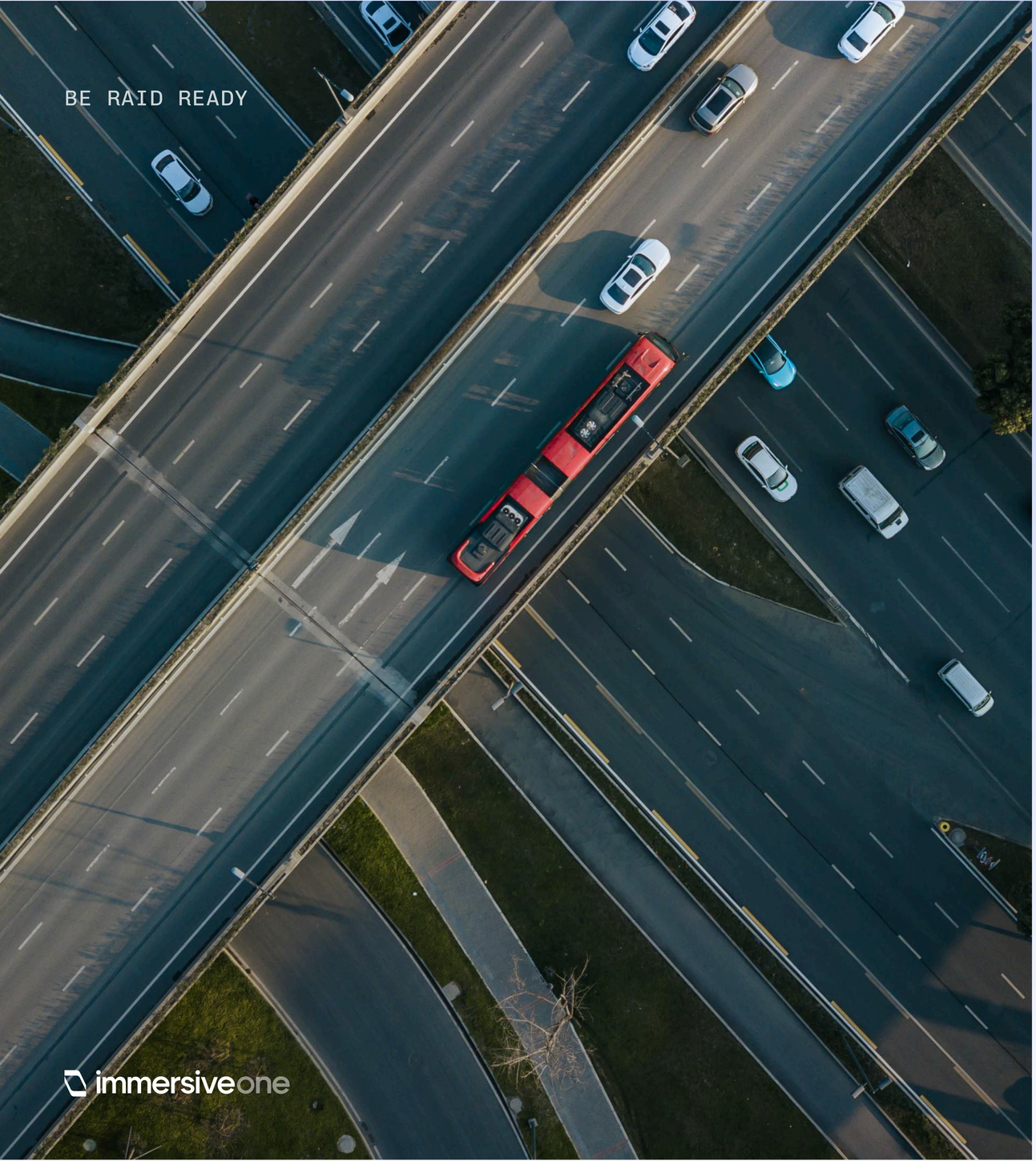
immersiveone

Mastering executive response in a high-stakes, all-hazards landscape



www.immersivelabs.com

EBOOK / 2026



The executive playbook for impact-based crisis response

In today's RAID (Relentless, Accelerated, Interconnected, and Dynamic) Landscape, crisis management is no longer a localized operational duty; it is a board-level strategic imperative. AI is accelerating how organizations operate and how quickly risk can become operational, while geopolitical tensions can trigger cascading disruptions across global supply chains and critical infrastructure.

