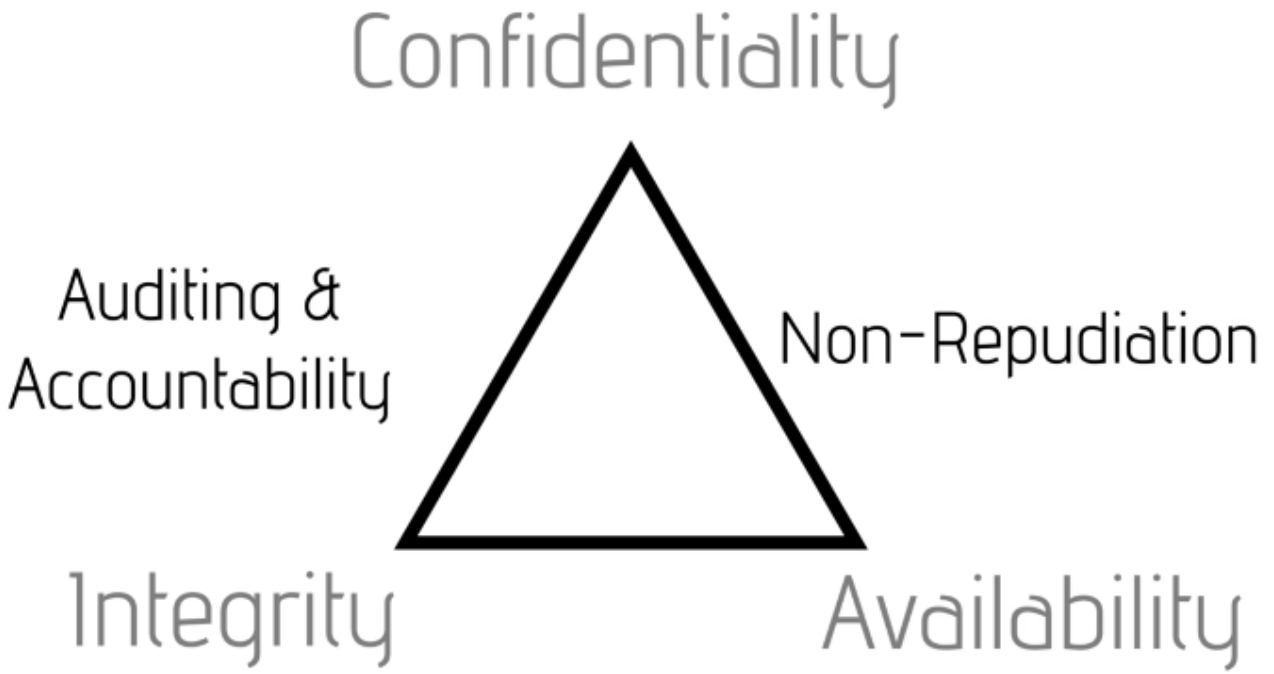
Section 1: Risk Management

1.Introduction

---

2. The CIA of Security

"CIA"
The CIA Triad is Critical for security.



Confidentiality - The goal of keeping data secret from anyone who doesn't have the need or the right to access that data.
Integrity - Ensures that the data and the systems stays in stay in an unalterd state. No unauthorized RWX.
Availability - Ensures that systems and data are available to authorized users when needed.
Auditing and Accounting - Keeping track of things that go on.
Non-Repudiation - A user cannot deny that they have performed a particular action.

---

3. What is risk?

Terms:

Assest: any part of our infrastructure that we are worried about getting harmed.
Vulerabilities: Weakness of an asset that leaves it open to Exploitation.
Threats: A threat is a discovered action that exploits a vulnerabiltiys potential to do harm to an asset.
Threat agent: A threat agent initiates a threat.

Likelihood: Defines the level of certainty that something will happen. Measured two different ways.
1. Quantitative: Percentage chance of something happening
2. Qualitative: Measures things that are hard to put a number against.

Impact: Impact is the harm caused by a threat.
1. Quatitative:
2. Qualitative:

a. (Threats -> Vulerabilities = Risk) "If an asset doesn't have any vulerability, or if there is no threat there is no risk."

b. If we have a risk then likelihood and impact matter.

