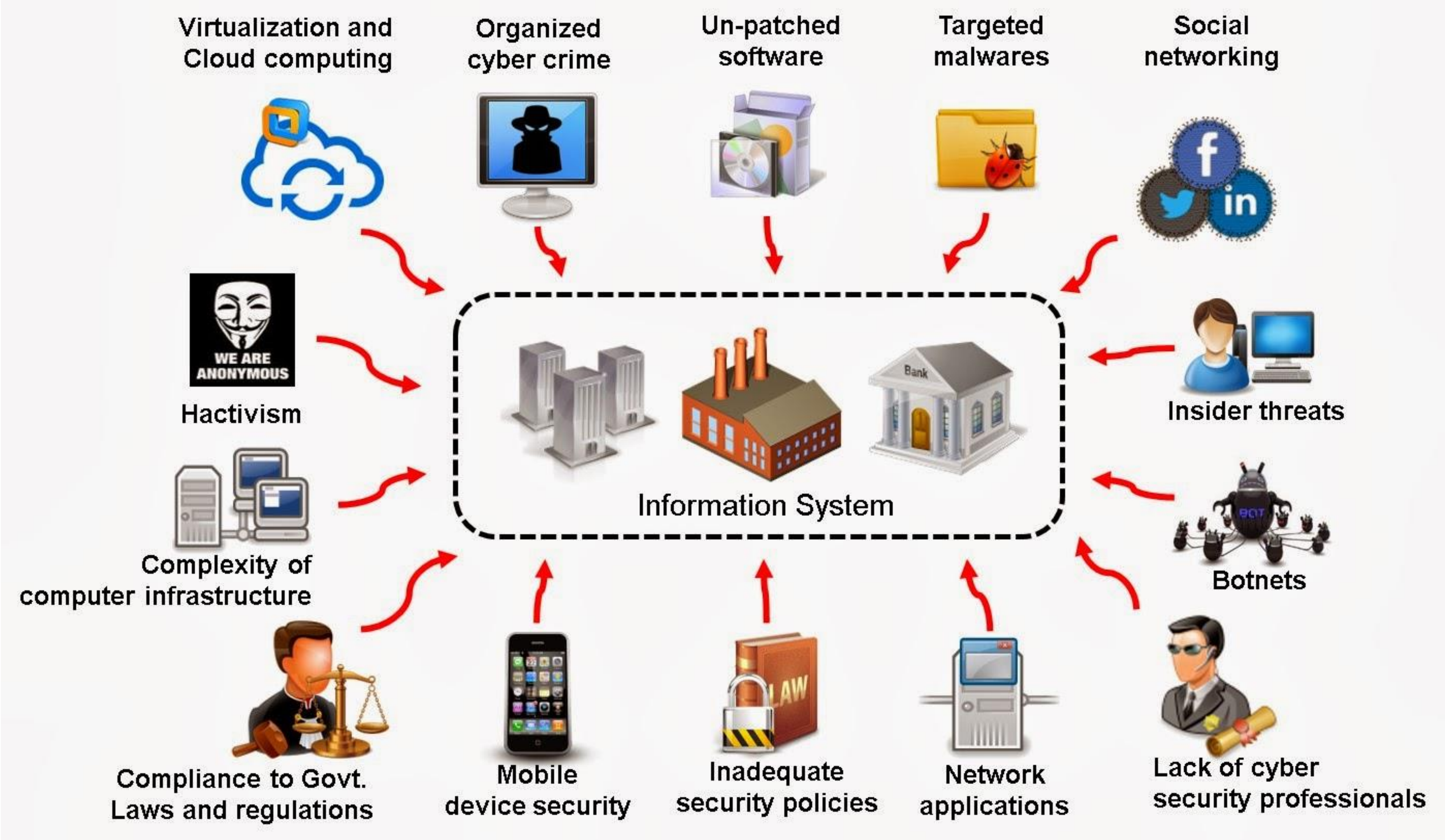
- Risk Management
- Risk Assessment
- Risk Response
- Business Impact Analysis

What is Risk?

- The probability that a threat may actually materialize and cause damage

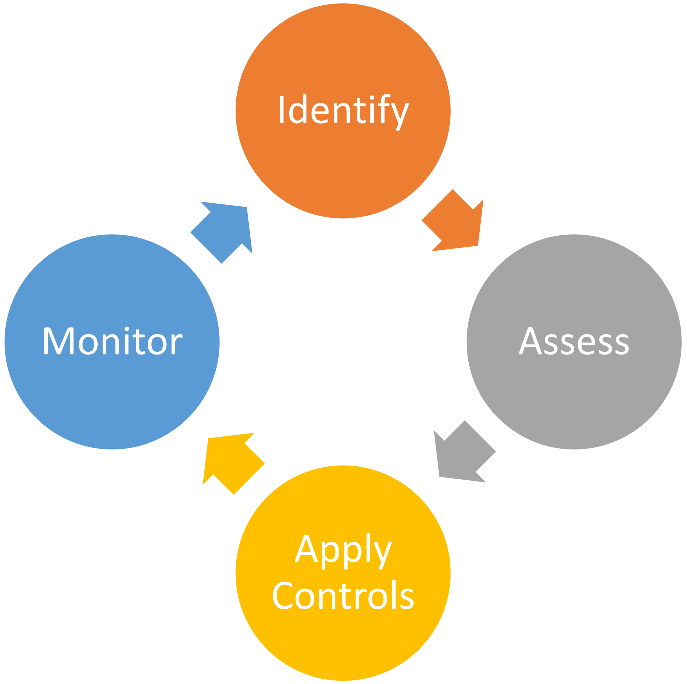


What are the risks for each of these?