The global cost of cybercrime is staggering, but the risks go far beyond malware. To command the RAID Landscape, organizations must understand the implications of each RAID pillar.

Relentless, Accelerated, Interconnected, Dynamic.

RELENTLESS:	Threat actors are industrialized and operate 24/7; crisis events occur anytime, anywhere. Annual compliance checks are no longer sufficient.
ACCELERATED:	AI-powered threats and AI-enabled workflows move faster than ever, compressing attack paths and shrinking the window for executive decision-making.
INTERCONNECTED:	A single compromised endpoint or a vulnerable third-party vendor can trigger a cascading firm-wide physical and digital crisis. Geopolitical tensions half a world away can indirectly disrupt you business given our interconnected economy.
DYNAMIC:	The enterprise risk environment is alive and constantly evolving. Threats extend far beyond malicious cyber actors to include severe weather, supply chain collapses, geopolitical shifts, and AI-accelerated risks. This unpredictable reality means static, slide-driven training aRnd infrequent tabletop exercises cannot prove teams and leaders can perform under pressure.

Contents

Preparation requires a collaborative, unified effort across all levels of executive leadership. Grounded in global standards such as ISO 22361 (Crisis Management) and the NIST Cybersecurity Framework, this document serves as a guide for the C-suite to understand their roles, refine decision-making under extreme pressure, and leverage the Immersive platform to build all-hazards resilience that is exercised, measured, and proven—not assumed.

