BITS Suggested Vulnerability Process Health Metrics

DEFINITION OF VULNERABILITY MANAGEMENT

The BITS membership recognizes Vulnerability Management as the practice of identification, assessment, reporting and disposition of technology weaknesses threatening information security associated with software and hardware that will serve as the basic foundation of the organization’s Vulnerability Management Program (VMP).

PURPOSE OF PROCESS HEALTH METRICS

This document comprises a primary set of metric definitions that can apply to all member organizations. The metrics are intended to measure the health of vulnerability management processes and to provide a foundation for potential benchmarks across member organizations. Included in this are:

- Requirements to proper metrics measurement
- Assumptions and category definitions
- Recommended metrics definitions
- An appendix of metrics with recommended audience and presentation considerations

REQUIREMENTS FOR PROPER VMP METRICS

Several key components and assumptions will aid in building a solid foundation for VMP process health reporting. These include:

- Accurate and complete software/hardware assets and application inventory
- Severity framework for threats and risk
- Risk appetite is defined and approved at the organization’s executive level
- Remediation Service Level Agreement (SLA) based on the severity of threats and risk. Optionally, separate SLAs can be defined for:
    - Externally facing assets (Internet)
    - Internally facing assets (Intranet)
- Organization policies, standards and guidelines defined, with a consequence model for non-compliance

KEY ASSUMPTIONS

Following are assumptions for successful process health metrics:

- Software and hardware asset and application inventory is accurate, complete and up to date
- Threat / risk severity is defined (3-4 tiers [Critical/Emergency | High | Medium | Low]*)
- A well-defined risk appetite drives prioritization and risk treatment
- Remediation SLA should be based on and driven by the risk appetite of the organization. Key Performance Indicator (KPI) for “Security SLA” will determine the true risk tied to vulnerabilities & relevant cyber risk, while Remediation SLA can provide an operational risk perspective.

- Organizations can define separate SLA for security and operations (e.g., *Vulnerability First Found* for Information Security & *Patch First Available* for IT Operations). In such cases, '***Security SLA***' compliance will show the 'true' threat-centric risk metrics.
- Remediation SLA is platform agnostic and applicable globally across all asset types (OS, platform, function, role, etc.).
- Policies / Standards / Guidelines are well defined and enforceable.

** Organizations may choose to adopt 3 tiers (High/Medium/Low) or 4 tiers (Critical or Emergency/High/Medium/Low)*

METRIC CATEGORIES

The BITS Vulnerability Management Working Group suggests three categories of metrics that define metric audience and intent. These are indicated by the column headings in the *Metrics Map*:

- **Operations:** Metrics that assist in managing the operations that discover and disclose vulnerabilities to the organization that are typically within the responsibility of Information Security (IS).
- **Response:** Metrics that assist in managing the operations that mitigate and remediate vulnerabilities for the organization, and that are typically within the responsibility of Information Technology (IT).
- **Risk:** Metrics that assist in managing the risk posed by vulnerabilities to the organization, and that are typically of interest to senior management.

BITS PRIMARY VULNERABILITY MANAGEMENT METRICS

The BITS Vulnerability Management Working Group suggests the following metrics to be of priority value in managing VMP operations, response and risk. The first level indent indicates the **intent** of the subordinate ***metrics***.

- Operations
  - **Coverage:** Indicates the scope of the vulnerability identification capability across the organization's known infrastructure against the desired scope. Two metrics are relevant here:
    - ***% Scanned***: The percentage of the organization's in-scope infrastructure and applications that is being scanned for vulnerabilities.
    - ***% Assessed within SLA***: The percentage of applications or infrastructure that is assessed within intended timelines.
  - **Depth:** Indicates the degree to which full discovery capability is exercised.
    - ***% Authenticated Scans***: The percentage of scans that leverage authentication to fully identify vulnerabilities within scanning capability.
- Response
  - **Most Vulnerable:** Indicates the most problematic infrastructure for remediation of vulnerabilities.
    - ***Hardware / Software with the Highest Risk***: A sorted listing of hardware or software with the highest risk (by severity & count of vulnerabilities), presented in descending order
  - **Remediation Success:** Indicates how well IT is meeting objectives for remediation.
    - ***% Fixed within Service Level Agreement (SLA)***: The percentage of vulnerabilities closed within SLA.
    - ***% Compliant Systems***: The percentage of deployed systems that are fully compliant with the organization's vulnerability management standards.

- **Risk**
  - <u>**Highest Risk**</u>: Indicates the exposure level due to highest risk vulnerabilities.
    - ***% of Overdue Highest Risk Vulnerabilities*:** The percentage of highest risk vulnerabilities that remain open past SLA.
  - <u>**Risk Exposure**</u>**:** Indicates the level of overall exposure, due to vulnerabilities, that is beyond accepted risk.
    - ***% of Overdue Open vulnerabilities*:** The percentage of all vulnerabilities that remain open past SLA.
    - ***% of Long Overdue Open vulnerabilities*:** The percentage of all vulnerabilities that remain open 180 days past SLA.
    - ***% Non-Compliant Systems*:** The percentage of deployed systems that are not fully compliant with security standards
    - **# Open Deferred / Excepted Vulnerabilities:** The count of open vulnerabilities acknowledged for remediation past SLA.
    - **% Risk Accepted/Policy Excepted Unassessed:** The percentage of assets and applications that have risk acceptance or policy exception allowing non-coverage by VMP