Risk Management

- The identification, evaluation, and prioritization of risks
- Followed by coordinated and economical application of resources
  - to minimize, monitor, and control probability or impact

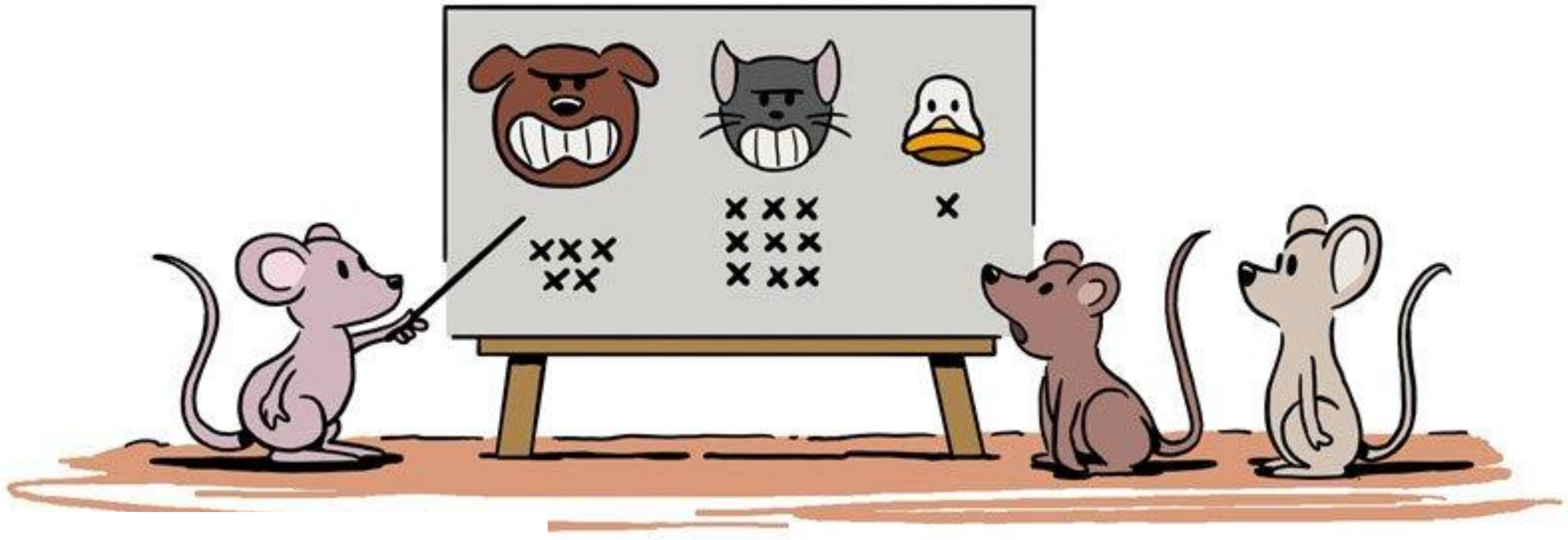


Before You Start

- Before you can analyze your risk, you need to know what you have to protect
- You will need a full inventory of all your IT assets including:
  - Device make and model, configurations, locations, network connections, running services and installed software

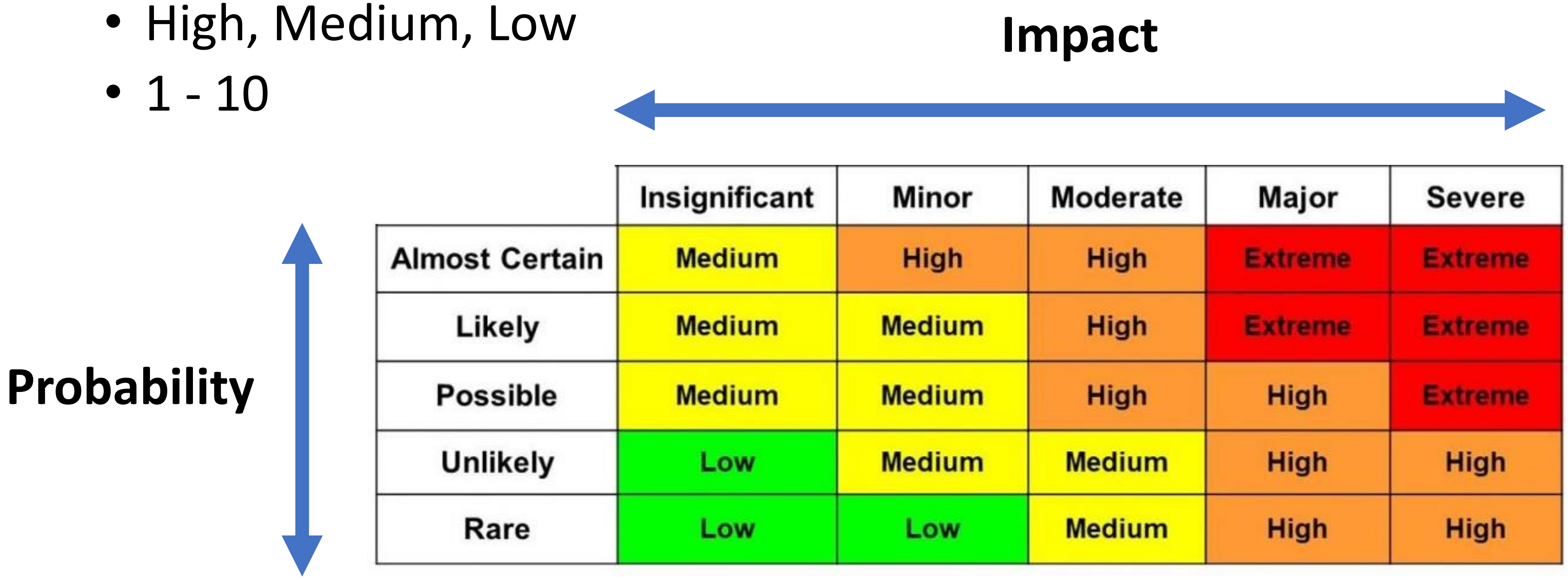
Risk Assessment

- The process of identifying security risks and assessing the threat they pose
- Includes risk identification, risk analysis, and risk response
- Threats must be evaluated in the context of the impact they will have to system and data confidentiality, integrity, and availability
- The ultimate purpose of IT risk assessment is to mitigate risks



