Section 19:Managing Risk

149.What is Risk Management?

Overview Ideas:

How to plan:

- Secure infrastructure from threats
- Security policies incorporate practices required by laws and standards (NIST - National Institure of Standards and Technology)
- Security policies incorportate industry standard best practices
- Security policies are printed or electronic documents (Overview statements)
- Security controls (In more depth how to handle a policy) are generated from security policies
- Security controls detail specifics and lead to procedures
- Procedures detail how to implement controls on systems (How do we do the security control)

Review:

*Security polices are documents with broad overview statements
*Security controls provide more details
*Procedures discuss specific implementation of policies

---

150. Security Policies

*A statement that an orgainization makes that defines the goals and motivations of that organization in terms of security policy
*Security policies are usually written documents

For the exam remember these security policies:

1. Acceptable Use Policy
   a. Defines ownership (e.g. the smart phone you have belongs to the company)
   b. Defines website access (e.g. Not allowed to go to facebook)
   c. Defines time (e.g. Not allowed to go to facebook before 5pm)
2. Remote Access Policy
   a. VPN (All connections to our network remotely requires a VPN)
   b. Authentication
3. Password Policy
   a. Complexity
   b. Age
   c. Lockout policy
4. IT Safety Policy
   a. Lifting equipment

    b. Equipment Handling
    c. Spills

More terms on the exam:

1. NDA (non-disclosure agreement)
2. License Restrictions
    a. Usage
    b. Transfer
    c. Renewal
3. International Export Control
    a. Military information
    b. Nuclear Information
    c. License Keys

---

151. Change Mangement

Change management team: (Manage Changes, Meet on a regular basis)
-Business analyst
-Marketing
-Operations
-Management

Strategic Change vs. Infrastructure Change

Strategic Change - a massive change that will substancially effect the business of the infrastructure itself. (e.g. Replacing all the computers, moving to a new country). The Change management committee does not make these changes.

Infrastructure Change - Makes changes, but does not make massive changes (this is what the change managment team is for)

Change Request Document:

1. Type of change
2. Configuration Procedures
3. Rollback process
4. Potential Impact
5. Notification

Change request is submitted to the committee and they make a decision.
Once the change request is accepted the change committee is still involved with implementation

Documentation is the last step in the change management Process

Review:

NET+ will test on these

*The change management team handles infrastructure-level changes
*The change process includes requests, types of changes, configuration procedures, rollback and more
*The end game is documentation of all the changes made

---

152. User Training

Areas that a good user training program covers:

- Acceptable use policy read and signed
- Users should get training on password policies
- Users need training on systems
- Teach users about social engineering
- Train users to avoid malware

Review:
*Network techs get called on for user training
*Train users on acceptable use and password policies
*users should recognize social engineering and avoid malware

---

153. Standard Business Documentation

Net+ covers 4 types:

1. Service Level Agreement (SLA)
   a. Between a customer and service
   b. Scope, quality and terms of service to be provided
   - Definition of service provided
   - Equipment
   - Technical support
2. Memorandum of Understanding (MOU)
   a. Defines an agreement between two parties
   b. Used where a legally binding contact is inappropriate
   - Definition of agreed duties
   - Time Frame
   - Could define lots of things depending on the type of MOU
3. Multi-Source Agreement (MSA)
   a. Companies make these between each other and stick to them and make the right kind of parts for each other
4. Statement of Work (SOW)
   a. Legal contract between two parties (Vendor and customer)
   -Defines the services to be performed/supplied

-Defines time frame/deliverables
-Defines milestones/defines progress

Review

- Standard business documentation is common in networking
- Standards on the exam include SLA, MOU, MSA, SOW
- These are real-world standards

154.Mitigating Network Threats

Four big areas:

1. Training and Awareness
2. Patch Management
3. Policies and Procedures
4. Incident Response

Review:

*Remember these four for the exam

*Implement proper mitigation techniques to protect a network
*Start with training and awareness, as well as patch management
*Finish by including polices, prodecures, and incident response

155. High Availablity

"To keep some form of service up and running despite any reason" or "Maintaining up-time" Or "things we can do to make sure we never go down"

High availability:

1. Redundancy
2. Fault tolerance

- NIC teaming (Two ports functioning for one Server if one goes down the other will keep running)
- Clustering (Multiple servers in their own network that will act together as a single device and if one goes down the other funtion just fine)

For the exam remember Redundacy and fault tolerance

Review:

*High availablity is supported with fault tolerance and redundancy
*High availablity means that services aren't lost, not how fast they are recovered
*Raid array, redundant power supply, UPS, clustering, and failover systems are high availablity methods

QUIZ

1. Which of the following is not an element of risk management?

   a. Secure infrastructure from threats

   b. Security policies

   c. Security controls

   d. Security Procedures

2. Which choice is not found in a change request?

   a. Type of change

   b. Configuration procedures

   c. Rollback process

   d. cost of implementation

3. Which area does not require user training?

   a. Acceptable use policies

   b. Recycle Policies

   b. Password policies

   c. System and workplace security

   d. Social engineering

   e. Malware avoidance

4. Which choice is not a standard business document?

   a. SLA

   b. MOU

   c. MSA

   d. WPA

   e. SOW

5. Which of the following is not a good approach to mitigating network threats?

   a. Training and awareness

   b. Patch management

   c. Policies and Procedures

   d. Documenting Chain of custody

   e. Incident response