NOPSEC

Vulnerability Risk Management Program Playbook

Creating a Vulnerability and Risk Management Program

Cyber risk grows exponentially every day – and the number of vulnerabilities in your organization's environment continue to multiply with it. Organizations must take effective countermeasures to avoid becoming another headline. This takes a deliberate, carefully considered strategy.

Organizations need a well-structured Vulnerability and Risk Management (VRM) Program.

Building a VRM Program can be a daunting task. With your team already stretched thin with too many demands and too little time, getting the foundation in place for a successful VRM Program is no easy feat.

This playbook delivers the framework and knowledge to build your own VRM Program. From the projects needed to get started, to the stakeholders whose buy-in you need, and templates to guide, everything you need is in one place.

Grow your Vulnerability Management maturity as an organization with a strong VRM Program foundation.

Where Do You Fall on the Vulnerability Management Maturity Matrix?

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
NON-EXISTENT	SCANNING	ASSESSMENT & COMPLIANCE	ANALYSIS & PRIORITIZATION	ATTACK MANAGEMENT	BUSINESS-RISK MANAGEMENT
No vulnerability scanning	Vulnerability assessment solution in place	Driven by regulatory framework	Risk-focused	Attacker and threat focused	Threat and risk aligned with business goals
Manual vulnerability assessments	Ad hoc vulnerability scanning	Scheduled vulnerability scanning	Scan data prioritized through analytics	Multiple threat-vectors tested and prioritized	All threat-vectors tested and prioritized
Haphazard patching	Rudimentary patching	Scan to patch lifecycle	Patching data-driven by priority	Patching based on risk to critical assets	Continuous scanning and patching
No processes exist	Basic processes	Emerging processes	Repeatable processes	Processes measured against SLAs	Unified business and IT processes
No metrics	Basic metrics	Little measurability, busy metrics	Emerging metrics and trends	Emerging metrics and trends	Measurement integrated to enterprise risk mgmt

Blissful Ignorance

Awareness & Early Maturity

Business Risk & Context

PEAK DATA OVERLOAD

EFFECTIVE PRIORITIZATION

Drive Vulnerability Management Maturity

Drive growth in your cybersecurity strategy maturity with a unified VRM strategy. This playbook outlines the projects, tools, and stakeholders you need on board for a successful VRM Program.
Start with your VRM Program Plan.

VRM Program Plan

Phase 1
Program Governance

Governance Framework

Scope

- **Program Health Assessment**

Health assessment to identify gaps

- **Cross Functional Governance Committee**

Key technical and non-technical stakeholders

- **Program Charter**

Define charter, mission statement, program goals

- **Policies and Procedures**

Develop or enhance existing policies and procedures

Phase 2
Asset Priority

Know What We Own

Scope

- **Infrastructure and Web Application Inventory**

By location, OS, app, library, owner, type of sensitive data

- **Prioritization of Assets**

By crown jewels, business critical, normal systems/apps, threat intelligence

Process

Phase 3
Training

Level Up Our People

Scope:

- **Program Training**

VRM and AppSec program management training and leadership briefing on threat landscape and best practices

- **Technical Training**

VRM tooling training to optimize full utilization of core features

People

Phase 4
Operationalize

Optimize Tooling

Scope:

- **Routine Scanning & Prioritization**

Infrastructure and apps

- **Security Control Validation on Crown Jewel Systems**

Infrastructure and apps

- **Integration with CMDB**

A full view into your asset inventory

- **Remediation Mgt**

Systematically track issues, remediation status & orchestration

- **Risk Mitigation Strategy**

Develop risk acceptance and risk reduction strategy and enable compensating controls

Technology & Services

Phase 5
Metrics Reporting

Report What Matters

Scope:

- **Program Success Criteria**

- **Key Metrics and Scorecards**

Business aligned metrics, operational metrics (volume, efficiency), benchmarking, program health

- **Project Roadshow**

"**Success Story**" with key stakeholders

Reporting

Begin with Your VRM Program Governance Project

Build the foundation for Vulnerability and Patching Management program with a proper VM program governance framework, policy, procedures, and operational KPIs. Use these guides to kick-off your VRM Program Governance Project.

VRM Program Governance Project

Get all your stakeholders on the same page with a VRM Program Governance Project. This ensures that everyone is aligned on expectations and processes as you build and roll out your VRM Program.