Qualitative Risk Assessment

- Subjective assessment
- Assigns relative probability and impact to a risk
- Can be measured on various scales:
  - High, Medium, Low
  - 1 - 10


Impact
Probability

	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	Extreme	Extreme
Possible	Medium	Medium	High	High	Extreme
Unlikely	Low	Medium	Medium	High	High
Rare	Low	Low	Medium	High	High

Qualitative Risk Assessment Example

On a scale of 1 – 5, with 5 being the highest

Threat	Probability	Impact	Score
Virus	5	3	15
Phishing	5	4	20
Supply Chain Compromise	2	5	10
Malicious Insider	1	5	5

Quantitative Risk Assessment

- Objective assessment
- Assigns a monetary value to risk
- Uses a formula:

  SLE x ARO = ALE

  - Single Loss Expectancy (SLE) - how much one incident will cost
    - SLE = Asset Value (AV) x Exposure Factor (EF)
    - AV = How much revenue the asset brings in or the cost to replace it
    - EF = What percentage of the AV is lost if there is an incident
  - Annual Rate of Occurrence (ARO) - how often the incident is expected to happen over a year
    - If less than one year, can be amortized over several years
  - Annual Loss Expectancy (ALE) - how much this risk will cost us annually
- Allows you to more concretely justify priority and remediation expense
  - You can determine if a control is more expensive than an asset

Quantitative Risk Assessment Example

1. A hard drive fails every three years -
2. The cost to buy a new hard drive is $300
3. It will require 10 hours to restore the OS and software to the new hard disk
4. It will require a further 4 hours to restore the database from the last backup to the new hard disk
5. Assume the EF = 1(100%)
6. The recovery person earns $10/hour

    - Hard cost (replace drive) = **+** Soft cost (labor) = (10 + 4)hours x $10/hr =

7. Calculate the SLE , ARO , and ALE 440/3 =
8. What is the closest approximate cost of this replacement and recovery operation per year?

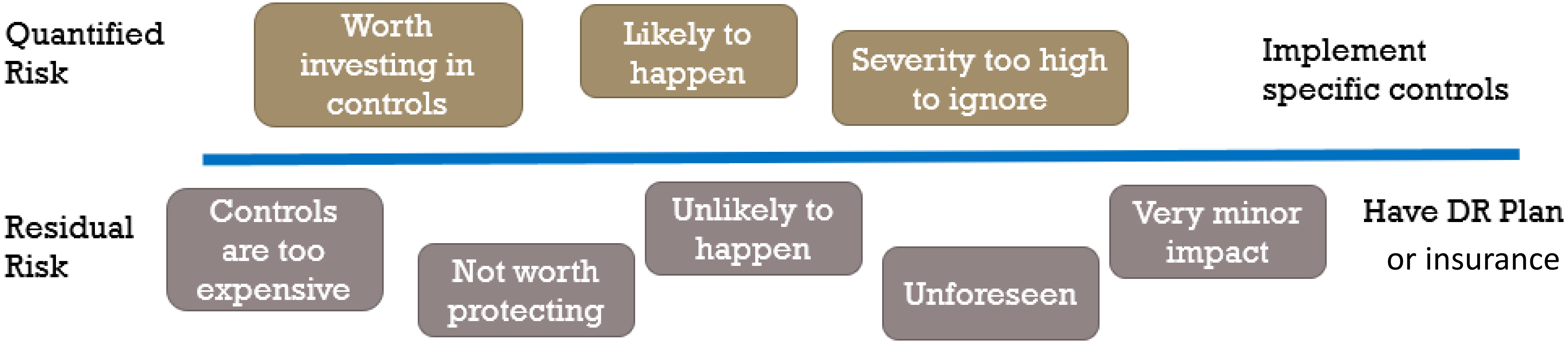
Quantitative Risk Assessment Example

1. A hard drive fails every three years - ARO = 0.34
2. The cost to buy a new hard drive is $300
3. It will require 10 hours to restore the OS and software to the new hard disk
4. It will require a further 4 hours to restore the database from the last backup to the new hard disk
5. Assume the EF = 1(100%)
6. The recovery person earns $10/hour
   - SLE: $440
   - Hard cost (replace drive) = $300 + Soft cost (labor) = (10 + 4)hours x $10/hr = $140
7. Calculate the SLE $440, ARO 1/3, and ALE 440/3 = ~$146.67
8. What is the closest approximate cost of this replacement and recovery operation per year?

   Slightly more than $146

“The Line” and Residual Risk

- All risks “above the line” are worth mitigating
  - Worth the time, effort and cost
- All risks “below the line” are not worth mitigating
  - Too costly, too unlikely to materialize
  - These risks are called “residual risk”
  - You can cover them all with a good backup/disaster recovery strategy or insurance



Risk Response

How will you manage your risk?

- Avoid
  - Stop doing the risky thing
  - Get rid of the risky asset
- Mitigate
  - Reduce the impact in case something happens
- Transfer
  - Make someone else responsible
  - Buy insurance
- Accept
  - Realize the risk could happen
  - but do nothing about it
- Reject
  - Deny that the risk even exists
  - (very bad strategy)

Risk Response Example

1. An Internet marketing company decided that they didn’t want to follow the rules for GDPR because it would create too much work for them
2. They wanted to buy insurance, but no insurance company would write them a policy to cover any fines received
3. They considered how much the fines might be and decided to ignore the regulation and its requirements
4. They chose to **accept** the risk

- Note: In this case, they tried to transfer the risk but couldn’t
- They don’t reject the risk - they realize it could happen - they’re just not going to do anything about it - if they get caught, they’re ok with paying the fine

