Crisis Communications Readiness

Capability Alignment Guide

Model: VMMM v2.0.0
Domain: Respond
Maturity Tier: Foundational

Purpose:

Crisis Communications Readiness ensures organizations are prepared to communicate effectively about vulnerability-related security incidents through documented communication plans, stakeholder notification procedures, message templates, and approval authorities enabling systematic disclosure rather than improvised crisis response.

This document is interpretive guidance. Normative definitions of the Crisis Communications Readiness capability and maturity levels are defined in the VMMM v2 Canon.

Executive Summary

Organizations operate vulnerability management without considering how to communicate about security incidents resulting from unpatched vulnerabilities. Critical vulnerability exploited in production affecting customer data. IT discovers breach Friday evening. Security contains incident over weekend. Monday morning: executive leadership asks "What do we tell customers?" No documented plan exists. Marketing says wait until investigation complete. Legal says notify immediately for regulatory compliance. Customer success says customers asking questions on social media. Executive team debates messaging in crisis mode creating inconsistent information shared with different groups.

Crisis Communications Readiness establishes procedures before crisis occurs. Communication plan documents: incident severity thresholds triggering external communication (Critical vulnerability exploited affecting customer data requires notification), stakeholder groups requiring notification (customers, partners, regulators, employees, media) with contact methods and timing, approval authorities for each stakeholder group (CISO approves customer notifications, legal approves regulatory filings, CEO approves media statements), message templates for common scenarios providing starting point for incident-specific customization.

Mature communication procedures operate strategically. Tabletop exercises test communication workflows identifying gaps before real crisis. Post-incident reviews analyze communication effectiveness improving templates and procedures. Stakeholder feedback incorporated into plan updates. Message templates customized for different audiences: customers receive actionable guidance, regulators receive compliance-focused details, media receives public-facing summary. Communication metrics measured: time to first notification, stakeholder satisfaction, regulatory compliance achievement.

This guide explains why crisis communication readiness matters, what communication maturity looks like, and how to use the detailed mapping document for compliance and organizational effectiveness.

This document is interpretive guidance. Normative definitions of the Crisis Communications Readiness capability and maturity levels are defined in the VMMM v2 Canon.

Why This Capability Exists

Friday 5 PM: IT security detects unusual database queries indicating possible breach. Investigation reveals Critical SQL injection vulnerability exploited over past 72 hours. Attacker extracted customer records including names, emails, payment information. Security team contains breach, patches vulnerability, begins forensic analysis. Monday 8 AM: Executive leadership convenes. CEO asks "What do we tell customers?" No documented communication plan exists. Marketing director says wait until investigation complete to avoid alarming customers prematurely. Legal counsel says notify immediately—regulatory requirements mandate disclosure within 72 hours, already approaching deadline. Customer success director says customers posting questions on social media based on service interruptions Friday evening. Finance worried about stock price impact. IT concerned premature disclosure compromises ongoing investigation.

Without crisis communications readiness, debate continues for hours. Legal drafts regulatory notification. Marketing drafts customer email. Messages differ significantly—legal focuses on compliance minimums, marketing emphasizes company response actions, neither coordinates with other. Security team tells board incident "minor" to avoid panic. Customer support tells affected customers investigation "ongoing" without providing timeline. Media publishes story Monday afternoon based on social media speculation because company provided no official statement. Regulatory body learns about breach from news article not company notification. Stock drops 15%. Customers angry about inconsistent information from different company representatives.

Customer notification finally sent Tuesday containing inadequate information triggering regulatory investigation into disclosure practices. Different executives give contradicting interviews: CEO says "customer data secure," CTO admits payment information accessed, CISO says forensics incomplete so impact unknown. Contradictions amplify negative coverage. Partners cancel contracts citing breach disclosure mishandling not breach itself. Board conducts internal review identifying lack of documented communication procedures as systematic gap enabling communication failures compounding technical incident.

Crisis Communications Readiness capability prevents these failures through documented procedures established before crisis. Communication plan defines incident severity thresholds: Critical vulnerability exploited affecting customer data triggers external notification, routine patching does not. Stakeholder groups documented with specific contact methods: customers via email with portal access for status updates, regulators via required filing systems within compliance timeframes, media via press releases and spokesperson coordination, employees via internal communications ensuring frontline staff informed before external disclosure.

Approval authorities explicitly defined: CISO approves customer notifications ensuring technical accuracy, legal counsel approves regulatory filings ensuring compliance, CEO approves media statements ensuring executive alignment, communications lead coordinates all external messaging ensuring consistency. Message templates provide starting point for incident-specific customization: customer template includes what happened, what data affected, what actions customers should take, how company responding; regulatory template includes discovery date, affected records count, remediation timeline, compliance contact information.