Project Scope

- Understand existing processes in place
- Develop foundational framework for VRM Program
- Prepare baseline VRM Program documentation
- Formalize VRM Program Charter to operationalize the program

Project Deliverables

- Develop VRM Program Governance framework
- Baseline VRM processes
- Document policies and procedures
- Provide knowledge transfer
- Design Program Charter, metrics, KPIs/SLAs for program monitoring and oversight

VRM Program Governance Project

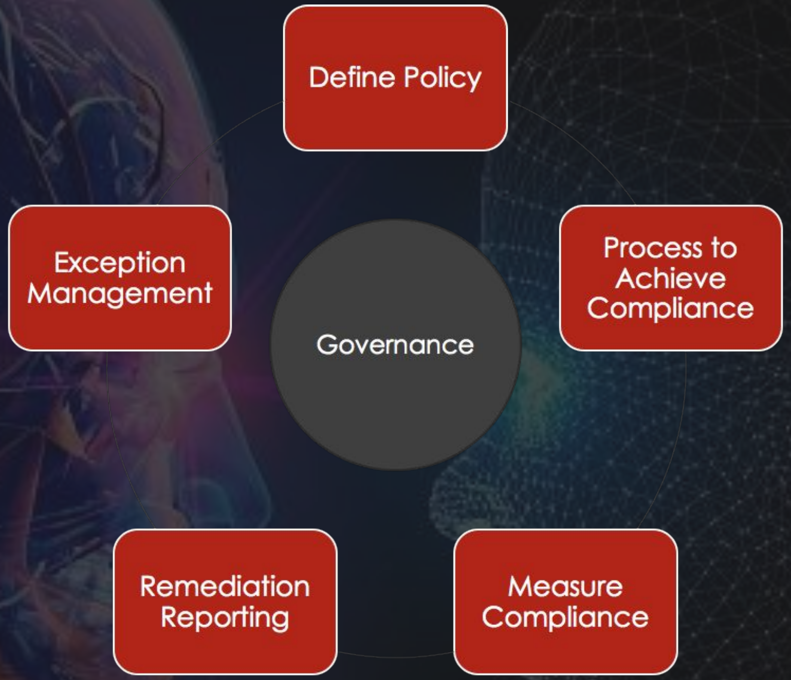
Cross Functional Leadership

- CISO
- Senior IT Leaders (infrastructure, applications & security)
- Risk partners (lines of defense)
- Program leaders
- PMO
- Execution team

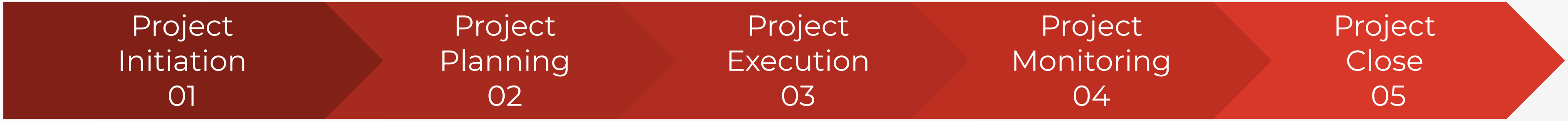
Monthly cadence to engage and communicate

Topics to Address

- Escalations & risk mitigation efforts
- Metrics trending red or yellow
- Prioritization of work efforts
- Remediation progress
- Proactive focus topics
- Resource planning



VRM Governance Project Plan



Project Initiation 01

Project Planning 02

Project Execution 03

Project Monitoring 04

Project Close 05

Milestone:
- Project Initiation

Deliverable:
- Project Charter

Milestone:
- Project scope
- Work Schedule
- Identify key stakeholders

Deliverable:
- Interview schedule

Milestone:
- Interview key stakeholders to understand existing processes

Deliverable:
- Program Charter
- Policies & procedures
- Process flows
- RACI chart

Milestone:
- Key stakeholder feedback on deliverable
- Internal peer review

Deliverable:
- Team workshop
- Management briefing

Milestone:
- Post Mortem
- Key stakeholders feedback on project

Deliverable:
- Management briefing
- Final deliverable and reporting

Gather Your Stakeholders

Get the right people in the room. These are the roles and teams that are crucial to creating a successful VRM Program.

