RISK APPETITE & TOLERANCE DEFINITIONS

Vulnerability Management Maturity Model (VMMM v2)

Domain: Prepare
Maturity Tier: Foundational

EXECUTIVE SNAPSHOT (30-60 seconds)

Why this matters:

- Teams lack criteria for when vulnerability exposure crosses from tolerable to intolerable risk

What breaks without it:

- Risk decisions made arbitrarily without organizational boundaries or acceptance criteria
- Similar vulnerabilities handled inconsistently based on politics or individual judgment

What "good" looks like:

- Level 3: Documented risk appetite with specific tolerance thresholds and acceptance criteria
- Level 4+: Embedded in tools with automated enforcement and periodic refinement

Who should care:

- Security leadership translating board risk appetite into operational VM thresholds
- Risk management teams establishing quantifiable vulnerability risk tolerances
- Technical teams understanding acceptable vs. unacceptable risk requiring action

URGENCY ASSESSMENT

(If unchecked at Level 2+, risk decisions are likely indefensible)

☑ Critical Foundation (enables risk-based decision framework)
☑ Compliance Driver (frameworks require risk-based approach)
☑ Operational Efficiency (enables consistent, objective decisions)

FRAMEWORK ALIGNMENT EXAMPLES

NIST 800-53: Documents risk management strategy with vulnerability tolerance thresholds

NIST CSF 2.0: Demonstrates risk management with documented tolerance levels

CIS v8: Provides organizational risk framework for remediation prioritization

ISO 27001: Shows risk-based vulnerability management within documented tolerances

MATURITY QUICK CHECK

Where are you today?

○ Level 1: No documented risk appetite, patch by severity alone
○ Level 2: Informal understanding, email approvals, inconsistent
○ Level 3: **Documented appetite, specific thresholds, acceptance criteria**
○ Level 4: Embedded in tools, automated enforcement, periodic review
○ Level 5: Continuous refinement, measured effectiveness

DEPENDENCIES & BOUNDARIES

Depends on: Program Governance, Risk-Based Prioritization, Context

Enables: Compensating Controls, Risk Acceptance decisions

This is NOT: A risk scoring formula, guarantee of zero risk

Related Resources: Risk Appetite & Tolerance Definitions Guide · Framework Mapping · Self-Assessment