13.1.8 Credential and Organizational Policies Facts

This lesson covers the following topics:

- Change-management policies
- Change-control policies
- Credential policies

Change-Management Policies

The steps involved in implementing a policy change in an organization could include:

- Identifying the need for a change, documenting it, and submitting a change request for approval. The approval process should be defined as well.
- Conducting a feasibility analysis that includes technical and budgetary considerations. It should also identify any potential impacts on the security of the network.
- Designing a method for implementing the change.
- Notifying all affected parties of the pending change.
- Implementing the change. This includes identifying a maintenance window during which the system will be unavailable. This is sometimes referred to as authorized downtime.
- Testing the implementation to make sure it conforms to the plan and that the change doesn't negatively affect the confidentiality, integrity, and accessibility of your IT infrastructure.
- Documenting the change. Documenting changes allows you to see the history of changes and can be a valuable tool for troubleshooting. For example, if the change includes new hardware, you'd want to document all IP addresses, MAC addresses, locations, manufacturers, and model numbers.

Change-management policies are helpful to an organization because they do the following:

- Help to understand what's needed
- Help to understand the impact of the proposed changes
- Help to manage the cost of the change
- Reduce the time needed to implement the change

Change-Control Policies

Change control is a standardized approach to managing any changes that are made at any time a production system is altered. This includes modifications of existing applications, implementation of new applications, removal of old applications, and upgrading or patching software. Change-control management is very similar to application development in its processes. Properly documenting and executing the change-control process is essential for changes to be effective and seamless. Change-control policies are beneficial because they:

- Help to streamline any changes made to new or existing software
- Help to reduce the risk associated with these changes
- Provide awareness to the consequences of an outage

The general steps in the process that should be considered are:

1. Recognize a need.
2. Submit a request. This step can be best documented with a change request form.

3. Start a feasibility analysis that includes technical feasibility, cost justification, and a security review.
4. Document the change plan.
5. Approach management for approval.
6. Submit the change plan to developers. Developers then perform the coding for the change.
7. Test the change for conformance to the plan and security practices.
8. Document the change.
9. Release the new revision to production through the librarian.

Credential Policies

A credential policy identifies guidelines for accessing network or system resources. Credential policies standardize requirements for user accounts and can also refer to device access. Rules may include:

- Password requirements, such as required length of a password, use of special characters, or restrictions on previously used passwords
- Account lockouts, such as how many attempts before a lockout, how long the lockout lasts, what needs to happen before the account can be unlocked
- Credential expiration, such as how many days before a credential expires