Key Stakeholders - Cyber Teams

Global Security Programs

- Global Regional Information Security Officers

Security Strategy & GRC

- Policy, Procedure, & Compliance
- Data Protection
- Security & Awareness
- Metrics, Automation, Dashboarding, & Reporting
- Office of the CISO

Cyber Fusion Center

- eDiscover & Forensics
- Threat Intel and Hunting
- Threat Detections & Monitoring
- Attack Surface
- Incident Response
- Vulnerability Management

Product Security

- Secure Development
- Research & Innovation
- Connected Product Security Lifecycle Framework

Security Architecture & Engineering

- Tool Management
- Security Architecture
- Identity and Access Management
- Cloud Security
- Application Security
- Public Key Infrastructure

Key Stakeholders

Outside of Cyber Teams

- Infrastructure
- Asset Management - CMDB
- Endpoint/Desktop/PC
- Cloud/Hosting
- Active Directory
- Application Support
- Metrics Team

Plan Your VRM Lifecycle Management

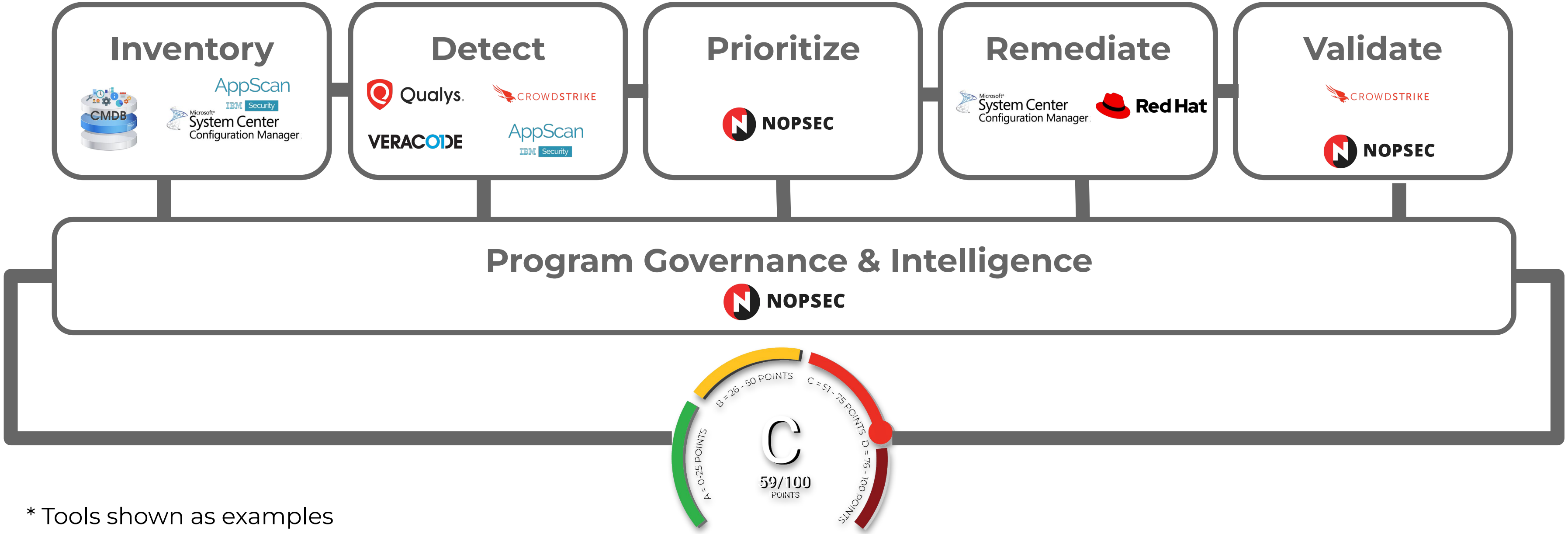
Here are the segments and toolsets to consider when planning your continuous VRM lifecycle management processes.

VRM Lifecycle Management

Capability	Description
Inventory	Develop complete inventory of systems, assets, data, and applications.
Detect	Develop and implement appropriate detection capabilities to provide proper scan coverage and cadence
Prioritize	Develop and implement the appropriate activities to prioritize risk based on threat, asset, vulnerability, exploitability and control contexts
Remediate	Develop and implement the appropriate activities to take action regarding prioritized vulnerabilities and threat vectors.
Validate	Develop and implement the appropriate activities to maintain plans for resilience and to validate the efficacy and effectiveness of remedial actions.