The National Institute of Standards and Technologies SP 800-30 (Large document of potential risks) Use as part of a risk assesment

---

4.Threat Actors: People that actually do the attacks

Attributes of a threat actor:

1. Internal or External
2. Level of sophistication
3. Resources and Funding
4. What is their intent
5. Use of open source intelligent (OSINT)

The Types of threat actors:

1.Script Kiddies: Trivial attack knowledge
2.Hacktivist: Intent is motivation 'Activist'
3.Organized Crime: Motivation is money
4.Nation states/advaanced persistent thret (Motivation is intelligence) (APT: Advanced persistent threat)
5.Insiders: Someone that is inside the company. (Works within the infrastructure, not always an employee.)
6.Competitors:

5.Managing Risk

Risk Identificaiton/Risk Assessment: Consists of a Vulerability assessment and a threat assessment

cve.mitre.org (common vulerabilities)

Steps:

1. Figure out all of our assets
2. Make a list of potential vulerabilties
3. Do a vulerability assessment(Nessus), use penetration testing.
4. Do a threat assessment
   Threat assessment Guidelines
   1. Adversarial: hacker/malware - intentional bad stuff

    2. Accidental: User error
    3. Structural: e.g. Power supply on you router dies etc.
    4. Environmental
5. Risk Response
    1. Mitigation: reduce the likelihood and impact of risk
    2. Transferrance: offload risk on to a 3rd party (e.g. Cloud based service)
    3. Acceptance: Reach a point of the likelihood and the impact are less than the cost of mitigation.
    4. Avoidance: The likelihood is so high i'm just not going to deal with it. (e.g. dont hold vital personal information. Use cc information and then just forget it/dont save it.)

Framework:
LOTS out there but the two examples here are
1. NIST Risk Managment Framework Special Publication 800-37
2. ISACA Risk IT Framework

---

6. Using Guides for Risk Assessment

Benchmark: Basically a baseline. Use threshold values to understand what should be happening

Secure configuration guides:
Platform and vendor specific guides: Web servers, operating systems etc.
Network Infrastructure Devices
General Purpose guides

7.Security Controls

Security controls do two things:

1. Protect our infrastructure from problems.
2. Remediate Problems

Apply, monitor, Adjust Security Controls

Categories of Security Controls:

1. Administrative Control (Mangement Controls): Controls actions towards IT security
    1. Laws
    2. policies
    3. Guidelines
    4. Best Pracices
2. Technical Controls: actions IT systems make towards IT security
    1.Firewalls
    2.Password links
    3.Authenication
    4.Computer stuff

3. Physical Controls: Controls action in the real world
    1. Gates
    2. Guards
    3. Keys
    4. Man traps

Security Control Functions:

1. Deterrent:
   -Deters the actor from attempting the threat
2. Preventative
   -Deters the actor from performing the threat
3. Detective
   -Recognizes an actors threat
4. Corrective
   -Mitigates the impact of a manifested threat
5. Compensating
   -Provides alternative fixes to any of the above functions

**Need to be comfortable looking at situations and what type of security controls need to be applied for that particular situation.

---

8. Interesting Security Controls

Examples:

1. Mandatory Vacations : Used to detect fraud and unauthorized activity
2. Job Rotation: Switching people around to work in different positions (avoids contempt of position and makes it possible for more
   than one person to do a job in case someone leaves or gets fired etc.)
3. Multiperson Control: More than one person works on the same thing and ensures things are done the correct way. "Checks and balances"
4. Separation of Duties: "Administrative control" Single individuals should not do all things e.g. HR does HR, Security does security, etc.
5. Principle of Least privledge: users only have the level of privledge neccessary to do their jobs "Need to know".

9.Defense in Depth (Aka. Layered Security)

Diversity vs. Redundancy

Redundancy: A security control applied over and over again (layered) Definition: Repeating the same controls at various intervals, diversity is using a variety of controls in a random pattern.