01 All-Hazards and Impact-Based Planning

02 The Psychology of Executive Decision-Making Under Pressure

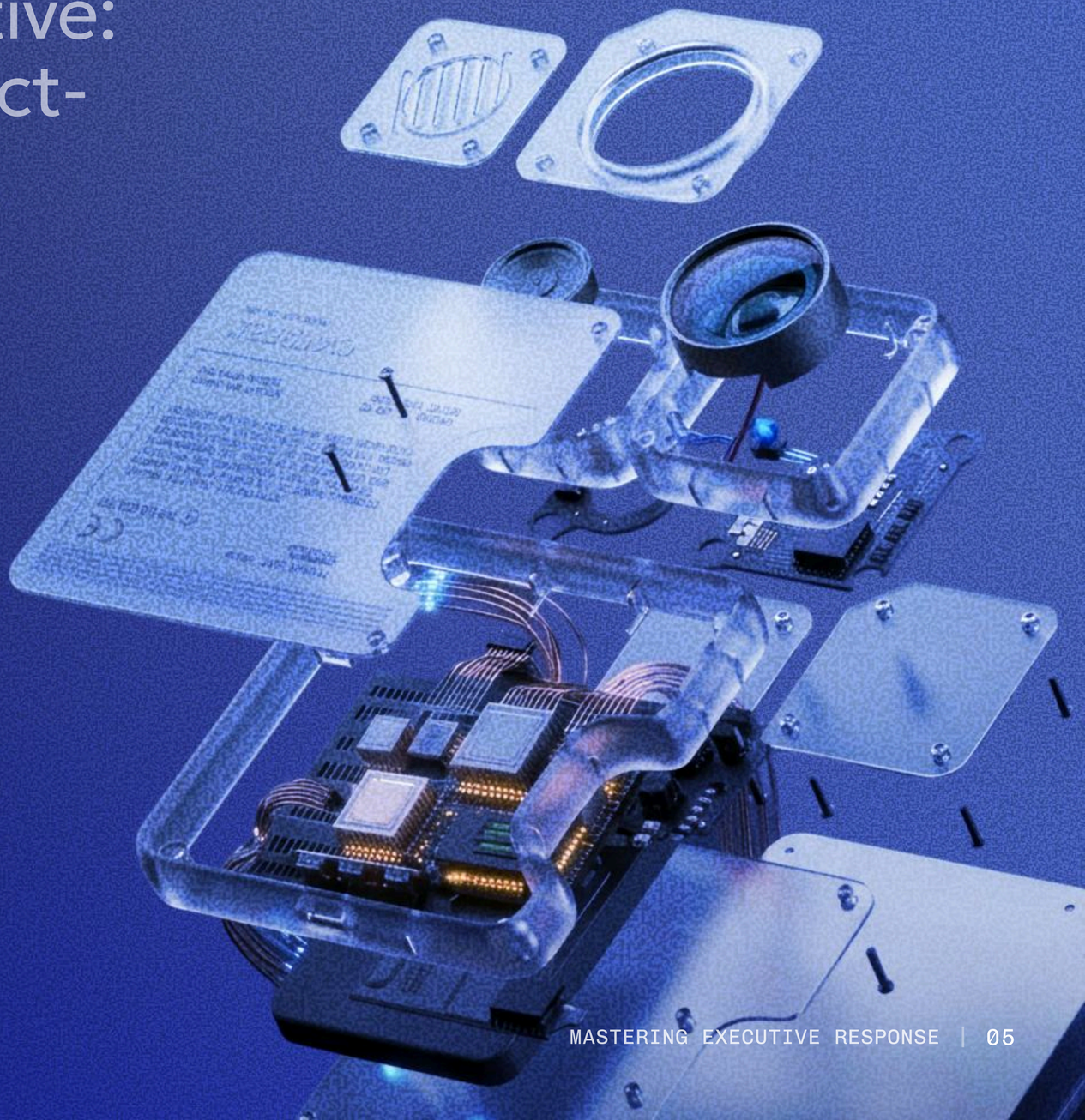
03 Role-Specific Crisis Readiness

04 Best Practice Framework: The Three-Tiered Response Structure

05 The Immersive Approach: Proving Resilience in a Dynamic World

A crisis challenges an organization beyond its inherent coping capacity, threatening its viability, reputation, and stakeholders. Traditional crisis preparation often relies on attempting to predict and plan for every specific scenario. But in a volatile environment—where AI can accelerate both business activity and threat activity—it is impossible to envision and prepare for every disruptive event.

01 The strategic imperative: all-hazards and impact-based planning



The Shift: impact-based planning

While threat-specific playbooks remain vital for regulatory compliance, security and risk management leaders must elevate their overarching strategy to an impact-based model. To build true resilience, organizations must adopt an All-Hazards approach. This means preparing a foundational response structure capable of handling any extreme disruption. It is vital to understand the distinctions and, more importantly, the commonalities between digital and non-digital crises:

THE DISTINCTION:

Cyber/digital crises (e.g., ransomware, destructive wiper malware) originate in the technology stack and often involve malicious, active adversaries deliberately trying to outmaneuver your defenses. Non-cyber/physical crises (e.g., natural disasters, physical supply chain failures, geopolitical conflicts) originate in the physical world and often require immediate life-safety considerations and physical logistics.

THE COMMONALITIES:

Regardless of the trigger, the impacts are often identical. Both a severed undersea internet cable (physical) and a massive ransomware attack (digital) result in catastrophic IT downtime. Both a rogue executive scandal and a major data privacy breach result in severe reputational damage, regulatory scrutiny, and financial loss.

TRANSITIONING TO IMPACT-BASED PLANNING SIMPLIFIES ESCALATION DECISIONS.

If your leadership team is prepared to handle severe communications disruptions, financial hemorrhaging, or technology outages, they establish a universal foundation of resilience. This ensures the organization survives the initial shock, giving leadership the bandwidth to navigate the unique, origin-specific complexities of the threat, whether that is a natural disaster or a targeted cyberattack.