Operationalize VRM Program Lifecycle Mgt

Centralize the Risk Quantification, Prioritization, Remediation and Management of your VRM Program.



Inventory

Detect

Prioritize

Remediate

Validate

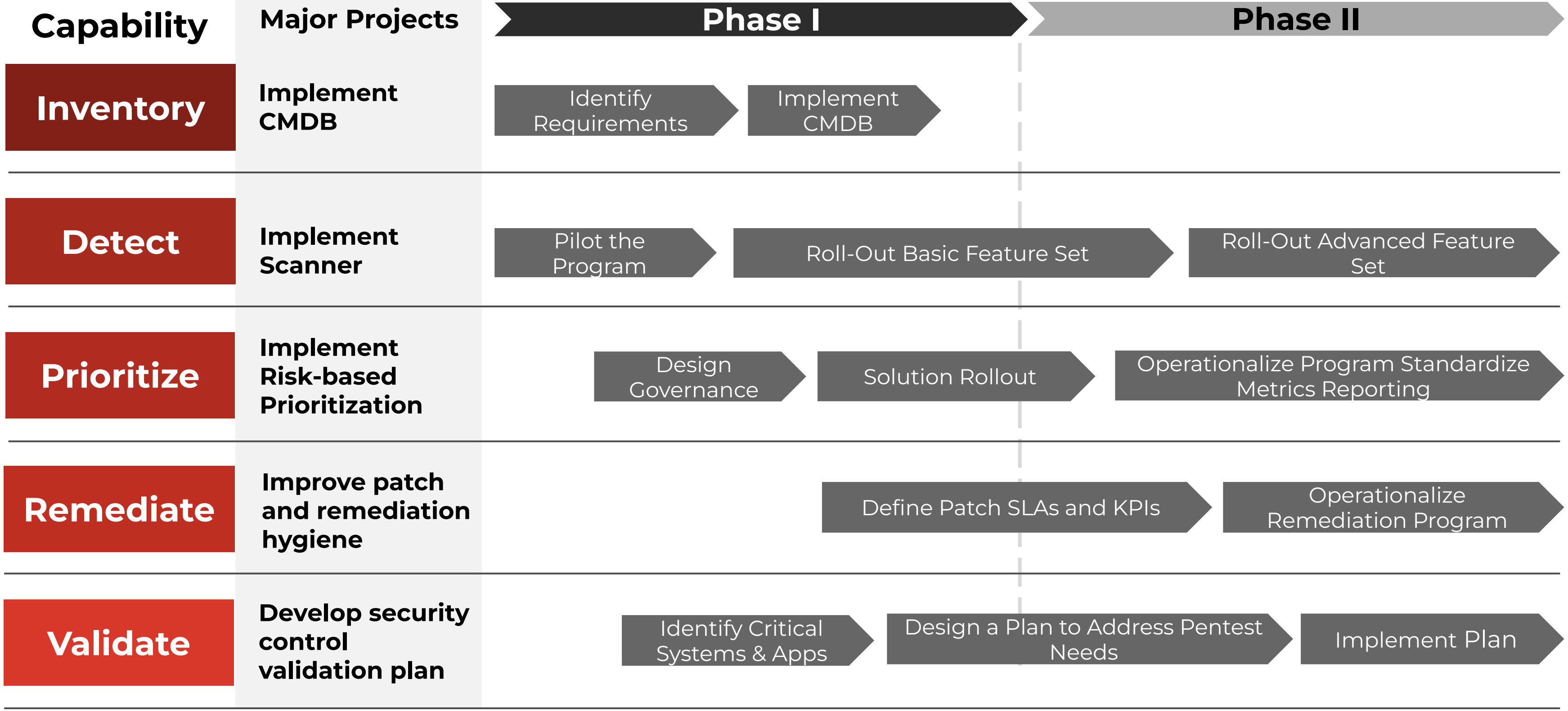
Program Governance & Intelligence

* Tools shown as examples

Follow the Roadmap to Success

Discover next steps and additional resources to help you reach your VRM program goals.

