strobes

CYBERSECURITY CENTRE of EXCELLENCE

A joint initiative of DSCI & Government of Telangana

DSCI PROMOTING DATA PROTECTION

A NASSCOM® Initiative

WeSecureApp

WHITEPAPER

WHAT DEFINES A ROBUST VULNERABILITY RISK MANAGEMENT STRATEGY?

Importance of efficient VRM for Security & Risk Management Leaders

CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

WeSecureApp

Table of contents

CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

WeSecureApp

Introduction

Cybercrime is increasing exponentially each year, with the annual global cost of such crimes now approaching more than **$100 billion per year**. The future looks equally grim and the damage via cyber-crime is projected to hit $6 trillion annually by 2022, with cybersecurity spending to hit **$1 trillion** over the next **four years**.

As digitalization is embraced across organizations, the need to deal with prevailing vulnerabilities is crucial. In 2020 itself, approx. **18,000 vulnerabilities** were published in the NVD(National Vulnerability Database), for which an update or a patch is nearly available for **~98% of these vulnerabilities**. Despite high dependency on third-parties, organizations are still not fully equipped to manage the risks in a holistic and coordinated manner, including those arising from external uncertainties.

Vulnerability Risk Management is one of the important aspect which organizations are always working to mature. It is one of those areas which is considered a challenge and at the same time a priority for the board. With such vulnerability overload in today's date, it is essential to understand that Vulnerability Risk Management goes beyond identifying the vulnerabilities – to also understanding the threats and risks from a business contextualization stance, and prioritizing the remediation based on the normalized threat to an organization.

> " The number of exploited vulnerabilities year over year for the last decade is actually flat, despite the number of breaches increasing and the number of threats appearing. Essentially, more security threats are leveraging the same small set of vulnerabilities."
>
> Gartner
>
> **"Focus on the Biggest Security Threats, Not the Most Publicized"**

In this paper, we discuss the ingredients to develop a Robust Vulnerability Risk Management program which also includes, opportunities for you to:

- Increase efficiency/effectiveness (e.g., improve processes, automate processes)
- Improve operational capabilities (e.g., enrich data/correlate data across tools to enable better risk response and decision making)
- Expand capabilities (e.g., add high-value operational processes to prioritize vulnerability assessment and remediation efforts)
- Refine the governance structure, end-to-end management processes, required capabilities, and architecture to organize and mature its Vulnerability Management (VM) Program and develop a roadmap for continual improvement toward a mature future state Vulnerability Risk Management program.

Key criteria to get it right

To achieve a robust vulnerability risk management program, organizations need to shift their focus from managing overload of vulnerabilities across varied sources, to managing risks pertaining to unique vulnerabilities. Organizations, thus, need to emphasize security tools and processes which could help them identify, detect, correlate, normalize and remediate security events.

We have defined the following key criteria to enable organizations to build a robust Vulnerability Risk Management program:

Know your Business and Risk Appetite

Know your Assets

Current Risk Posture

Vulnerability Management Lifecycle

Know your business and risk appetite

For any organization and its stakeholders - the mission-critical step before thinking of a vulnerability risk management program is to have a clear understanding of the business profile and associated risk appetite for the organization. Have a clear grasp on the business processes helps the organization to develop and understand the information and infrastructure these business processes depend on.

As vulnerabilities are associated primarily with the assets, either infrastructure or application services that support the business, having this business context helps to define the criticality of these assets – for instance, the applications which host mission-critical processes. This also assists in understanding the overall risk to the organization.

Once the business processes and risk appetite has been implicitly agreed upon, the most optimal way to utilize this into the Vulnerability Risk Management Program is via Threat Modelling. This helps organizations to get clarity on actual threats, risks, and impacts posed to the organization.