Diversity: lots of different type of controls (e.g. Vendor diversity) Definition: Use a variety of physical, administrative, and techinical controls

**Vendor Diversity is a method of defense in depth with technical controls

---

10. IT Security Governance

Security Governance: Influences how the organization conducts IT Security

Sources of Security Governance(**REQUIRED**):

1. Laws and Regulations: (ex. HIPPA)
2. Standards (2 Types)
    1. Government
    2. Industry (Ex. PCI-DSS 'Credit card on the internet')
3. Best Practices
4. Common Sense and Experience

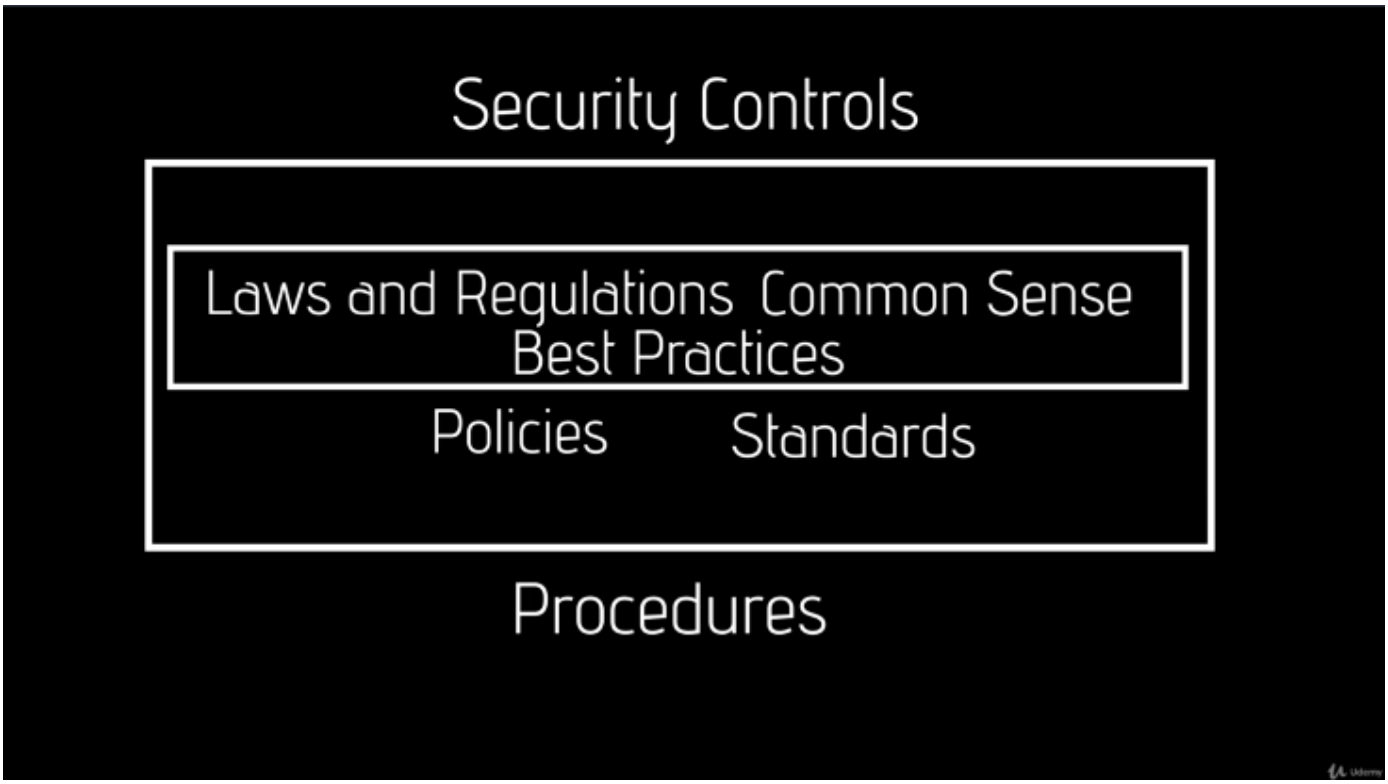
Policies(**REQUIRED**): (Document that defines how we are going to do something) e.g. Acceptable use policies

1. Broad in nature
2. used as Directives
3. Define roles and Responsibilities

Organizational Standards (**REQUIRED**): Define the acceptable level of performace of a policy (More detailed than a policy)
e.g Password policy: 'Defines that we should use strong passwords', organizational Policy: 'That password should be letters numbers etc.'