Strategies for Re-assessing Risk

- Recurring – on a regular schedule, such as annually or semi-annually
- Ad hoc – as situations arise, preferably in addition to recurring
- One-time
  - Useful when considering and comparing potential solutions
  - Once a system is deployed, you should switch to recurring or continuous
- Continuous
  - Respond More Quickly to New Risks
  - Check the Effectiveness of Controls Sooner
  - Requires leadership buy-in and automation tools

Additional Risk Terminology

Term	Description
Key Risk Indicators	Metrics used to monitor changes in risks, such as qualitative or quantitative ranking
Risk Owner	• The person ultimately accountable for ensuring that risk is managed appropriately • Typically the head of the IT department
Risk Threshold	The maximum amount of risk that an individual or organization is willing to accept
Risk Tolerance	• The degree to which an organization requires its information to be protected against confidentiality leaks or compromised data integrity • Focused on controlling risk
Risk Appetite	• The amount of risk that an organization is willing to accept to achieve its objectives • Focused on taking risk to improve productivity • Can be expansionary (willing to take more risk), conservative (not willing to take more risk), or neutral
Risk Reduction	The act of implementing controls of any type to limit risk
Risk Reporting	Creating a formal report for management identifying potential impact of risk to business

Risk Register

- A repository of risk information, including known risks over time and risk responses
  - Typically a document that records and tracks the risks associated with a project, system, or organization
- Includes information such as the risk:
  - description, owner, probability, impact, level, response strategy, status
- A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders
- A risk register can also help document the risk tolerance and thresholds of an organization:
  - the acceptable levels of risk exposure
  - the criteria for escalating or mitigating risks

Business Impact Analysis (BIA)

- First step in planning for when risk management fails
- Predicts how disruptive events will affect business operations
- Used to create a:
  - Business Continuity Plan (keep the business running in case of disaster)
  - Disaster Recovery Plan (restore IT services in case of disaster)
- A disaster recovery plan should include the following maintenance metrics:
  - Recovery Time Objective (RTO)
    - How long before various services are restored
  - Recovery Point Objective (RPO)
    - How much of a service will be restored
  - Mean Time to Repair (MTTR)
    - How long it will take to repair/replace a failed component
  - Mean Time Between Failures (MTBF)
    - Expected time before a component fails under normal conditions
    - Published by the manufacturer

Question

- Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?
- Risk tolerance
- Risk transfer
- Risk register
- Risk analysis

Question

- Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?
- Risk tolerance
- Risk transfer
- **Risk register**
- Risk analysis

Question #2

- You want to reduce the cost of your annual cyber insurance policy by removing the coverage for ransomware attacks.
- Which of the following analysis elements are you most likely to use in making this decision?
- SLE
- ARO
- ALE

Question #2

- You want to reduce the cost of your annual cyber insurance policy by removing the coverage for ransomware attacks.
- Which of the following analysis elements are you most likely to use in making this decision?
- SLE
- **ARO**
- ALE

Question #3

- You purchased cyber insurance to address items listed on the risk register
- What type of risk response is this?
- **Transfer**

Question #4

- What information do you need before you can start performing risk analysis?
- **A full inventory of all your IT assets**

Question #5

- What will contain:
  - Ranked and ordered information on the likelihood and potential impact of disasters that may affect business processes and systems
  - A list of residual risks that need to be managed after mitigating controls have been implemented
- **Risk register**

Question #6

- What is the formula to calculate the total loss expected per year due to a threat targeting an asset?
- **SLE x ARO**

Question #7

- What is a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?
- **Mean Time To Repair (MTTR)**

Question #8

- What is a tool organizations use to identify, log, and track any potential risks and corresponding information?
- **Risk register**

Third-Party Risk Assessment and Management

- Vendor Assessment
- Supply Chain Analysis
- Agreement Types
- Vendor Monitoring

What is Third-party Risk Assessment?

- An analysis of the risks introduced to your organization via third-party relationships along the supply chain
- Your third parties can include vendors, service providers, software providers and other suppliers
- Third-party risk assessment is a crucial part of your risk management plan

Vendor Selection Considerations

- Due diligence
  - The process of evaluating the risks involved in partnering with a vendor, supplier, or business
  - Enforces objectivity when selecting a vendor
  - Can be initiated by either the buyer or the seller
  - Involves an independent third-party assessment of various aspects of the vendor's performance, such as finances, legal matters, security posture, market sector, and management team
  - Required under federal law and is necessary for running a successful operation
- Conflict of interest
  - Occurs when a supplier or prospective supplier has an unfair advantage or engages in conduct that may give it an unfair advantage
  - Usually facilitated by a decision-maker or influencer in the organization buying the vendor’s goods or services

Vendor Assessment

"To what extent do your vendors perform their own IT security due diligence?"

Assessment Type	Description
Penetration testing	• Do they perform or engage pentesting on their own systems? • Did they remediate any identified gaps?
Right-to-audit clause	• A contract provision that gives one party the right to audit the other party • Used to verify their compliance with the contract terms and conditions • Provides transparency, accountability, and verification mechanisms to ensure that the obligations outlined in the contract are being met
Evidence of internal audits	• Can they prove that security audits were conducted • What were the outcomes?
Independent assessments	Did they engage independent auditors?
Supply chain analysis	How secure and reliable is the supply chain behind your vendors?

