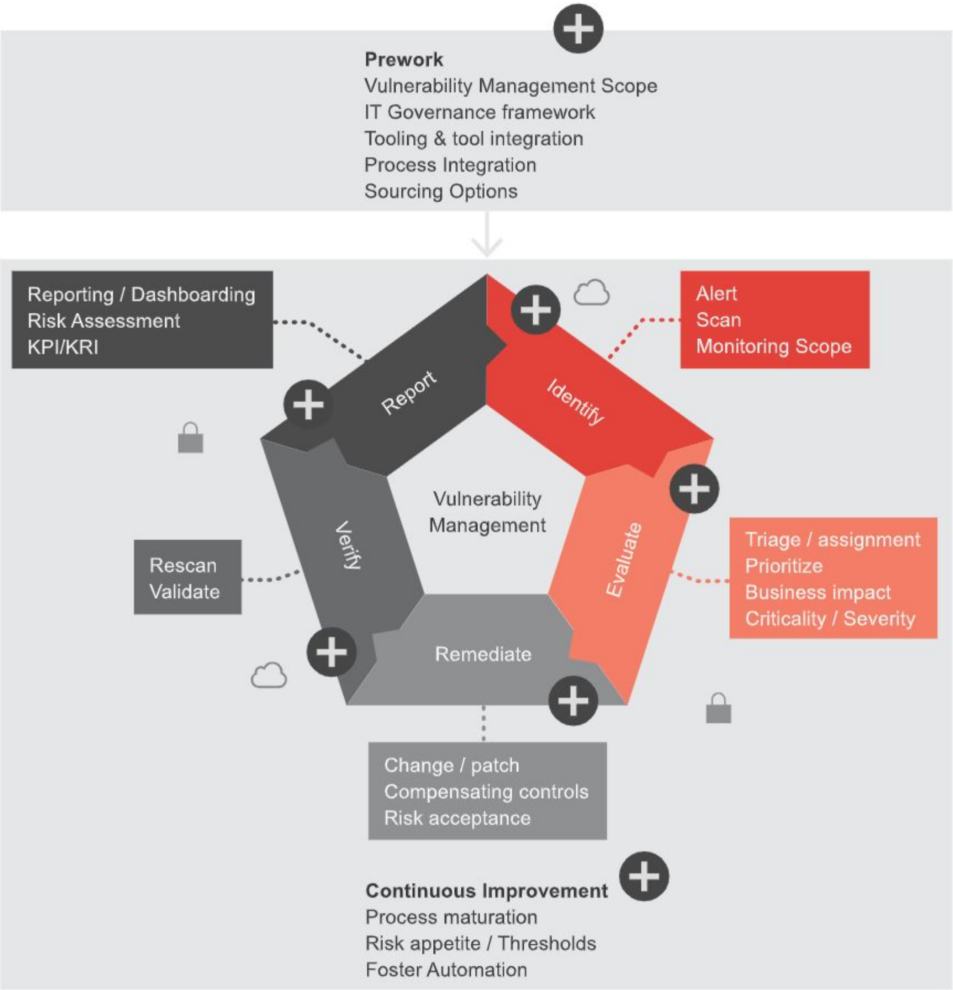
IT System Security Baseline



Prework
Vulnerability Management Scope
IT Governance framework
Tooling & tool integration
Process Integration
Sourcing Options

Vulnerability Management

Identify

Alert
Scan
Monitoring Scope

Evaluate

Triage / assignment
Prioritize
Business impact
Criticality / Severity

Remediate

Change / patch
Compensating controls
Risk acceptance

Verify

Rescan
Validate

Report

Reporting / Dashboarding
Risk Assessment
KPI/KRI

Continuous Improvement
Process maturation
Risk appetite / Thresholds
Foster Automation

Implementing Security Baseline in the Prework Phase

- Perform asset discovery and create an inventory of all IT assets.
- Document the ownership and business criticality of these assets.
- Define asset groups based on their function, data classification, or environment.
- Determine which compliance standard(s) to follow based on industry and data sensitivity.
- Define roles and responsibilities for security, IT operations, and asset owners.

PROCESS INTEGRATION

Vulnerability management is not a new process, but rather a different angle on IT monitoring, event management and incident response. This includes incident management for handling a critical vulnerability. Consequently, compliance needs to be managed by defining technical standards and systematically monitoring compliance with the IT standards.

Process Integration: Vulnerability Management

- Integrate vulnerability management into existing IT processes.
- Define technical standards for compliance.
- Monitor compliance with IT standards.
- Develop incident response plans, including for critical vulnerabilities.
- Ensure IT monitoring and event management are aligned with vulnerability management.

Continuous Improvement: Key Steps

- Alert: Central asset inventory and scanning method. Scope in assets and critical assets.
- Evaluate: Company-specific risks and vulnerabilities. Context, criticality, severity.
- Remediate: Address vulnerabilities and patch management process. Consider compensating measures and residual risk.
- Verify: Timely rescan, periodic reviews, and escalation process.
- Report: Stakeholder-specific reporting and dashboard overview.