Security Controls come from the policies and standards

Procedures (**REQUIRED**:
Step by step how we do the task.



Guidelines(**OPTIONAL**):
Considerd something optional

---

11. IT Security Policies
SECURITY POLICIES ON THE SEC+

1. Acceptable use policy: Defines what a person can and cannot do on company assets.
   a. Personal use of the computer
2. Data Sensitivity and Classificaion policies: Define the importance or nature of different types of data.
3. Access Control Policies: Defines how people get access to data or resources
   a. What type of data do users have access to
   "Addresses Data access and classification restrictions"
4. Password Policy: Defines how you deal with passwords.
   a. Password Recovery
   b. Bad login
   c. Password retention
   d. Password reuse
5. Care and use of equipment: How you maintain company Equipment
6. Privacy Policies: Often used for customers
   a. e.g. web apps ebay, google, facebook. Users have to accept these. Defines your privacy.
   "Define how your data, or data usage will be shared with other resources"
7. Personnel Policies: Has to do with the people who a dealing with our data.
   a. e.g. Background checks, job rotation, mandatory vacations.

MEMORIZE ALL OF THESE and the details

12. Frameworks

Framework is a process idea "list of the big things you have to do as an it security person"

Types:

1. Regulatory frameworks
   e.g. NIST SP800-37
2. Non-regulatory framworks
   e.g. ISACA IT infrastructure
3. National standards
4. International Standards
   e.g. ISO 27000
5. Industry specific standards

NIST Risk management frameworks:

1. CATEGORIZE YOUR INFORMATION SYSTEMS
   Have an understanding of your workflows and processes and all of your inputs and outputs
2. SELECT SECURITY CONTROLS
   Start to figure out what you are going to do as far as your security controls
3. IMPLEMENT SECURITY CONTROLS
4. ASSESS THE SECURITY CONTROLS
   verify that everything works the way we want it to. (Done through a sandbox 'Test environment')

5. AUTHORIZING THE CONTROLS
   Some big boss has to give everything the go ahead
6. MONITORY SECURITY CONTROLS
   Watching what it is doing

REPEAT THE PROCESS

Quick Review:

-Frameworks come from a variety of sources including regulatory, non-regulatory, national, and industry standards (best practices)
-Evaluate security controls to verify what is feasible to implement in an environment
-Authorization is an important process when defining implementing, and measuring security controls.