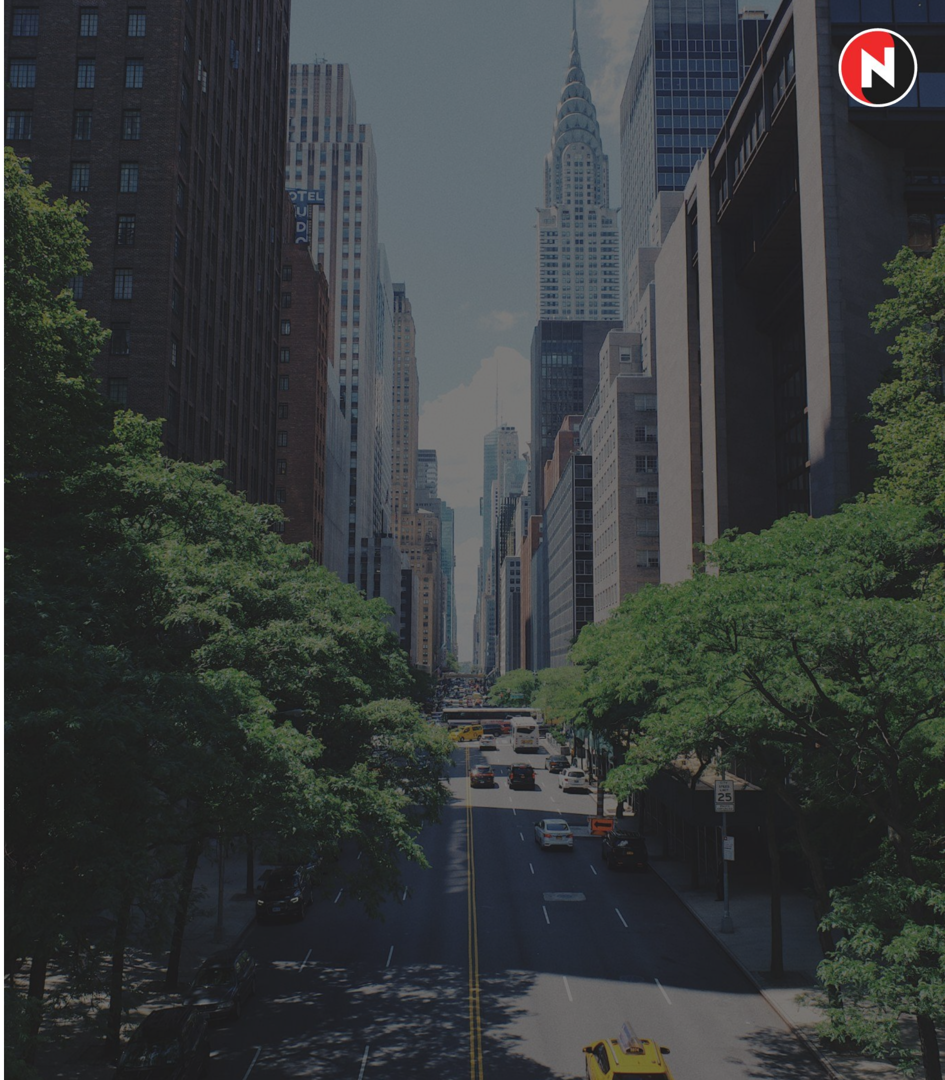
Roadmap to Success



Capability	Major Projects	Phase I	Phase II
Inventory	Implement CMDB	Identify Requirements Implement CMDB	
Detect	Implement Scanner	Pilot the Program Roll-Out Basic Feature Set	Roll-Out Advanced Feature Set
Prioritize	Implement Risk-based Prioritization	Design Governance Solution Rollout	Operationalize Program Standardize Metrics Reporting
Remediate	Improve patch and remediation hygiene	Define Patch SLAs and KPIs	Operationalize Remediation Program
Validate	Develop security control validation plan	Identify Critical Systems & Apps	Design a Plan to Address Pentest Needs Implement Plan

Resources

1. VRM Program Charter Template
2. VRM Program Governance Project Charter Template
3. Vulnerability and Patch Management Policies Template
4. Vulnerability and Patch Management Procedures Template
5. Vulnerability and Patch Management Inventory and Asset Management Workflow
6. Vulnerability and Patch Management Validation Metrics and Reporting Workflow



Let's shape the future work in cyber.

Schedule a demo.

✉ sales@nopsec.com

☎ +1 (646) 502-7900

🌐 www.nopsec.com