The following metrics can be used for conducting threat modeling and to identify the security risk to an asset:

- Exposure of the assets across public/private/internal business trust zones
- The Potential of an adversary to target systems and crown jewels
- Data types (PII/Regulatory etc.) related to the assets and their sensitivity to the business
- Controls in place to protect the asset (from a Confidentiality, Integrity, and Availability standpoint)
- Susceptibility of identified vulnerabilities to the assets value to adversaries
- Potential time to compromise as per controls in place to the ease of technique, tools, & resources available

Know your assets

Along with having meaningful insights into the business processes, the other vital attribute to emphasize is to have a grip on what the organization needs to protect. The process of manually and automatically discovering, tracking, and centrally managing hardware, software, or cloud based information technology (IT) assets and relevant attributes (e.g. risk attributes, configuration attributes, etc.) with the organization comes as a part of Asset Management.

It is crucial for an organization to have adaptive asset management requirements and processes, to implement automated discovery capabilities, and determine opportunities for automated reconciliation of inventory data.

For organizations of all sizes, asset management is a challenging task. Thus to simplify the process, the following points would help:

- Implement broad, automated asset discovery capabilities which provide the ability to automatically detect all IT assets including hardware, software, middleware, and virtual or cloud assets, and relationships between assets accordingly.
- In addition to basic asset attributes, the processes should be capable of collecting and maintaining key attributes (e.g. business owner, operating system and application remediation owners, host location, application and platform criticality, etc.) required to practice risk-based vulnerability management.
- Integrate the centralized asset inventory with other existing business processes (e.g. change management, procurement, decommissioning, etc.) to require stakeholders to review and update inventory data
- Maintain date of last update/review to facilitate automatic/manual reconciliation of items not updated in the last 12 months.
- Integrate centralized asset inventory with a centralized Risk Vulnerability Management platform to improve reconciliation, tracking, and prioritization of assets and vulnerabilities

Current risk posture

Understanding the risk posture of an organization's assets is imperative for understanding the organization's risk posture.

Risk classification and criteria for IT assets with processes and procedures for rating platforms and applications should be defined and tailored for the organization. This would also influence the phases of the vulnerability management lifecycle

The following recommendations would facilitate risk management for an organization:

- Define and document a risk classification and scoring system or criteria for all assets, assigning risk ratings based on key attributes (e.g. data classification, business criticality, level of isolation, etc.).

- Develop processes and procedures that describe proper use and application of the risk classification criteria and initiate communication and training plan for employees.

- Assess, at a minimum, all assets including in the cloud, to assign business criticality and the other attributes required to generate risk scores

- All critical assets should be flagged in the centralized asset inventory as critical (i.e. Crown Jewels).

- Establish processes and procedures to identify, review, update, and communicate organizational risks, threats, and attackers; and risk classification criteria.

- Define and develop, standards, processes, and procedures for prioritizing vulnerabilities based on vulnerability severity and available risk data.

