Zero-Day Readiness

Capability Alignment Guide

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

Purpose:

Zero-Day Readiness enables organizations to respond effectively when vulnerabilities emerge with active exploitation, no patches available, and decision timelines measured in hours rather than days.

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

Executive Summary

Zero-day vulnerabilities expose the difference between documented processes and organizational muscle memory. When Log4Shell, MOVEit, or similar threats emerge on Friday afternoons, routine vulnerability management processes become inadequate. Response requires emergency executive meetings, patch-or-shutdown decisions with incomplete information, and coordination across teams who rarely work together under normal conditions.

Zero-Day Readiness capability transforms crisis from chaos into coordinated response. Organizations practice through tabletop exercises and simulations, discovering gaps in safe environments before real incidents occur. Playbooks document who gets called, who has decision authority, what communication templates exist, and what compensating controls can be deployed quickly.

Mature organizations activate practiced playbooks when zero-days hit. Response times measure in hours instead of days. Decisions get made by designated authorities instead of consensus paralysis. Stakeholders receive consistent messages instead of conflicting communications. The zero-day still causes disruption, but coordinated response minimizes damage and demonstrates organizational resilience.

This guide explains why crisis preparedness matters, what readiness maturity looks like, and how to use the detailed mapping document for exercise planning and framework alignment.

Why This Capability Exists

Routine vulnerability management assumes time for assessment, testing, and planned deployment. Zero-day events compress timelines to hours. Patches may not exist. Information remains incomplete and contradictory. Business stakeholders need immediate answers about customer impact and service availability.

Organizations without zero-day readiness discover response gaps during actual incidents. Nobody knows who makes the decision to take production systems offline. Communication templates do not exist for customers or regulators. Compensating controls remain untested. Teams burn hours arguing about response while attackers exploit systems.

Effective crisis response requires practice before crisis arrives. Tabletop exercises reveal unclear decision authority, missing contacts, inadequate communication plans, and untested mitigations. Post-incident reviews after simulations capture lessons in environments where mistakes do not create actual damage. Improvements integrate into playbooks before the next real zero-day emerges.

Before and After Comparison

WITHOUT MATURE ZERO-DAY READINESS:

- Critical zero-day announced Friday 3pm. Teams scramble to find contact lists and figure out who should be involved
- 12 hours of meetings to determine if systems should go offline. No clear decision authority
- Customer communication delayed 24 hours while teams debate wording. Media reports breach before official statement released

WITH MATURE ZERO-DAY READINESS:

- Critical zero-day announced Friday 3pm. Crisis playbook activated, designated leads notified within 15 minutes
- 2 hours to assess impact and deploy pre-tested compensating controls. CISO has clear decision authority documented in advance
- Customer communication sent within 6 hours using pre-approved templates. Coordinated message controls narrative

Maturity is about practiced coordination under pressure. Clear decision authority, tested workflows, pre-approved communications, and continuous improvement from exercises and actual events.

Maturity Progression

The maturity ladder shows how zero-day response capability evolves from reactive chaos to practiced crisis coordination.

LEVEL 5 STRATEGIC	**Automated threat detection, workflow automation, continuous improvement from every event** Significant investment - consider for high-frequency threat environments
LEVEL 4 ENHANCED	**Scenario-specific playbooks, regular simulations, measured response improvements**
LEVEL 3 DOCUMENTED	**Defined process, documented roles, communication channels established** ← *Baseline crisis preparedness for most organizations* *Demonstrates planned response to auditors and boards*
LEVEL 2 REACTIVE	**Ad hoc procedures, response depends on individual effort, ownership unclear**
LEVEL 1 AD HOC	**No formal process, teams react inconsistently, limited coordination**

What Changes at Each Level

Level 1 to 2: Some informal procedures emerge, but response depends on individual heroics and tribal knowledge.

Level 2 to 3: Organization documents crisis process with assigned roles, contact lists, and communication channels. Response becomes repeatable.

Level 3 to 4: Regular simulations practice response. Scenario-specific playbooks address different threat types. Response times improve through measurement.

Level 4 to 5: Automation accelerates detection and initial response. Continuous improvement from every exercise and incident. Investment justified for high-threat environments.

Framework Alignment at a Glance

Zero-Day Readiness strengthens incident response and contingency planning requirements across security frameworks by demonstrating preparedness for highest-pressure scenarios.

NIST 800-53 (Incident Response, Contingency Planning)

Demonstrates IR-4 (Incident Handling) capability under most demanding conditions. Provides IR-8 (Incident Response Plan) addressing time-critical scenarios. Supports CP-2 (Contingency Plan) for rapid response and service continuity decisions.