Questionnaires

- AKA vendor risk management questionnaire, third-party risk assessment questionnaire, or vendor risk assessment questionnaire
- Designed to help your organization identify potential weaknesses among your third-party vendors and partners that could result in a data breach, data leak or other type of cyber attack.
- Can include sections such as:
  - Information security and privacy
  - Physical and data center security
  - Web application security
  - Infrastructure security

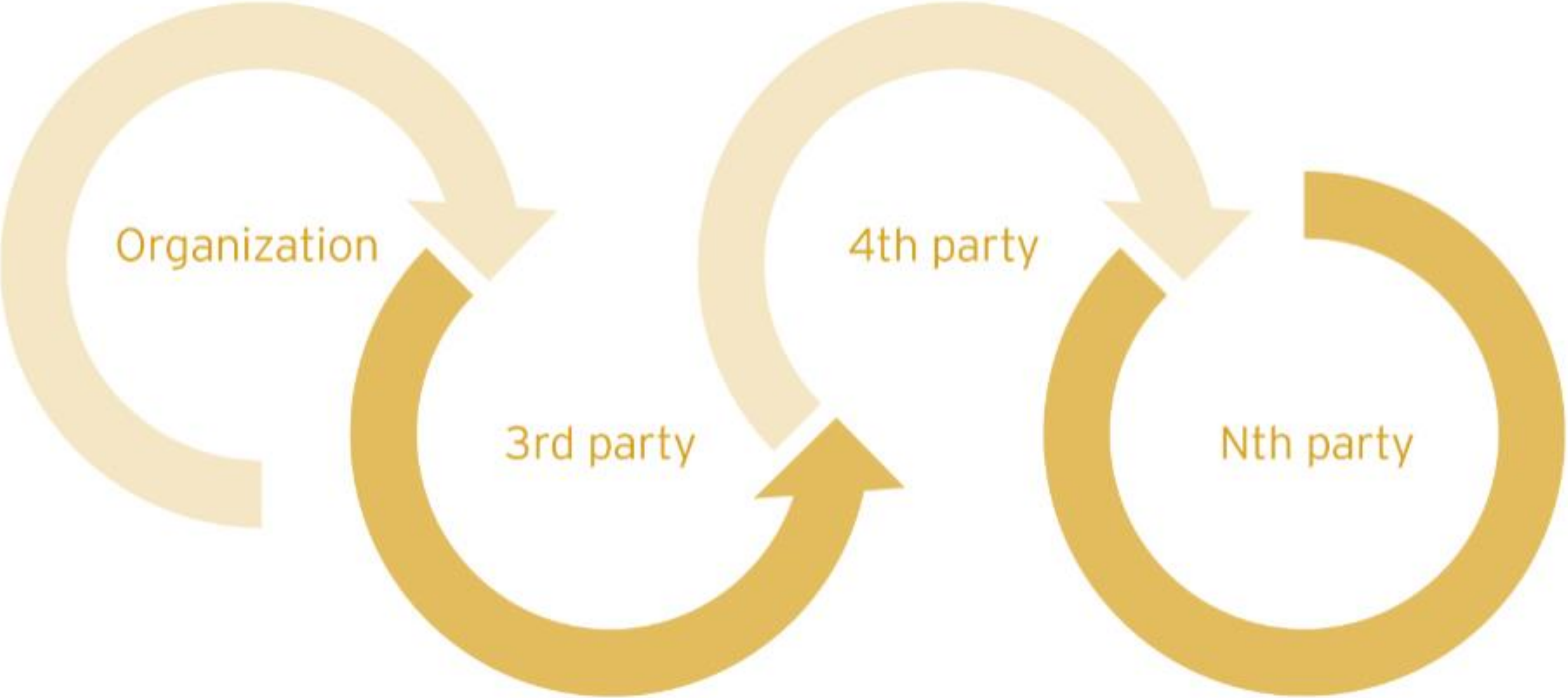
Third-party Penetration Testing

- AKA external penetration testing
- A cybersecurity practice in which an external firm or individual accesses the security system of the company
- The objective is to identify weaknesses and vulnerabilities
- The pentester will provide repeatable methods, evidence of compromise, and recommendations for remediation
- In addition to Rules of Engagement, the pentest team should sign an NDA to help protect your sensitive and proprietary information

Supply Chain Analysis

- Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network
- You must understanding roles and responsibilities of managing risk when doing business with fourth parties
  - Evaluate the riskiest or most critical fourth/Nth parties and focus efforts there
  - Understand how the organization's third, fourth and Nth parties conduct ongoing monitoring of their third parties
  - Develop an automated, data-driven approach that enables assessment of fourth/Nth parties in a more real-time manner
- Data transparency that reflects supplier risk is key to keeping your supply chain moving as the threat of disruption grows
- Proactive, ongoing monitoring and risk due diligence can inform your source-to-pay decisions to enable greater agility and resilience

Supply Chain Example



Supply Chain Analysis Steps

1. Identify all fourth parties
   - Maintain a central fourth-party inventory
   - Determine the significance of each fourth party
2. Establish a trusted relationship with the OEM and authorized resellers
3. Request documentation and certification of the hardware from the OEM or authorized resellers
4. Inspect the software/hardware components for any signs of tampering, such as mismatched labels, serial numbers, or components
5. Test the components for functionality, performance, and security
6. Implement a tracking system to monitor the components throughout their lifecycle
7. Reporting any suspicious or counterfeit components to the OEM and law enforcement agencies
8. Maintain a backup plan and exit strategy

Counterfeit Hardware

- Counterfeit hardware is hardware that is built or modified without the authorization of the original equipment manufacturer (OEM)
- It can pose serious risks to network quality, performance, safety, and reliability
- Counterfeit hardware can also contain malicious components that can compromise the security of the network and the data that flows through it
- To address the risks associated with procuring counterfeit hardware, a company should conduct a thorough analysis of the supply chain
    - the network of entities involved in the production, distribution, and delivery of the hardware
- By analyzing the supply chain, the company can:
    - verify the origin, authenticity, and integrity of the hardware
    - identify any potential sources of counterfeit or tampered-with products

Agreement Types

Type	Description
Service-level Agreement (SLA)	• A document that outlines a commitment between a service provider and a client • Includes details of the service, the standards the provider must adhere to, and the metrics to measure the performance
Memorandum of Agreement (MOA)	• A legal document describing a business partnership between two parties that have agreed to cooperate to meet an agreed objective or complete a project • Lays out the agreed terms and outlines the steps to reach the desired goal of the agreement • Typically used when money is involved
Memorandum of Understanding (MOU)	Describes each party's point of view about a project before entering into it
Non-disclosure Agreement (NDA)	• A legally binding contract that establishes a confidential relationship • Parties that sign agree that they will not disclose confidential information to others