Vulnerability Management Lifecycle

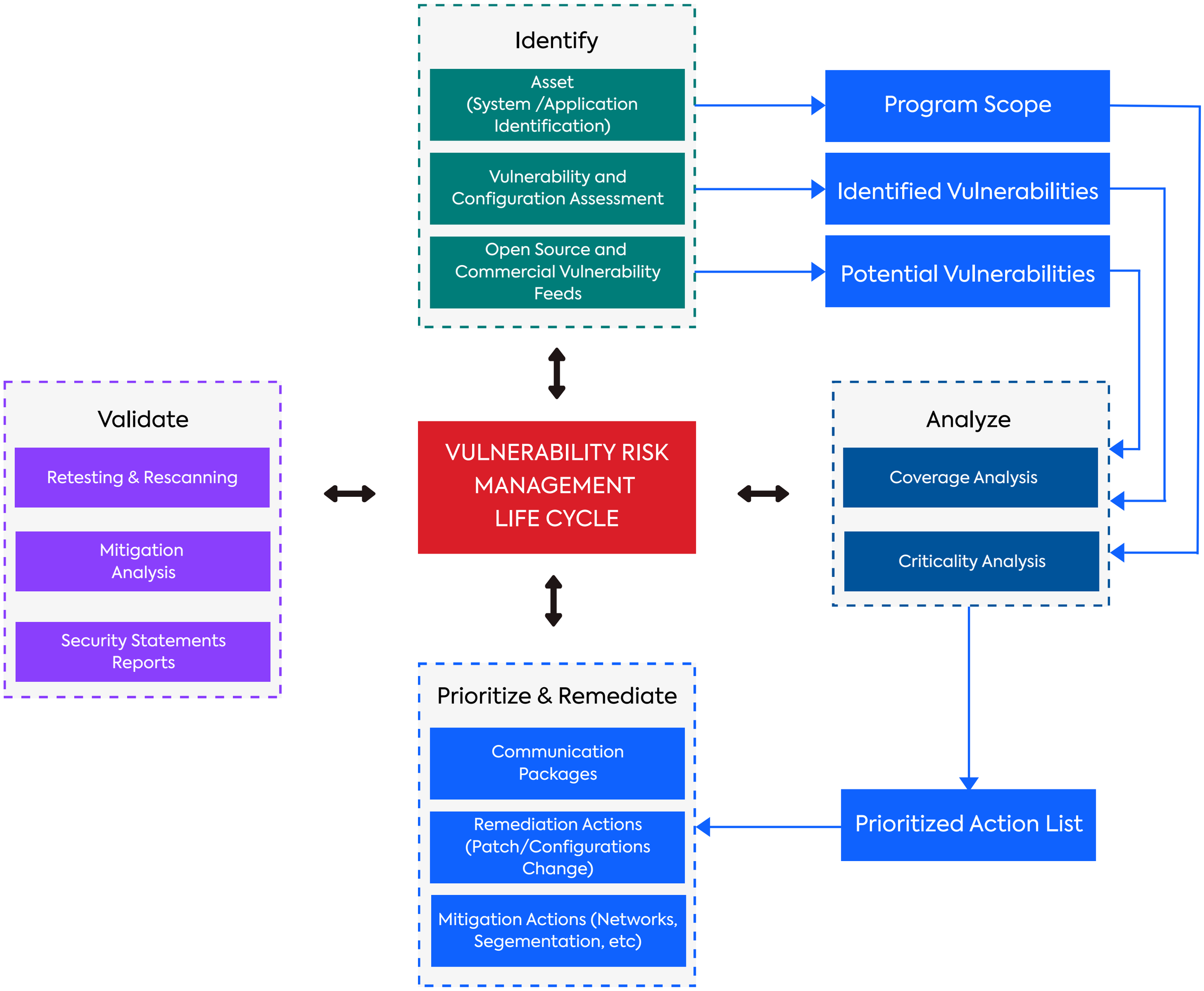
Vulnerability Management Lifecycle can be considered as a set of logical dissection of a Vulnerability Management Program which allows leadership, operators, and analysts (and other stakeholders) to focus on manageable processes versus focusing on the entire, complex program. The program lifecycle can be divided into four phases; Identify, Analyze, Prioritize and Remediate, and Validate, which are illustrated in the lifecycle diagram.

Identify – Identify assets, onboard into centralized asset inventory platform or vulnerability risk management platform, identify vulnerabilities from various sources (3rd party threat solutions, internal threat intelligence, and sources), ensure registration on appropriate systems, reconcile exceptions and execute assessments to identify weakness and vulnerabilities in those assets.

Analyze – Perform Data enrichment, correlation, normalize & prioritize assessment results, populate reporting and dashboards, assign business severity, and create remediation packages.

Prioritize and Remediate – Distribute remediation packages, file for exceptions as needed, perform configuration changes, and distribute patches out to systems.

Validate – Perform Data Enrichment on re-scan results, report creation, validate report accuracy, generate reports, distribute reports, assess risk tolerance, accept or mitigate risk.



An effective VM lifecycle will exhibit the following characteristics, which would enable a comprehensive Vulnerability Risk Management:

- Provides an improved security posture through cross-functional adoption of a continuous lifecycle to address configuration/setting deficiencies and remediate identified vulnerabilities
- Implements uniform reporting, translation, and distribution of the risk represented by the identified vulnerabilities and configuration deficiencies
- Reduces the risk and potential damages to technical assets
- Minimizes the number (striving for zero) of orphaned assets and systems which are out of compliance
- Reduces the risk of breaches and their associated cost
- Reduces audit time and its associated cost
- Has appropriate and timely monitoring, management, and reporting of asset security deficiencies
- Provides a streamlined execution of the individual processes comprising the overall Vulnerability Management program (i.e., Vulnerability Management, Patch Management, Configuration Management).