---

13. Quanitative Risk Calculations

1. Asset Value : Cost of replacement
2. Exposure Factor: Percentage of an asset thats lost as the result of an incident

Asset Value x Exposure Factor = SINGLE LOSS EXPECTANCY

E.g: Router

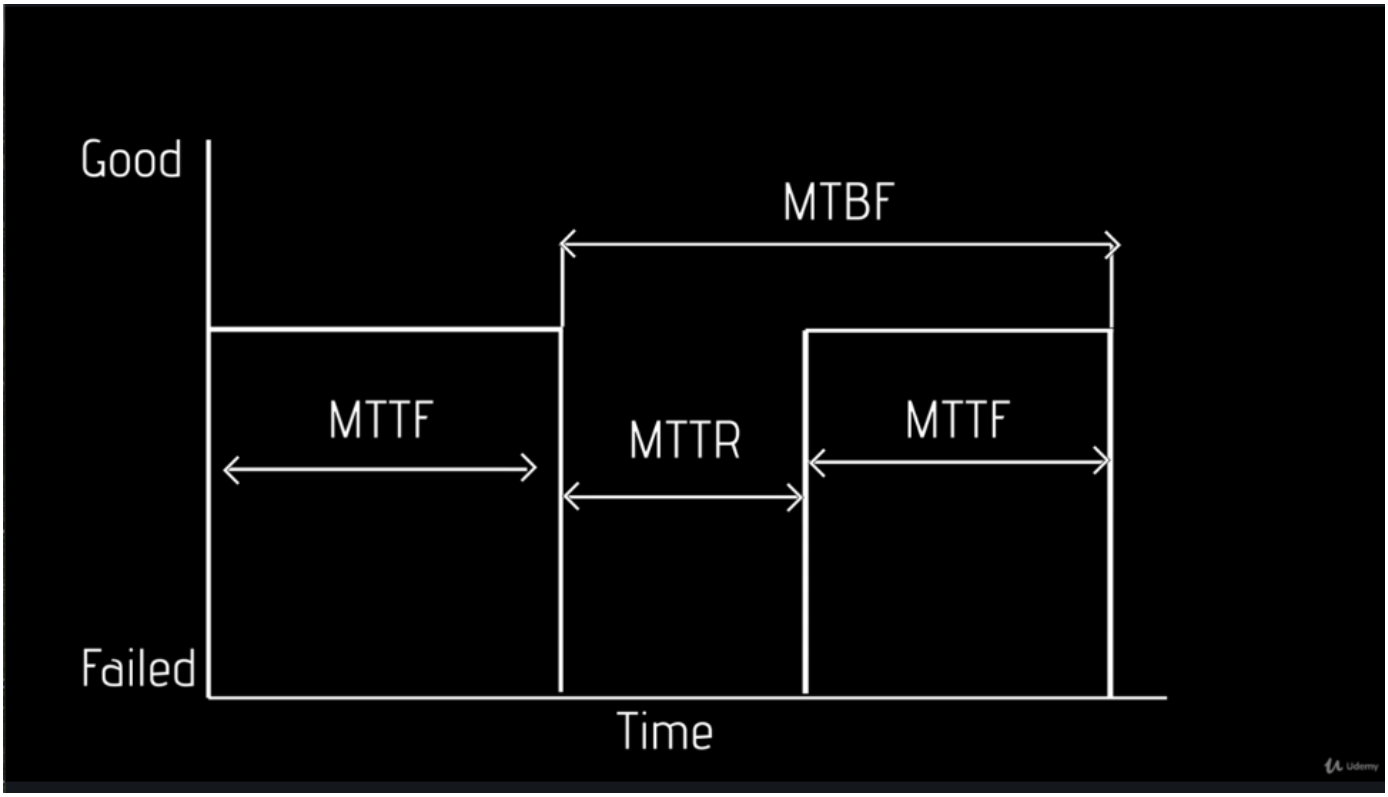
Asset Value: $5000.00
Exposure Factor: 1
Single Loss Expenctancy(SLE): $5000.00

What are the chances of this taking place?

Annualized Rate of Occurance (ARO): What are the chances of something happening annually.

e.g. : If the chances of the server room flooding are once every 20 years we do 1/20 and get .05

We take our SLE x ARO = *ANNUALIZED LOSS EXPECTANCY (ALE)*



MTBF IS USUALLY PROVIDED FOR THINGS THAT CAN BE REPAIRED
MTTF IS USUALLY APPLIED TO THINGS THAT CANNOT BE FIXED

NEED TO KNOW THESE CALCULATIONS FOR THE EXAM.

Quick review:

SLE = Asset Value x Exposure Factor

ALE = SLE x ARO

ALE = Annualized Loss Expectany

14. Business Impact Analysis

The three primary steps to Business Impact Analysis

1. Determine mission processes and recovery criticality
2. Identify resource requirements
3. Identify recovery priority for system resources

Breaking the 3 steps down:

1. Determine mission processes: What are the things we do within our IT infrastructure to do the things we do. (Mission essential funtions)
2. Recovery Criticality:
   Single Points of failure
3. Identify Resource Requirements

4. Identify Recovery Priority for system resources (what are the steps I need to take to get us back up and running the best)

IMPACT:

1. Property: loss of equipment, etc. Real things we could lose.
2. Money
3. People:
    1. Safety: avoid people getting hurt
    2. Life:
4. Finance:
    1. Credit
    2. Cash Flows
    3. Accounts Receivable
5. Reputation:
    1. Privacy is a killer of repuation

PRIVACY

PII (Personally Identifiable Information)
PHI (Personal Health information)

1. PIA (Privacy impact assesment): What happens if privacy is compromised?
2. PTA (Privacy Threshold assessment): What is this data, where is it, how do we store it? Often an in-house document.