Agreement Types (cont’d)

Type	Description
Master Service Agreement (MSA)	• A contract that lays out a framework of general terms and conditions between two parties in an ongoing, working relationship • Can save time for ongoing related projects or tasks • The parties only need to negotiate the terms once, at the beginning of the business relationship
Work Order (WO) / Statement of Work (SOW)	• Defines the current project • Includes specifications like pricing, deadlines, and expected output • If there's an MSA, the SOW will be short—often one page—making it much easier for the parties to agree upon.
Business Partners Agreement (BPA)	• A legal document that dictates how a small for-profit business will operate under two or more people • Establishes rules for the business operations, ownership stakes, financials, responsibilities, and decision-making strategies of each partner

Service-Level Agreement (SLA)

- An SLA is a document that defines the level of service expected by a customer from a service provider
- It indicates:
    - the metrics by which that service is measured
    - the remedies or penalties, if any, should the agreed-upon levels not be achieved
    - The minimum uptime or availability of a service, such as 99.99%
    - The consequences for failing to meet that standard

Rules of Engagement (RoE)

- To set up a successful relationship between vendors and companies, you need to have clear rules of engagement
- RoE sets expectations and performance guidelines at the beginning of the relationship

Typical RoE Elements

- The type and scope of the test:
  - black box, white box, or gray box
  - target systems, networks, applications, or data
- Timeline and duration of the test, and the hours of operation and testing windows
- Client contact details and the communication channels for reporting issues, incidents, or emergencies during the test
- Testing team credentials and the authorized tools and techniques that they can use
- Sensitive data handling and encryption requirements:
  - how to store, transmit, or dispose of any data obtained during the test
- Status meeting and report schedules, formats, and recipients
- Confidentiality and non-disclosure agreements for the test results
- Professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information

Vendor Monitoring

- Continuously understand the risk of doing business with your vendors, suppliers, service providers, third parties, etc.
- Conduct periodic "check-in" assessments related to your vendors' controls to surface risks so you can take action
- Performed by procurement and information security teams

Question

- You are engaging a third-party vendor to do a penetration test of a new proprietary application prior to its release
- To protect your intellectual property, which document type should you require them to review and sign?
- **NDA**

Question #2

- Which agreement type defines the time frame in which a vendor needs to respond?
- **SLA**

Question #3

- You are required to use certified hardware when building networks.
- What would best address the risk of inadvertently procuring counterfeit hardware?
- **A thorough analysis of the supply chain**

Question #4

- What document provides the details about the terms of a test with a third-party penetration tester?
- **Rules of engagement**

Question #5

- A client demands at least 99.99% uptime from a service provider's hosted security services.
- Which of the following documents includes the information the service provider should return to the client?
- MOA
- SOW
- MOU
- SLA

Question #5

- A client demands at least 99.99% uptime from a service provider's hosted security services.
- Which of the following documents includes the information the service provider should return to the client?
- MOA
- SOW
- MOU
- **SLA**

Question #6

- A client asked a security company to provide a document outlining the project, the cost, and the completion time frame
- Which of the following documents should the company provide to the client?
- MSA
- SOW
- SLA
- BPA

Question #6

- A client asked a security company to provide a document outlining the project, the cost, and the completion time frame
- Which of the following documents should the company provide to the client?
- MSA
- **SOW**
- SLA
- BPA

Question #6

- Outside of your own team and their work, what are likely vectors for the unauthorized inclusion of vulnerable code in a software release?
- **Included third-party libraries, vendors/supply chain**

Effective Security Compliance

- Compliance Concepts
- Privacy Terminology and Concepts

Compliance Concepts

- Due diligence
  - The process of conducting a thorough investigation, audit, or analysis of a third party’s compliance with regulatory bodies, both governmental and non-governmental
  - Essentially seeks to establish whether the supplier/vendor is following the rules as they should be.
- Due care
  - Taking reasonable steps to protect your organization’s reputational, financial, and legal best interests, especially if a third-party supplier or vendor has gaps in their own security management
- Attestation and acknowledgement
  - Using an independent third party to audit and verify that the third party’s cybersecurity controls and management are sufficient
- Internal and External
  - You can have your own team perform compliance monitoring to remediate known issues before an external firm performs their audit of you
- Automation
  - Compliance automation is the process of using technology, such as artificial intelligence (AI), to continually check systems for compliance
  - Compliance automation solutions replace manual processes
  - Automation tracks all compliance efforts from one location

Compliance Reporting

- Internal
    - Private
    - Pull together data to make decisions within the organization
- External
    - Offer information that specifically relates to what the clients, sponsors, or partners need to know
    - This data is more focused on their specific needs, such as client goals, ad budget spending, and success rates
    - Don’t waste anyone’s time by offering information they are not interested in

Consequences of Noncompliance

- Fines
  - Monetary penalties
- Sanctions
  - Penalties that may include fines, restrictions, orders to compensate customers, freezing or seizing of assets, etc.
- Reputational damage
  - Loss or harm that results from a negative shift in stakeholder or public perceptions of an organization
  - Can affect financial capital, social capital, market share, or shareholder value
- Loss of license
  - The organization can lose its license to operate in a certain industry, region, or service type
- Contractual impacts
  - Your contract could specify financial or other penalties for non-compliance

Privacy Terminology

Term	Description
Data Subject	An “identified or identifiable natural person”—a living individual with privacy rights that must be fulfilled
Data Controller	Collects the data, and controls the procedures and purpose of data usage Example: a company with a website that collects customer data
Data Processor	• Processes any data that the data controller gives them • Does not own the data that they process nor do they control it • Is not able to change the purpose and the means in which the data is used • Example: Google Analytics processes data for various organizations
Data ownership	Any personal information a data controller might collect remains the property of the subject (person it is about)

Privacy Terminology (cont’d)

