ZERO-DAY READINESS

Vulnerability Management Maturity Model (VMMM v2)

Domain: Prepare
Maturity Tier: Foundational

EXECUTIVE SNAPSHOT

Why this matters:

- Organizations have no formal process to respond to high-impact zero-day vulnerabilities

What breaks without it:

- Teams react inconsistently during zero-day crisis. No coordination. Unclear who decides emergency actions
- Ad hoc response depends on individual effort. Not repeatable. Ownership unclear during high-pressure events

What "good" looks like:

- Level 3: Defined response process, communication channels, designated leads, documented response steps
- Level 4+: Playbooks, crisis simulations, measured timelines, cross-functional crisis response framework

Who should care:

- Security teams responding to critical zero-day vulnerabilities requiring rapid coordinated action
- Incident response teams coordinating emergency patching and crisis response workflows
- IT leadership managing organizational response during high-pressure zero-day events

URGENCY ASSESSMENT

☑ Critical Foundation (prevents chaotic crisis response)

☐ Compliance Driver

☑ Risk Mitigation (reduces exposure window during zero-day events)

☑ Operational Efficiency (enables rapid coordinated response)

☐ Strategic Enhancement

(If unchecked at Level 2+, organization responds to zero-days chaotically without coordination)

FRAMEWORK ALIGNMENT EXAMPLES

This capability supports accountability requirements in commonly adopted security frameworks. These examples illustrate alignment, not exhaustive control coverage.

NIST 800-53: Demonstrates incident response with documented zero-day response procedures

NIST CSF 2.0: Shows incident response planning with crisis management capabilities

CIS v8: Provides incident response management with zero-day response workflows

ISO 27001: Demonstrates incident response with emergency procedures for critical events

MATURITY QUICK CHECK

○ Level 1: No formal zero-day process, inconsistent reaction, limited coordination

○ Level 2: Ad hoc procedures, depends on individual effort, not repeatable, unclear ownership

○ Level 3: **Defined response process, communication channels, designated leads, documented steps**

○ Level 4: Playbooks, pre-established workflows, regular crisis simulations, measured timelines

○ Level 5: Cross-functional crisis framework, real-time data, automated workflows, performance tracking

DEPENDENCIES & BOUNDARIES

Depends on: Incident Response Integration, Roles & Responsibilities, Crisis Communications

Enables: Coordinated crisis response, rapid decision-making, reduced exposure window

This is NOT: General incident response, guarantee of zero downtime during zero-days

Related Resources: Zero-Day Readiness Guide · Framework Mapping · Self-Assessment