PIA AND PTA ARE DONE TO UNDERSTAND THE POTENTIAL IMPACT OF LOSS OF PERSONAL INFORMATION CAN DO TO A BUSINESS

RTO (Recovery Time Objective): The minimum time neccessary to restore a critical system OR
Maximum time critical systems down without substantial impact

RPO (Recovery Point Objective): maximum amount of data that can be lost without substantial impact.

Quick Review:

-Recovery priorities help define what needs to be addressed to mmaintain business continuity
-Impact can be measured in terms of property and asset loss, productivity cost, and financial effect.
-PIA estimates the cost of loss of personal privacy or proprietary data.

---

15. Organizing Data

Data Sensitivity and Data Labeling

ORGANIZING DATA TYPES:

```
1. Public
        1. No restrictions
```

2. Confidential data
    1. Limited to authorized viewing as agreed on by the parties involved.

3. Private
    1. Limited to only the individual to whom the information is shared
    2. PII (Personally identifiable information)

4. Proprietary
    1. Like private information but at corporate level

5. Protected Health Information (PHI)
    1. HIPPA - Health insurance portability and accountability act

DATA ROLES:

1. Owner
    1. Legally responsible for the data

2. Steward/Custodian
    1. Maintain the accuracy and integrity of data

3. Privacy Officer
    1. Ensures data adheres to privacy policies and procedures

DATA USERS (USER ROLES):

1. Users
    1. Assigned standard permissions to complete a task

2. Privledged Users
    1. Increased access and control relative to a user

3. Executive Users
    1. Set policy on data and incident response actions

4. System administrators
    1. have complete control over the data OR system. Responsible Day to day manipulation of information and access

5. Data Owner/System Owner
    1. people who have legal ownership and legal responsibility

QUICK REVIEW:

- Data Labeling allows recipients of the data to know if or how the data can be shared
- The "Owner" role in the data role model has the legal responsibility of the data
- User permissions are set with just enough permissions to accomplish the tasks

---

16. Security Training

*OnBoarding (Remember for the exam):

```
1. Requires a good background check
2. NDA (Non disclosure agreement)
3. Standard Operating procedures
4. Specialized issues
5. Rules of behavior (e.g. Acceptable Use Policy)
6. General Security policies
```

All employees will be subject to continuing education

OffBoarding (Remember for the exam):

```
1. Disable accounts
        1. Never delete an account!
2. Return Credentials
3. Exit Interview
4. Knowledge Transfer
```

PII (Personally Identifiable Information):

```
EXAMPLES:

1. Full Name
2. Home address
3. Email address
4. National Identification Number
5. Passport Number
6. Vehicle Registration Plate Number
7. Drivers License Number
8. Face, Fingerprint, or handwriting
9. Credit card numbers
10. Digital Identity
11. Date of birth
```

Personnel Managment Controls

```
1. Mandatory Vacations
        1. Require
        2. Two weeks
        3. Dependency issues
```

4. makes fraud harder
5. prevents collusion

2. Job Rotation
    1. Redundancy and backup
    2. makes fraud more difficult
    3. Allows for cross training

3. Separation of duties
    1. Requires dual Execution

Roles

1. System Owner
    1. management level role
    2. maintains security if the system
    3. Defines a system administrator
    4. Works with all data owners to ensure data security

2. System Administrator
    1. Day-to-Day administration of a system
    2. implement security controls on that system

3. Data Owner
    1. Defines the sensitivity of the data
    2. Defines the protection of the data
    3. Works with the system owner to protect the data
    4. Defines Access to the data

4. User
    1. Accessess and uses the assigned data responsibly
    2. Monitors and Reports Security Breaches

5. Privledged User
    1. Has special access to data beyond the typical user
    2. Works closely with system administrators to ensure data security

6. Executive User
    1. Read only access but can look at all business data on the system

Quick Review:

-Onboarding is the starting point for security training, but good security training is an ongoing process
-Offboarding is an important time to talk to the exiting employee, find out where their data is stored, and other pertinent information
-Personnel controls and role-based data controls help secure functions and the dat within an organization

