Armaan Shamsaasef

Change Management

Notes: Change Management (SY0-701 - 1.3)

Core Concept: Change Management is a formal, structured process for making changes to an IT environment. Its primary goal is to ensure that changes are made in a controlled, coordinated, and documented way to **avoid unintended consequences and security vulnerabilities.**

The Purpose & Benefits

- **Avoid Downtime:** Prevent service outages caused by poorly planned changes.
- **Increase Security**: Ensure changes do not inadvertently create new security gaps.
- **Improve Communication:** Keep all stakeholders (management, IT teams, security, etc.) informed.
- **Create a Rollback Plan:** Have a predefined way to reverse the change if it fails.
- **Maintain Documentation**: Keep a clear record of *what* was changed, *why*, *when*, and *by whom*.

The Standard Change Management Process

The process follows a clear, step-by-step lifecycle for every proposed change.

1. Request & Proposal

- A formal request is submitted detailing:
    - What the change is.
    - Why the change is needed (the business reason).
    - The specific configuration modifications required.

2. Approval Process

- The request is reviewed by a Change Control Board (CCB), which typically includes:
    - Management
    - Security Team Members
    - Application and System Owners
    - Network Administrators
- The board assesses the risk, purpose, and business impact of the change.

3. Documentation

- Once approved, the change is fully documented.
- Key Details to Document:
    - Purpose of the change.
    - Backout/Rollback Plan: The exact steps to undo the change if it causes problems.
    - Scope: Which systems and users will be affected.
    - Maintenance Window: The scheduled time for the change to occur to minimize disruption.

4. Testing & The Rollback Plan

- Testing: The change should be tested in a non-production environment first to identify issues.
- Rollback Plan: This is a critical safety net. It must be tested and confirmed to work *before* implementing the change in production.

5. Implementation

- The change is deployed during the approved maintenance window, following the documented plan.

6. Post-Implementation Review

- After the change is complete, the team verifies that it was successful and did not cause any negative impact.
- The documentation is updated to reflect the final outcome.

Example from the Video

Scenario: A system administrator needs to update the firmware on a network firewall.

1. **Request**: The admin submits a request explaining that the update patches a critical security vulnerability.
2. **Approval**: The Change Control Board approves the request but mandates it be done during a weekend maintenance window.
3. **Documentation**: The admin documents the exact steps for the update and, crucially, the process to revert to the old firmware if the new version causes network issues.
4. **Implementation**: During the maintenance window, the admin applies the update.
5. **Review**: After the update, the team confirms the firewall is operational and the vulnerability is patched.

Key Takeaway

Change Management replaces informal, ad-hoc changes with a disciplined process. It is a fundamental security control that prevents misconfigurations, outages, and security weaknesses by ensuring that every modification is reviewed, approved, documented, and reversible.