Evidence: Crisis response playbooks, simulation records, communication templates, decision authority documentation

NIST CSF 2.0 (Respond)

Supports RS.MA (Incident Management), RS.AN (Analysis), and RS.CO (Communications) during crisis scenarios requiring rapid coordination, decision-making under uncertainty, and stakeholder notification.

Evidence: Incident management procedures, analysis workflows, communication processes

CIS Controls v8 (Control 17 - Incident Response Management)

Implements 17.1 (Designate Personnel) with clear crisis authority. Demonstrates 17.9 (Conduct Exercises) through regular simulations addressing zero-day and critical vulnerability scenarios.

Evidence: Personnel designations, exercise records, incident response procedures

ISO 27001:2022 (Incident Management)

Core capability for A.5.26 (Response to Information Security Incidents) demonstrating preparedness for crisis-level scenarios. Shows A.5.24 (Planning and Preparation) through documented procedures and regular testing.

Evidence: Incident response planning documentation, preparation activities, testing records

How to Use the Mapping Document

This guide provides crisis preparedness overview. The detailed mapping document contains framework control mappings and evidence requirements for audit preparation.

Reader Navigation

Executives and Board Members: Read Executive Summary and Maturity Snapshot to understand organizational crisis preparedness. Skip technical details unless specific questions arise.

CISOs and Security Leadership: Read entire guide, then use mapping document to develop crisis playbooks and communication templates.

Incident Response Teams: Focus on Maturity Progression and Why This Exists sections to understand response requirements, then reference mapping document for playbook development.

GRC and Audit Teams: Read Framework Alignment overview, then use mapping document for detailed control mappings and evidence requirements.

Use Case Scenarios

Scenario 1: Crisis Preparedness Assessment

- Read: Why This Exists + Maturity Snapshot
- Use: Evaluate current crisis readiness, identify gaps
- Then: Use mapping document for detailed gap analysis

Scenario 2: Tabletop Exercise Planning

- Read: Maturity Progression focusing on Levels 3-4
- Use: Design exercise scenarios testing coordination and decision-making
- Then: Use mapping document for exercise templates and success criteria

Scenario 3: Incident Response Plan Development

- Read: Full guide for crisis response requirements
- Use: Understand required elements (roles, procedures, communications)
- Then: Use mapping document for plan structure and content

Scenario 4: Board Reporting

- Read: Executive Summary + Framework Alignment
- Use: Demonstrate organizational crisis preparedness
- Then: Use mapping document for detailed evidence if questioned

Common Misconceptions

MISCONCEPTION: "Having a playbook means we are prepared for zero-days"

REALITY: Maturity requires testing through simulations. Untested playbooks often fail under actual pressure when gaps and assumptions are exposed.

MISCONCEPTION: "Zero-day response is a technical security problem"

REALITY: Effective response requires cross-functional coordination including legal, communications, business leadership, and external stakeholder management. Security alone cannot respond effectively.

MISCONCEPTION: "This capability guarantees successful zero-day response"

REALITY: Preparation reduces chaos but does not eliminate risk. Zero-days remain disruptive. Maturity enables coordinated, measured response rather than guarantee of success.

Boundaries and Non-Claims

What This Guide Is NOT:

- A complete incident response playbook ready for use
- A guarantee that zero-day response will be successful
- A substitute for threat intelligence and vulnerability detection capabilities
- A framework compliance certification or accreditation

What This Guide Provides:

- Guidance on crisis preparedness maturity characteristics
- Framework alignment for incident response requirements
- Examples of evidence demonstrating readiness
- Pathway to detailed mapping document for implementation

Critical Dependencies:

Zero-Day Readiness depends on Threat Intelligence (detection and assessment), Compensating Controls (emergency mitigations), Crisis Communication Readiness (stakeholder notification), and Program Governance (executive decision authority). Without these capabilities, playbooks lack inputs, mitigations, communication channels, and decision-makers.

Readiness degrades without continuous practice. Personnel turnover, system changes, and threat evolution require regular exercises and playbook updates. One-time preparation becomes obsolete without ongoing investment in simulations and improvement.

Next Steps

Assess Your Current State

- Review existing incident response plans for zero-day specific procedures
- Identify gaps in roles, playbooks, communications, and testing

Identify Your Target State

- Level 3 provides baseline crisis preparedness for most organizations
- Consider Level 4 if high-threat environment or regulatory requirements demand regular testing

Plan Your Journey

- Develop crisis playbooks documenting roles, procedures, and communications
- Schedule initial tabletop exercise involving cross-functional teams
- Establish regular exercise cadence and improvement process

Resources Available

- VMMM self-assessment tool for capability evaluation
- Detailed mapping documents for all 40 capabilities
- Exercise templates and crisis playbook guidance

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