Policy & Standards
Policy and standards are defined in specific processes and are reviewed and updated as a result of successes or failures. Employees are made aware of standards and training requirements as available.

Level 2: Defined
Policy and standards have been carefully considered and clearly defined. Training on required policies and standards is available.

Level 3: Quantitatively Managed
Policies and standards are clearly defined and communicated. Training on required policies and standards is required.

Level 4: Optimizing
Policies and standards are clearly defined and communicated. Policies and standards are reviewed and updated on a regular basis.

Context
Critical data (e.g., asset details, ownership, and common vulnerabilities) can be individually assessed with varying degrees of accuracy.

Level 2: Defined
There is a central repository of contextual information that is consistent and up to date for all systems and applications.

Level 3: Quantitatively Managed
The central repository requires that certain contextual information requirements be analyzed and validated, and that it is used on program needs.

Level 4: Optimizing
Context is used to define contextual information requirements and to define, prioritize, and refine contextual options.

Automated
Infrastructure and applications are managed with automation and technology to identify vulnerabilities, flaws, deficiencies, and other categorized reports.

Level 2: Defined
There are defined and mandated organization-wide automated or technology-assisted processes and procedures that are defined and followed for certain departments or locations.

Level 3: Quantitatively Managed
There are defined and mandated organization-wide automated or technology-assisted processes and procedures that are defined and followed for certain departments or locations. Technology is made available through enterprise licensing agreements as a service.

Level 4: Optimizing
Scanning coverage is measured and includes the documentation of automated scanning activity, such as automated scanning (where applicable). Automated or technology-assisted processes and procedures are designed to achieve or exceed the goals.

Level 5: Optimizing
Automated or technology-assisted processes and procedures that are defined and followed for certain departments or locations are updated based on previous measurements.

Manually
Manual testing or review occurs when specifically required or requested.

Level 2: Defined
Manual testing or reviewing processes are established and followed for certain departments or locations.

Level 3: Quantitatively Managed
Manual testing or review occurs specifically when required by policy or policies. Manual testing or review processes are established and followed for certain departments or locations.

Level 4: Optimizing
Deviations from manual testing or reviewing requirements are tracked and reported.

Level 5: Optimizing
Manual testing or review processes include automated or technology-assisted processes that are available to provide specific vulnerabilities or risks.

External
External vulnerabilities and documents are handled on a case-by-case basis.

Level 2: Defined
External vulnerabilities disclosure policy (VDP) and external information requirements and procedures are not documented.

Level 3: Quantitatively Managed
More comprehensive VDP in place, along with terms and conditions for providing external vulnerability reports. Policies, requirements, and procedures are documented.

Level 4: Optimizing
Compliance with VDP and terms and conditions for providing external vulnerability reports is used to streamline processes and evaluate vendors and research.

Root Cause Analysis
Root cause analysis is performed based on cost of incident investigation.

Level 2: Defined
Root cause analysis is performed based on cost of incident investigation. Root cause analysis is performed when necessary.

Level 3: Quantitatively Managed
Root cause analysis is performed based on cost of incident investigation. Root cause analysis is performed when necessary and is reviewed as part of incident response.

Level 4: Optimizing
Root cause analysis is performed based on cost of incident investigation. Root cause analysis is performed when necessary. Root cause analysis is documented and reviewed.

Metrics & Reporting
Simple, point-in-time operational metrics are available primarily from external sources, and from reports leveraging contextual scanning or filtering.

Level 2: Defined
Reporting and compliance requirements are initially defined on a case-by-case basis.

Level 3: Quantitatively Managed
Reporting requirements, including all required programs, operational, and external metrics are defined and measured.

Level 4: Optimizing
Custom reporting is available as a service or on site with assistance in refining metrics. Custom reporting is available as a service or on site with assistance in refining metrics.

Alerting
Alerting is either not available or only available within security-specific technologies.

Level 2: Defined
Alerting is available for specific departments or divisions. Alerts are reviewed and deployed on a case-by-case basis.

Level 3: Quantitatively Managed
Alerting is available for specific departments or divisions. Alerts are reviewed and deployed on a case-by-case basis.

Level 4: Optimizing
Alerting is available for specific departments or divisions. Alerts are reviewed and deployed on a case-by-case basis.

Change Management
Changes related to vulnerability management activities are reviewed through the organizational change management process.

Level 2: Defined
Changes related to vulnerability management activities are reviewed through the organizational change management process. Changes related to vulnerability management activities are reviewed through the organizational change management process.

Level 3: Quantitatively Managed
Changes related to vulnerability management activities are reviewed through the organizational change management process. Changes related to vulnerability management activities are reviewed through the organizational change management process.

Level 4: Optimizing
Changes related to vulnerability management activities are reviewed through the organizational change management process.

Patch Management
Patches are applied manually or scheduled by systems and staff.

Level 2: Defined
Patches are applied manually or scheduled by systems and staff.

Level 3: Quantitatively Managed
Patches are applied automatically or scheduled by systems and staff.

Level 4: Optimizing
Patch management activities are tracked along with compliance metrics and remediation timelines and the success rate.

Configuration Management
Configuration requirements are not well-defined and changes are either applied manually or scheduled by systems and staff.

Level 2: Defined
Configuration requirements are well-defined and changes are either applied manually or scheduled by systems and staff.

Level 3: Quantitatively Managed
Configuration requirements are well-defined and changes are either applied manually or scheduled by systems and staff.

Level 4: Optimizing
Configurations are defined for all supported platforms and technologies are available to automate major configuration changes for all platforms.

Vulnerability Management Model

Preparedness

Identify

Analyze

Communicate

Alert

Treat

Context

Automated

Manual

External

Prioritization

Root Cause Analysis

Metrics & Reporting

Change Management

Patch Management

Configuration Management

Vulnerability Management Metrics