Communication roles assigned before crisis: incident commander coordinates overall response including communication timing, communications lead drafts messages using templates, legal reviewer ensures regulatory compliance, technical reviewer ensures accuracy, executive sponsor provides final approval. When breach occurs, team executes documented plan rather than improvising. Friday breach discovered, documented procedures followed: incident

commander activated Saturday, communications lead drafted notifications using templates Saturday evening, legal reviewed for compliance Sunday morning, executive sponsor approved Sunday afternoon, customer notification sent Monday 8 AM meeting 72-hour regulatory requirement with coordinated, accurate messaging.

Before and After Comparison

WITHOUT CRISIS COMMUNICATIONS READINESS:

- Breach Friday evening. Monday morning executive debate: what to tell customers? No documented plan. Hours wasted debating instead of communicating
- Different teams draft different messages. Legal focuses compliance, marketing emphasizes response. Messages contradict. Stakeholders confused
- Media publishes story from social media speculation. Company provided no official statement. Regulatory body learns from news not company. Stock drops
- Customer notification delayed, inadequate. Regulatory investigation triggered. Executive interviews contradict. Partners cancel citing communication mishandling

WITH CRISIS COMMUNICATIONS READINESS:

- Breach Friday evening. Documented procedures consulted Saturday. Incident commander activates communication plan. Team executes established workflow
- Communications lead drafts using templates Saturday evening. Legal reviews Sunday for compliance. Executive approves Sunday afternoon. Messages consistent, coordinated
- Customer notification sent Monday 8 AM meeting 72-hour requirement. Media receives official statement simultaneously. Regulatory filing submitted on time
- Stakeholders receive clear, accurate information from single coordinated source. Post-incident review improves templates. Confidence maintained through transparency

Maturity is about replacing crisis improvisation with documented procedures. Defining communication thresholds, establishing approval authorities, providing message templates, testing workflows, continuously improving through feedback.

Maturity Progression

The maturity ladder shows how crisis communication capability evolves from improvised crisis response to continuously optimized stakeholder communication with measured effectiveness.

LEVEL 5 STRATEGIC	**Stakeholder feedback surveys, automated notifications, measured communication metrics, continuous plan updates** Investment for organizations requiring demonstrable communication program optimization
LEVEL 4 ENHANCED	**Tabletop exercises, customized templates, annual review, post-incident communication analysis**
LEVEL 3 DOCUMENTED	**Communication plan, stakeholder procedures, approval authorities, message templates, role assignments** ← *Baseline for systematic crisis communication* *Eliminates improvised crisis response*
LEVEL 2 REACTIVE	**Informal understanding, ad hoc coordination, inconsistent messaging, no templates**
LEVEL 1 AD HOC	**No communication plan, crisis mode debates, inconsistent stakeholder information, improvised response**

What Changes at Each Level

Level 1 to 2: Organization recognizes need for communication plan but relies on informal coordination and ad hoc messaging.

Level 2 to 3: Organization documents crisis communication plan: incident thresholds, stakeholder procedures, approval authorities, message templates, role assignments.

Level 3 to 4: Communication procedures tested through tabletop exercises, templates customized for stakeholders, annual reviews, post-incident communication analysis.

Level 4 to 5: Continuous optimization through stakeholder feedback surveys, automated notification systems, measured communication metrics, plan updates from regulatory changes.

Framework Alignment at a Glance

Crisis Communications Readiness capability provides stakeholder notification procedures required by frameworks for incident response communication and disclosure.

NIST 800-53 (Incident Response)

Core capability for IR-4 (Incident Handling) with stakeholder notification procedures, IR-6 (Incident Reporting) extending to external communication, AU-6 (Audit Review) supporting audit finding disclosure.

Evidence: Crisis communication plan, stakeholder notification procedures, message templates, approval authorities

NIST CSF 2.0 (Respond)

Demonstrates RS.CO (Response Communications) coordinating with stakeholders including customers, suppliers, regulators during vulnerability-related incident response.

Evidence: Stakeholder notification procedures, communication coordination documentation

CIS Controls v8 (Incident Response)

Supports Control 17.9 (Incident Response Plan) by providing stakeholder communication component of comprehensive incident response procedures.

Evidence: Incident response plan including communication procedures

ISO 27001:2022 (Incident Management)

Core demonstration of A.5.26 (Response to Incidents) with stakeholder notification procedures and A.5.27 (Learning from Incidents) analyzing communication effectiveness.

Evidence: Incident response procedures with communication protocols, post-incident communication reviews

How to Use the Mapping Document

This guide explains why crisis communication readiness matters and what communication maturity looks like. The detailed mapping document contains framework control mappings and implementation guidance.

