

# VM Program Kit

Everything you need to stand up a defensible, risk-based vulnerability management program  
— built by a practitioner, ready to adapt. Rank by real exploitability, not raw CVSS.

## What's inside

- 1 **FlintScope-VM-Program-Overview.pptx — the orientation.** The whole program on eleven editable slides with speaker notes. Rebrand it and present it to your own leadership.
- 2 **FlintScope-VM-Policy.docx** — the governing policy & standard: scope, roles (RACI), asset tiering, the prioritization method, the severity & SLA matrix, exceptions, governance.
- 3 **FlintScope-Prioritization-Model.xlsx — the engine.** Paste a scanner export, map its columns once; it scores each finding on exploitability, criticality, and exposure, assigns priority and SLA, tracks opened and closed dates, and runs the Dashboard tab: MTTR, SLA attainment, backlog, aging, open KEV exposure. Tunable; wired for 2,000 findings.
- 4 **FlintScope-Triage-Remediation-Runbook.docx** — the operating procedure: intake → triage → prioritize → route → remediate → verify → close, with escalation paths and a worked example.
- 5 **FlintScope-Exception-Register.xlsx** — the governed risk-acceptance register the policy requires: approver set by priority, an expiry that flips to an SLA breach, live counts of what's open.
- 6 **FlintScope-Scanner-Onboarding-Notes.docx** — bringing any scanner into the program: the fields the model needs, authenticated coverage, tuning, with notes for Tenable, Qualys, Rapid7, Wiz, and Snyk.
- 7 **FlintScope-Executive-Reporting-Template.docx** — the one-page leadership summary that answers "are we exposed, and is it improving?"
- 8 **FlintScope-Framework-Crosswalk.xlsx** — every program element mapped to NIST CSF 2.0, PCI DSS v4, ISO 27001:2022, and SOC 2, with the evidence each produces. For audits and questionnaires.
- 9 **FlintScope-VM-Maturity-Model.docx** — six dimensions × five levels, scored the same way as the free assessment, plus what to fix first at each level and the 90-day roadmap.

## Suggested order

Read the **Overview** first; it doubles as your stakeholder kickoff deck. Adopt the **Policy**, wire up the **Prioritization Model**, and operationalize with the **Runbook** and the **Exception Register**. Onboard your scanner with the **Scanner Notes**, then stand up measurement with the Model's **Dashboard** tab and the **Executive Template**. Reach for the **Crosswalk** when an auditor shows up, and the **Maturity Model** every six months.

## Customize before you deploy

- Replace every bracketed field — **[Company]**, **[CISO]**, **[dates]** — with your specifics.
- Map the RACI roles to your real titles.
- Confirm your asset criticality tiers (Tier 0–3).
- Ratify the SLA thresholds against your risk appetite — set once on the Model tab; the policy quotes them.
- Replace the sample findings, assets, and feed rows in the Model with your own.

## Pairs with

The free **VM Maturity Self-Assessment** at flintscope.com — share it to show where a program stands today, then this kit closes the gaps it surfaces.

## Who built this

**Nick Strupp, CISSP** — 15+ years in security. Built and scaled an AppSec/vulnerability-management program from 12 to 60 people across more than 5,000 applications; US Patent 11,106,801 in vulnerability-triage orchestration. This kit is that program, generalized so you can adopt it without re-learning its lessons the slow way.