Term	Description
Data inventory and retention	• A comprehensive catalog of all the data in an enterprise system • Data retention guidelines are a key feature of data privacy laws
Right to be forgotten	• The right to have private information about a person be removed from Internet searches and other directories under some circumstances • Recently updated as “right to erasure”
Annual Privacy Notice	• A clear and conspicuous notice to customers that accurately reflects your privacy policies and practices • Must be provided at least once in any period of 12 consecutive months during the continuation of the customer relationship

PII/PHI Data Roles

Role	Description
Data Subject	• Individual whose personal data is collected, processed, or stored by an organization • Has certain rights and expectations regarding how their data is handled, such as the right to access, correct, delete, or restrict their data
Data Owner	• Works for (or is) the organization that collected the data • Has the authority and responsibility to determine how data that has been collected is classified, protected, and used
Data Processor	• Individual or entity that performs operations on data on behalf of the data owner, such as collecting, modifying, storing, or transmitting the data
Data Custodian	• Individuals or entity that implements the security controls and procedures specified by the data owner to protect data while in transit and at rest • Examples: Database administrator, sysadmin

Privacy Implications

Term	Description
Legal	Failure to follow applicable data privacy laws may lead to fines, lawsuits, and even prohibiting a site's use in certain jurisdictions
Local/regional	• Local, state, and regional jurisdictions may implement their own privacy requirements • The risk is overlapping, confusing, or even contradictory requirements for businesses that operate in multiple locations
National	• Each country has its own data privacy laws. Examples: • US HIPAA, Fair Credit Reporting, GLBA, Family Education Rights and Privacy Act • Switzerland – enshrines privacy into its constitution • Japan – Act on the Protection of Personal Information • South Africa - The Protection of Personal Information Act
Global	• Legal frameworks that regulate the collection, management, and protection of personal data and privacy rights of individual • They vary across countries and regions, but some common principles include: stronger consent requirements, data breach notification, and the appointment of data protection officers • Example: EU General Data Protection Regulation (GDPR)

Question

- A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations.
- What should the hosting provider consider first?
- **Local data protection regulations**

Question #2

- Moo, a customer, received a notification from his mortgage company stating that his PII may be shared with partners, affiliates, and associates to maintain day-to-day business operations.
- What document did Moo receive?
- **An annual privacy notice**

Question #3

- Your marketing department collects, modifies, and stores sensitive customer data.
- The infrastructure team is responsible for securing the data while in transit and at rest.
- What data role describes the customer?
- **Subject**

Question #4

- You plan to use drones for your facility’s perimeter and boundary monitoring.
- What legal concern does this raise?
- **Privacy**

Audits and Assessments

- Attestation
- Internal Audit
- External Audit
- Penetration Testing

Attestation

- A cyber attestation is an objective, independent review and confirmation that:
  - an organization’s internal controls and cybersecurity risk management program meets the standards and requirements set out by a governing body
- Performed by an independent firm
  - The independent auditor is then able to provide an opinion about internal control effectiveness surrounding the cybersecurity risk management program.
- Used to build trust with your stakeholders

Internal Audit

- Performed by you
- Might be under the direction of an audit committee
- A self-assessment to ensure compliance

External Audit

- Performed by an independent third party
- Used to satisfy regulatory or contractual requirements
- An IT security audit is typically required before a financial audit can be conducted

Penetration Testing

- AKA Pentesting, Ethical Hacking
- Engaging a third-party to simulate a cyber attack
- Identify vulnerabilities before they are actually exploited
- Should include:
  - Scope
  - Timeframe
  - Limits
  - Full report with Executive Summary, reproducible steps, recommendations

Penetration Testing Terminology

Concept	Description
Penetration Test	An authorized, simulated cyber attack on a computer system or network
Physical Pentest	A test of the physical security of a datacenter
Offensive Pentest	• AKA Red Teaming • A group of security professionals who perform offensive security assessments covering penetration testing and social engineering • The Red Team simulates real-world attacks and exploits the vulnerabilities of a target organization, system, or network • They aim to test the effectiveness of the security controls, policies, and procedures of the target, as well as the awareness and response of the staff and the Blue Team • The Red Team can be hired as an external consultant or formed internally within the organization

Penetration Testing Terminology (cont'd)

Concept	Description
Defensive Pentest	AKA Blue Teaming A group of pentesters defend the system against Red Team attacks
Purple Team	A team that performs either/both offensive and defensive actions
White Team	• During a penetration testing exercise, the white team is responsible for acting as a referee and providing oversight and support to ensure that the testing is conducted safely and effectively • They may also be responsible for determining the rules and guidelines of the exercise, monitoring the progress of the teams, and providing feedback and insights on the strengths and weaknesses of the organization's security measures
Integrated Pentest	• The inclusion of automated pentesting in a Continous Integration/Continuous Delivery (CI/CD) application development pipeline

Penetration Testing Terminology (cont'd)

Concept	Description
White Box Pentest	• The pentester starts with full knowledge of the target and its environment • Gives the pentester insights that an actual hacker might miss
Grey Box Pentest	The pentester starts with partial knowledge of the target and its environment
Black Box Pentest	• The pentester starts with no knowledge of the target • The environment is unknown • Most closely simulates actual hacking

Reconnaissance

- First step in penetration testing
- Gather data on the target
- Probe for weak points

Passive Reconnaissance

- AKA Footprinting, or Open Source Intelligence (OSINT) activity
- The attacker searches for information without interacting with the target
  - Searches publicly available information
  - Gathers employee email addresses and social media accounts for social engineering
- The victim has no way of knowing or recording the attacker's activity
- Focuses on establishing:
  - Who has access to a target system
  - A map of the target's infrastructure:
    - security tools, software, devices,
    - target's overall security posture

Active Reconnaissance

- A type of reconnaissance that involves sending packets or requests to a target and analyzing the responses
- Can reveal information such as open ports, services, operating systems, and vulnerabilities
- More likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems

Scanning Targets

- Live systems
- Open ports
- Network paths
- OS and service versions
- Firewall rules
- Possible ways of bypassing the firewall

Network Scanning Tools
Nessus
nexpose
Nikto
OpenVAS
Open Vulnerability Assessment System
NMAP

Question

- A penetration tester begins an engagement by performing port and service scans against the client environment
- according to the rules of engagement.
- Which reconnaissance type is the tester performing?
- **Active**

Question #2

- A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering
- Which of the following teams will conduct this assessment activity?
- Red
- Blue
- Purple
- White

Question #2

- A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering
- Which of the following teams will conduct this assessment activity?
- **Red**
- Blue
- Purple
- White

Question #3

- You want a third-party vendor to do a penetration test that targets a specific device
- You have provided basic information about the device
- What type of pentest is this?
- Fully known environment – white box
- Partially known environment – grey box
- Unknown environment – black box

Question #3

- You want a third-party vendor to do a penetration test that targets a specific device
- You have provided basic information about the device
- What type of pentest is this?
- Fully known environment – white box
- **Partially known environment – grey box**
- Unknown environment – black box

Question #4

- You complete a vulnerability assessment on your network and find several vulnerabilities, which you have remediated
- What should you now do?
- **Rescan the network**

Question #5

- What type of requirement is the best reason to complete an audit in a banking environment?
- **Regulatory**

Question #6

- Which team combines both offensive and defensive testing techniques to protect an organization's critical systems?
- **Purple**

Question #7

- What type of team acts as a referee during a penetration-testing exercise?
- **White team**

Security Awareness Practices

- Security Awareness Training
- Security Training Topics
- Verifying Training Effectiveness

Security Awareness Program

- Activities and initiatives that aim to educate and inform the users about security policies, procedures, and best practices
- Can help to reduce the human factor in security risks, such as social engineering, malware, data breaches, and insider threats
- Should include multiple elements of communication such as:
  - Newsletters, posters, videos, webinars, quizzes, games, simulations, and feedback mechanisms
  - Reinforce the message and security culture
- Should include how to recognize and report phishing attempts or other suspicious activities

Security Awareness Training

- Depending on your environment, you will want to develop and execute security awareness training
- There will be different levels of training for different audiences:
    - Management
    - Staff
    - IT help desk
    - IT admins
- You can reinforce key points with messages, announcements, incentives, games, etc. to keep security consciousness ingrained into your staff
- You will want to regularly monitor and report on the effectiveness of your training efforts

Security Awareness Training Curriculum Plan

Your training curriculum plan should address the following:

- The threat vectors based on the industry in which the organization operates
  - This will help the employees to understand the specific risks and challenges that their organization faces, and how to protect themselves and the organization from cyberattacks
  - For example, a healthcare organization may face different threat vectors than a financial organization, such as ransomware, data breaches, or medical device hacking
- The cadence and duration of training events
  - This will help the employees to retain the information and skills they learn, and to keep up with the changing security landscape
  - The training events should be frequent enough to reinforce the key concepts and behaviors
    - But not too long or too short to lose the attention or interest of the employees
    - For example, a security awareness program may include monthly newsletters, quarterly webinars, annual workshops, or periodic quizzes
- How frequently the content is updated
  - With cybersecurity, new threats constantly appear
  - A popular approach is to provide annual base training, with regular incremental updates

Security Awareness Training Curriculum Plan (cont’d)

- Target audience
  - Certain audience types will have specific training topic needs
  - Consider having a baseline set of topics that apply to all staff
  - Then have additional training for specific roles and responsibilities

  Note: target audience provides a refinement/additional topics for specific job roles; it is an add-on to base security training requirements that all staff should complete
- Training modality
  - Determine which courses can/should be:
    - Self-paced
    - Virtual
    - Face-to-face / in-person
    - Hybrid
  - Note: modality is less critical than the actual subject, but still very useful for convenience, compliance, and overall program effectiveness

Security Training Topics

- Organizational and regulatory policy
  - Where to find/how to use handbooks for reference
- Situational awareness
- Insider threat
- Anomalous behavior recognition
  - Risky, unexpected, unintentional
- Monitoring and reporting
  - Initial instance
  - Recurring issues
- Password management
- Removable media and cables
- Social engineering
  - Awareness, recognition, and response
- Operational security
- Hybrid/remote work environments

Phishing Recognition and Response Example

1. You are a help desk technician
2. You get a phone call from someone claiming to be a part of the cybersecurity incident response team
3. They ask you to verify the network's internal firewall IP address
4. What should you do?
5. Get as much information about the caller as possible
6. Decline to answer their question
7. Hang up, and notify your cybersecurity officer/team

Verifying Training Effectiveness

- After training, you can perform unannounced, simulated attacks to measure training effectiveness
  - See if staff recognizes the attempt and responds accordingly
  - Create Key Performance Indicators (such as pass rate) to track effectiveness
- Examples include:
  - Phishing Campaigns
  - Pretexting calls to the Help Desk
  - Piggybacking and tailgating attempts
  - Situational awareness/physical security issues
  - “See something, say something” scenarios
  - Fake malware
  - Dashboards to see numbers of incidents and responses
- Consider your target audience:
  - Reports in dashboard/chart format for management
  - Surprise simulations for end users

Question

- After a security awareness training session, a user called the IT help desk and reported a suspicious call
- The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice
- What topic did the user recognize from their training?
- **Social engineering**

Question #2

- You want to improve the situational and environmental awareness of existing users as they transition from remote to in-office work
- What should you do regarding your training program?
- **Modify the content of recurring training**

Question #3

- A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization
- You are creating a way to present the data to the board of directors
- What should you use?
- **Dashboard**

Question #4

- Users are receiving phishing emails that bypass the current email-filtering technology
- With no controls to evaluate the safety of included links, users are being tricked into clicking on malicious URLs
- What can you do to immediately address this problem?
- **Give users updated awareness training**