Reader Navigation

Incident Response Teams: Read entire guide to understand stakeholder communication planning for vulnerability-related incidents.

Communications Teams: Focus on message templates and approval authorities for crisis disclosure.

Security Leadership: Read Why This Exists to understand eliminating improvised crisis response through documented procedures.

GRC Teams: Read Framework Alignment overview, then use mapping to demonstrate communication readiness to auditors.

Use Case Scenarios

Scenario 1: Communication Plan Development

- Read: Why This Exists + Before/After comparison
- Use: Develop stakeholder notification procedures and approval authorities
- Then: Use mapping for regulatory compliance requirements

Scenario 2: Message Template Creation

- Read: Full guide for stakeholder-specific messaging
- Use: Create templates for customers, regulators, media
- Then: Use mapping for compliance language examples

Scenario 3: Tabletop Exercise

- Read: Maturity Progression for testing procedures
- Use: Design vulnerability disclosure scenario testing communication workflows
- Then: Use mapping for exercise evaluation criteria

Scenario 4: Audit Preparation

- Read: Framework Alignment + Boundaries
- Use: Demonstrate crisis communication readiness to auditors
- Then: Use mapping to compile communication procedure evidence

Common Misconceptions

MISCONCEPTION: "Having PR team means we have crisis communication readiness"

REALITY: Existence of communications department does not automatically mean documented procedures exist for vulnerability-related incident disclosure. Mature capability requires documented severity thresholds, stakeholder notification procedures, approval authorities, message templates, and tested communication workflows. General PR capabilities provide foundation but vulnerability-specific procedures require explicit definition and testing.

MISCONCEPTION: "Communication plan eliminates all stakeholder concerns"

REALITY: Even mature crisis communication cannot eliminate all negative stakeholder reactions to security incidents. Goal is transparency and systematic disclosure, not universal satisfaction. Documented procedures enable timely, accurate, consistent communication reducing confusion and demonstrating organizational preparedness, but cannot prevent all reputational impact or stakeholder concern about incidents themselves.

MISCONCEPTION: "Message templates can be used verbatim for any incident"

REALITY: Message templates provide starting point requiring incident-specific customization, not fill-in-the-blank forms used without adaptation. Each incident has unique circumstances requiring tailored messaging about affected systems, data types, timeframes, and remediation status. Templates accelerate initial drafting and ensure key elements addressed but must be customized for accuracy and relevance to specific incident details and stakeholder needs.

Boundaries and Non-Claims

What This Guide Is NOT:

- A replacement for technical incident response procedures (communication complements not replaces containment)
- A legal opinion on specific disclosure requirements (organizations must consult legal counsel)
- A determination that specific communication timing appropriate for all incidents (must reflect severity)
- A guarantee that communication eliminates all stakeholder concerns (transparency is goal not universal satisfaction)

What This Guide Provides:

- Guidance on communication maturity characteristics and crisis communication planning
- Framework alignment for incident response communication requirements
- Examples of evidence demonstrating stakeholder notification readiness
- Pathway to detailed mapping document for implementation

Critical Dependencies:

Crisis Communications Readiness depends on Program Governance (provides approval authorities for stakeholder notifications), Roles & Responsibilities (defines who performs communication activities), and Incident Response Integration (triggers communication procedures when incidents occur). Without these, unclear who has authority to approve disclosure, who executes communication activities, and when communication procedures should activate during incident response.

Regulatory requirements vary by jurisdiction and industry—communication plan must address applicable disclosure obligations. Legal review essential before implementing procedures. Communication timing critical—delayed notification increases penalties and distrust, premature disclosure may provide incomplete information requiring correction. Cultural and linguistic considerations important for international stakeholder populations.

This document is interpretive guidance. Normative definitions of the Crisis Communications Readiness capability and maturity levels are defined in the VMMM v2 Canon.

Next Steps

Assess Your Current State

- Identify whether organization has documented crisis communication plan for vulnerability-related incidents
- Evaluate whether stakeholder notification procedures exist or organization improvises crisis response

Identify Your Target State

- Level 3 provides baseline communication plan eliminating improvised crisis response
- Consider Level 4 if you need tested procedures through tabletop exercises and post-incident analysis

Plan Your Journey

- Document crisis communication plan with incident thresholds and stakeholder procedures
- Establish approval authorities and create message templates for common scenarios
- Assign communication roles and test procedures through tabletop exercises

Resources Available

- VMMM self-assessment tool for capability evaluation
- Detailed mapping documents for all 40 capabilities
- Communication plan templates and message examples

Questions or Feedback?
Contact ZenzizenSec for additional information or clarification.