CRISIS COMMUNICATIONS READINESS

Vulnerability Management Maturity Model (VMMM v2)

Domain: Respond
Maturity Tier: Foundational

EXECUTIVE SNAPSHOT

Why this matters:

- Organizations lack documented procedures for communicating about vulnerability-related incidents

What breaks without it:

- Crisis mode debates about what to tell stakeholders—hours wasted instead of communicating
- Different teams send contradicting messages—stakeholders confused, organization loses credibility

What "good" looks like:

- Level 3: Communication plan, stakeholder procedures, approval authorities, message templates
- Level 4+: Tabletop exercises, customized templates, post-incident reviews, measured effectiveness

Who should care:

- Incident response teams preparing stakeholder communication for vulnerability-related incidents
- Communications teams establishing crisis procedures ensuring consistent, accurate messaging
- Security leadership defining escalation criteria and approval authorities for disclosures

URGENCY ASSESSMENT

☑ Critical Foundation (prevents improvised crisis response)

☑ Compliance Driver (regulatory disclosure requirements)

☐ Risk Mitigation

☐ Operational Efficiency

☑ Strategic Enhancement (maintains stakeholder confidence)

(If unchecked at Level 2+, organization unprepared for regulatory disclosure and stakeholder notification)

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 handling with stakeholder notification procedures

NIST CSF 2.0: Shows response communications coordinating with stakeholders

CIS v8: Provides incident response plan with communication procedures

ISO 27001: Demonstrates incident response with documented stakeholder communication

MATURITY QUICK CHECK

○ Level 1: No communication plan, crisis mode debates, improvised response

○ Level 2: Informal understanding, ad hoc coordination, inconsistent messaging

○ Level 3: **Communication plan, stakeholder procedures, approval authorities, templates**

○ Level 4: Tabletop exercises, customized templates, post-incident analysis

○ Level 5: Stakeholder feedback, automated notifications, measured effectiveness

DEPENDENCIES & BOUNDARIES

Depends on: Program Governance, Roles & Responsibilities, Incident Response

Enables: Systematic stakeholder notification, regulatory compliance, reputation management

This is NOT: Technical incident response, legal opinion on disclosure requirements

Related Resources: Crisis Communications Readiness Guide · Framework Mapping · Self-Assessment