---

17.Third Party Agreements

Business Partners Agreement (BPA):
*BPAs are very common

```
A good BPA Includes:

        1. Primary Entities
        2. Time Frame
        3. Financial Issues
        4. Management
```

Service Level Agreement(SLA):

```
A good SLA Includes:

        1. Service to be provided
        2. Minimum up-time
        3. Response Time (Contacts)
        4. Start and end data for the service
```

Interconnection Security Agreement (ISA):

```
        NIST 800-47 - This document quantifies how more than one government
entities can transfer data safely

A good ISA includes:

        1. Statement of requirements
                1. Why are we interconnecting?
                2. Who is interconnecting?
        2. System Security Considerations
                1. What information is interconnecting?
                2. Where is this information going?
                3. What services are involved?
                4. What encryption is needed?
        3. Topological Drawing
        4. Signiture Authority
        5.
```

Memoradum of Understanding/Memorandum of Agreement (MOU/MOA)

```
A good MOU/MOA includes:
        1. Purpose of the interconnection
        2. Relevant Authorities
        3. Specify the responsibilities
                1. Downtime
                2. Billing
        4. Defines the terms of the agreement
                1. cost
        5. Termination/Reauthorization
```

QUICK REVIEW:

- Remember the four types of agreements and their functions
- BPAs and SLAs are used in the private sector
- ISAs and MOU/MOAs are used in the public sector
- Have a clear understanding of when and where to use each of these third-Party agreements

---

QUIZ 1: RISK MANAGEMENT QUIZ

Question 1:

What is the CIA triad of security?

- (●) Confidentiality, integrity, and availability
- ( ) Censorship, information, and accessibility
- ( ) Correlation, information, and availability
- ( ) Confidentiality, information, and auditing

Question 2:

Which of the following threat actors is motivated by intent to make a public social statement?

- Script kiddie
- Organized crime
- Nation States
- (●) Hacktivist

Question 3:

What is the process of having an outside or 3rd party assess an organization's security vulnerabilities?

- Nessus
- (●) Penetration (pen) testing
- Adversarial
- Accidental

Question 4:

Manufacturer and vendor guides can provide which of the following?

- (●) Setup suggestions
- All known security controls
- All pertinent information for installing the device in a network configuration
- Most recent virus/malware associated with a device

Question 5:

Which one of the following is a category of security control?

- Malware installation
- Installing locks
- Training users
- Administrative (managerial)

Question 6:

A self-directed combination of administrative, physical, and technical controls is an example of:

- Defense in depth
- Vendor diversity
- IT governance
- AAA

Question 7:

What describes the set of overarching rules that defines how an organization and its employees conduct themselves?

- Common sense
- Governance
- Best practices
- Laws and regulations

Question 8:

Which term defines how people get access to data and other resources?

- Acceptable use policy
- Data classification policy
- Access control policy
- Password policy

Question 9:

Framework sources can come from which of the following?

- Regulatory bodies
- Industry standards
- National standards
- Non-regulatory bodies
- All of the above

Question 10:

True or false: when calculating asset value, you only need to be worried about the cost to replace the item itself.

- True
- False

Question 11:

What is the purpose of a privacy threshold assessment (PTA)?

- ○ To monitor compliance, which is only necessary for HIPAA information
- ○ To measure how much damage a company can handle and still maintain business operations
- ● To analyze how personal information is consumed, transferred, and transmitted within an information system
- ○ It's a made-up term not found in Security+

Question 12:

When defining users' roles, which users have the legal responsibility and liability for the data?

- ○ User
- ○ Privileged user
- ○ System administrator
- ● Owner
- ○ Privacy officer

Question 13:

Which personnel management control allows for cross-training?

- [x] Job rotation
- [ ] Mandatory vacation
- [ ] Separation of duties
- [ ] System owner

Question 14:

Which type of agreement is needed when two private-sector people or organizations wish to work together?

- [ ] Service level agreement (SLA)
- [x] Business partners agreement (BPA)
- [ ] Interconnections security agreement (ISA)
- [ ] Memorandum