To achieve a robust Vulnerability Risk Management program, the vulnerability management lifecycle needs to mature via a process or a platform to aggregate and normalize the vulnerabilities across multiple sources, prioritize the vulnerabilities based on the risk identified as per the business contextualization (classified as per the threat intel, vulnerability context and risk for the asset and the organization) and provide sufficient privilege to increase the operational time from the vulnerability management.

Role of governance

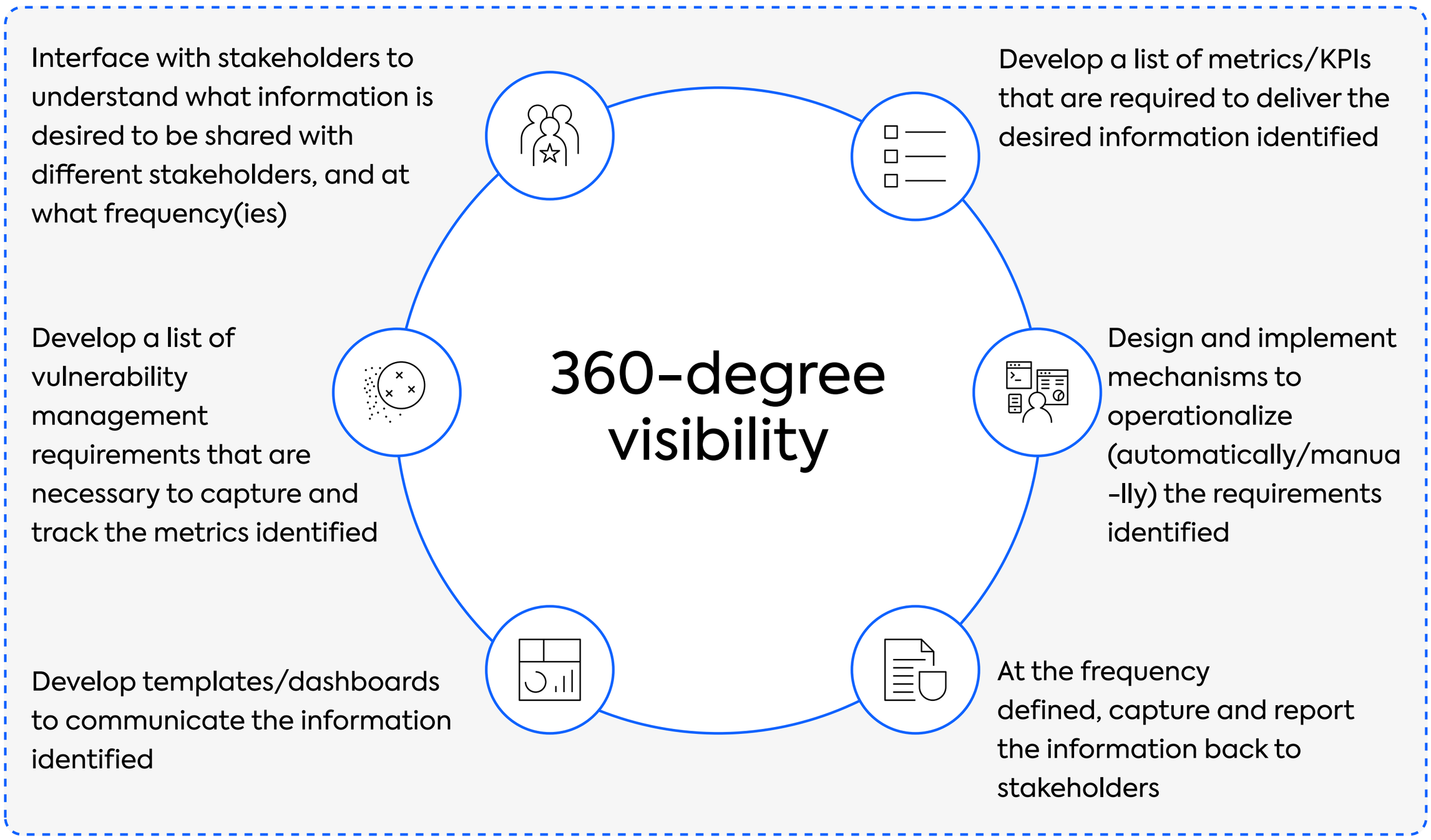
Governance is one of the biggest factors ensuring the success of a Vulnerability Risk Management program. The governance models the key goals of the program, in place processes, KPIs and metrics, roles and responsibility of personnel involved, risks and external dependencies of the program. Governances provide administrative guidance for the ongoing vulnerability management program.

