Exam Cram Notes: General Security Concepts – Change Management

1. What is Change Management?

Change management is a structured process for implementing changes in IT environments while **minimizing security risks** and **ensuring business continuity**. It ensures changes are **documented, tested, approved, and monitored**.

---

2. Key Phases of Change Management

1. **Request for Change (RFC)** – A formal proposal to modify a system or process.
2. **Change Evaluation & Risk Assessment –** Determines impact, security risks, and feasibility.
3. **Approval Process** – Change Advisory Board (CAB) or management **approves or rejects** the change.
4. **Testing & Validation –** Change is tested in a **staging environment** before deployment.
5. **Implementation & Deployment –** Change is applied following a structured **rollout plan**.
6. **Monitoring & Review** – Ensures change is working correctly and addresses **any issues**.
7. **Documentation & Audit Logs –** Records change details for future reference and compliance.

---

3. Configuration Management

- Ensures **systems maintain a consistent, secure state** after changes.
- Uses **configuration baselines** (standardized system settings).
- Example: **Automating firewall rule updates** while ensuring compliance with security policies.

---

4. Patch Management

- Part of change management that handles **software updates** to fix security vulnerabilities.
- Patch management process:
  1. **Identify required patches** (via vendor updates, vulnerability scanning).
  2. **Test patches** in a controlled environment.
  3. **Deploy patches** to production systems.
  4. **Monitor for failures or issues** after deployment.
- Example: Applying **critical security patches** to fix OS vulnerabilities.

---

5. Change Control Documentation

- Every change must be **documented** with:
  - Reason for change
  - Risk assessment results
  - Implementation steps
  - Testing results
  - Approval records
  - Post-change monitoring results
- Example: A company implementing a **new VPN solution** must document potential risks and rollback plans.

Key Exam Tips

✅ Know the **steps of the change management process** and their purpose.
✅ Understand **how configuration and patch management** fit into security.
✅ Expect scenario-based questions on **handling IT changes securely**.
✅ Be familiar with **change control documentation** and compliance requirements