Organized Notes on IT Security Gap Analysis

1. Definition and Purpose

A gap analysis is a study to compare the current state ('where we are') to the desired future state ('where we would like to be'). In IT security, gap analyses help identify future security needs and create a plan to bridge the gaps.

2. Complexity of the Process

While simple to explain, the process is complex and involves:

- Understanding all aspects of IT security in the organization.
- Gathering and analyzing data across weeks, months, or even years.
- Involving multiple stakeholders and extensive project planning.

3. Baseline Establishment

A baseline is essential for comparison and goal setting. Common baselines include:

- NIST SP 800-171 Rev. 2: Protecting Controlled Unclassified Information.
- ISO/IEC 27001: Information Security Management Systems.
- Custom baselines tailored to organizational needs.

4. Evaluating People and Processes

Assess people:

- Formal experience in IT security.
- Training and knowledge of security policies.

Review processes:

- Alignment of existing IT systems with organizational security policies.

5. Conducting the Analysis

Comparison of Systems:

- Identify weaknesses in current systems.
- Evaluate processes to mitigate these weaknesses.

Detailed Breakdown:

Start with broad categories (e.g., access control) and divide into smaller tasks. Example from NIST SP 800-171:

- Access control: Limit system access to unauthorized users, processes, and devices.
- Subtasks: User registration/deregistration, privileged access management, access rights reviews.

6. Documenting Findings

Compile data on all processes, devices, and locations. Compare:

- Current state vs. baseline objectives.
- Identify gaps and areas for improvement.

7. Planning for the Future

Develop a path to move from the current state to the desired state:

- Consider time, budget, equipment needs, and change control processes.
- Summarize findings and recommendations in a gap analysis report.

8. Final Gap Analysis Report

Key components:

- Detailed findings of the current state.
- A pathway to meet baseline objectives.
- Recommendations for improvements.

Example Report Format:

- System Requirements Table:
- List all system requirements and assess them across multiple locations.

- Use color-coded markers:
    - Green: Locations close to meeting baseline.
    - Yellow: Locations needing moderate improvements.
    - Red: Locations needing significant work.

Prioritize improvements: Address red areas first, followed by yellow, and then green. Include detailed explanations for color coding and strategies to meet baseline goals.

9. Summary

The gap analysis report provides a comprehensive understanding of:

- Current IT security posture.
- Steps and resources needed to achieve desired security standards.
- A roadmap for future improvements.