To achieve a robust Vulnerability Risk Management program, governance must ensure getting 360-degrees visibility, KPIs to measure the success of the program, and report/associated metrics for the program.

Getting 360-degree visibility

Organizations can get 360-degree visibility via ensuring consistent tracking and monitoring via a process or platform, with custom reports based on the information garnered through the scans, and key metrics / KPIs that may be used to such as scan completion timeframe, number of findings per scan, response times for requests, etc.

Organizations should at a minimum ensure, the following governance related characteristics are tailored to the organization:



KPIs for robust Vulnerability Risk Management

KPIs are crucial for the success of vulnerability management governance. We have listed some of the key KPIs organizations should consider implementing:

- Percentage of critical systems scanned per quarter
- Number of unique vulnerabilities enumerated (post normalization and correlation across multiple sources)
- Percentage of systems with no known severe vulnerabilities
- Percentage of detected vulnerabilities associated with accepted risks or non-technical controls
- Percentage of vulnerabilities associated with known patch fixes
- Monthly counts of vulnerabilities discovered (by type, by platform and by operations/business)
- Percentage of systems introduced with known patches, fixes, or configuration deficiencies
- Number of changes tickets created per month
- Number of orphan vulnerabilities (by type, by platform and by operations/business)
- Mean time between vulnerability identification and remediation
- Percentage of assets/resources as per the risk scores (per business contextualization)
- Mean time between review/revision of vulnerability scanning and validation/remediation
- Number of assets detected
- Number of Critical, High, Medium and Low -risk assets detected
- Number of failed tests (as per the integration across multiple sources)
- Current risk/maturity level across assessment domains (Organization Risk Score)
- Target risk/maturity level across assessment domains
- Initiative roadmap cost and timeline

Report and metrics

With vulnerability overload from multiple sources – redundant reports across multiple automated vulnerability management solutions, manual assessments, and inconsistent reports pose a great challenge to organizations.

At any point in time, management should be able to consume:

An **executive management** summary with key unique vulnerabilities across the organization would reflect the organization's risk score and overall status quo of the risks associated with vulnerabilities/recommendations (presented in a high level improvement plan). As required, integration with the above-discussed KPIs and metrics relevant for the business, would be very valuable.

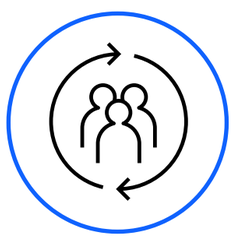
Detailed technical observations grouped by risks, including a summary of the security vulnerabilities, systems / accounts applicable, an explanation on how to exploit, including screenshots to allow replay, description of the risk (likelihood and impact), and detailed recommendation for remediating or mitigating the identified vulnerabilities.

Roles and responsibilities

While the security team often takes the responsibility for vulnerability management, it must be a team effort to be successful. As security stakeholders may not be in a position to apply patches, fix code, or update systems, cooperation from the organization's IT operations and associated business units are vital for the success of the vulnerability management program.

Risk management, thus, should be incorporated into operations across the organization. On a high level, it can be classified as follows:

Security Teams can measure the threat to the asset as per the identified vulnerability, the potential risk and understand how best to reduce it. Security teams come to be more effective at strengthening an organization against identified threats and at-risk vulnerabilities.



Executive Teams enabled via governance, should have a clear understanding of an organization's security posture, including the changing dynamics, as well as the efforts and investments needed for continued improvement.

Remediation Teams across the business operations can continue to work with existing tools, processes and platforms while gaining increased visibility into the risks facing the business. With a risk- based approach, remediation teams can focus their efforts on the most strategically impactful actions say. In addition, remediation teams can make more effective use of their time, as they no longer have to shift through giant reports or hunt down fixes, if the security team follows a robust vulnerability risk management program.

CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

DSCI PROMOTING DATA PROTECTION
A NASSCOM® Initiative

WeSecureApp

How strobes helps organizations get it right

Strobes is a **risk-centered vulnerability management platform** that enables you to integrate with various cybersecurity tools to power up and streamline your vulnerability management process. This is to help your organization in aggregating and de-duplicating vulnerabilities.

Using machine learning and threat intelligence, the platform will associate real-world risk to the organization and prioritize the vulnerabilities based on various business and technical metrics so that you're closing the right vulnerabilities at the right time. With this auto prioritization of vulnerabilities, Strobes offers security managers a mechanism to proactively manage and mitigate cyber risk operations.

Key Benefits of Strobes:

- Focus on fixing the right vulnerabilities that matter the most.
- Streamline your vulnerability management lifecycle by bringing all the security stakeholders under one single roof.
- Drastic improvement in IT efficiency by vulnerability aggregation, de-duplication, and prioritization.
- Gain visibility into the organization's security posture.
- Make better decisions and estimate the value addition of your security scanners.
- Integration with 40+ security and IT tools.
- Monitor your organization's security health index over a time period.

CYBERSECURITY CENTRE of EXCELLENCE

A joint initiative of DSCI & Government of Telangana

DSCI PROMOTING DATA PROTECTION

A NASSCOM® Initiative

WeSecureApp

About Cybersecurity Center of Excellence

The Cybersecurity Center of Excellence (CoE) is a joint initiative of the Government of Telangana and Data Security Council of India (DSCI) to accelerate the cybersecurity momentum and create a conducive cybersecurity ecosystem that nurtures innovation, entrepreneurship and capability building. CoE works with all industry organisations, government agencies, academia and R&D centers and user groups and collaborates with other industry bodies, incubators and accelerators to accomplish its mission. DSCI is a not-for-profit, industry body on data protection in India, set up by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI is the apex industry body for Cybersecurity in India.

https:/ccoe.dsci.in ccoe.hyd CCoE_Hyd cybersecurity-ceo-telengana dscivideo

About WeSecureApp

WeSecureApp is a new age cybersecurity company, pivoted on advanced technology innovations to solve critical issues in the application, network, and cloud security space. Through an AI-powered platform called Strobes, WeSecureApp is also helping organizations in the Vulnerability Management domain and manage Security Engagements. A highly skilled team operates round-the-clock cohesively to monitor, prevent, detect, analyze and respond to cybersecurity incidents. With a comprehensive approach and a spectrum of offensive and defensive security offerings, WeSecureApp has been protecting over 150 companies globally every year.

wesecureapp.com wesecureapp.wsa wesecureapp we-secure-app wesecureapp

CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity Centre of Excellence, (DSCI)

C/o CtrlS data Centers, No 16, Software Units Layout,

Madhapur (Hitech-City), Hyderabad – 500081,

Telangana, India

FOR ANY QUERIES:

P: +917989467107

E: marketing.ccoe@dsci.in

WESECUREAPP

Rent-A-Desk, 5th Floor, Babukhan Rasheed Plaza,

Aditya Enclave, Venkatagiri, Jubilee Hills,

Hyderabad,Telangana – 500033

FOR ANY QUERIES:

P: (+91) 855 594 1404

E: security@wesecureapp.com

strobes

Take your vulnerability management to new heights

CYBERSECURITY CENTRE *of* EXCELLENCE

A joint initiative of DSCI & Government of Telangana

FOR ANY QUERIES:

P: +917989467107

E: marketing.ccoe@dsci.in

W: https:/ccoe.dscii.in