02 The psychology of executive decision-making under pressure

During a crisis, executives face extreme psychological pressures, high levels of uncertainty, and an abundance of incomplete information.

The C-suite must recognize that crisis decision-making is fundamentally different from day-to-day operations and often involves facing high-stakes scenarios, or “wicked problems,” where there are no perfect solutions, only calculated trade-offs that require absolute executive alignment.

NAVIGATING DILEMMAS:	Crisis decisions often involve moral hazards where there are no perfect answers, only "better" or "worse" outcomes (e.g., paying a ransom to save lives vs. funding terrorism).
COMBATING DECISION PARALYSIS:	Uncertainty can block or delay teams from implementing decisions due to the fear of accountability with hindsight. Doing nothing can be perceived as less blameworthy, but failing to act is often the most damaging choice.
MANAGING COGNITIVE BIASES:	Executives cannot defeat psychological biases simply by being aware of them. They must expose them through live-fire simulations. By tracking decision-making pathways under pressure, organizations can identify and actively counteract anchoring bias, confirmation bias, and overconfidence with objective data.
ESTABLISHING PSYCHOLOGICAL SAFETY:	Leaders must foster a safe environment where team members feel comfortable voicing concerns or challenging assumptions to avoid dangerous groupthink.



03 The top 10 actions **executives** must prepare for

To command the RAID landscape, organizations cannot rely on theory; they must operationalize their defense. The following ten actions are not just planning steps, they are the required capabilities to counter a Relentless, Accelerated, Interconnected, and Dynamic threat environment. Documenting these actions is only step one; organizations should continuously exercise, measure, and validate these capabilities under realistic pressure so readiness is proven rather than assumed:_x000B_

01 Define Viability Thresholds: Systematically evaluate what specific failures (financial, operational, or reputational) would put the firm's overall viability at risk.

02 Adopt Impact-Based Escalation: Implement simplified escalation procedures and scorecards based on business impact rather than specific threat scenarios, enabling faster activation of the Crisis Management Team (CMT). This escalation velocity should be tested regularly through dynamic simulations.

03 Establish Alternate Communications: Plan for normal collaboration tools to be compromised and secure out-of-band communication channels.

04 Appoint and Empower Delegates: Ensure all key participants have appointed first and second delegates who are empowered to make strategic decisions.

05 Resource the Support Teams: Form a dedicated support group (incident loggers, crisis coordinators, client advocates) who can step out of their day jobs to assist the executive team full-time.

06 Map Critical Dependencies: Understand the exact operational, technology, and vendor linkages the organization relies on across all geographies. Use cross-functional cyber drills to uncover hidden dependencies before an attacker exploits them.

07 Prepare for Regulatory Escalation: Know exactly which regulators, boards, and law enforcement agencies must be notified, in what order, and within what timeframes.

08 Document Decision Rationale: Ensure a "log keeper" meticulously records what decisions were made, the options considered, and the rationale.

09 Formulate a Unified Message: Speak with one consistent voice across all channels. Acknowledge uncertainty early, provide known facts, and prioritize empathy.

10 Mandate Postmortems and Dynamic Calibration: After a crisis or simulation, conduct rigorous reviews to uncover inefficiencies and root causes. Furthermore, recognize that a playbook is a living document; continuously calibrate your crisis scenarios against major geopolitical shifts, public competitor breaches, and new regulatory mandates to ensure your readiness matches the current reality.

04

Role-specific crisis readiness

EXECUTIVE ROLE:	KEY CRISIS RESPONSIBILITIES & PREPARATION FOCUS:
Chief Executive Officer (CEO)	Acts as the ultimate Crisis Commander. Must prioritize the organization's core values, interface with the Board, lead the team's executive meetings, and make final calls on viability-threatening dilemmas.
Chief Financial Officer (CFO)	Assesses the financial impact of the crisis and response. Must prepare for liquidity funding issues, missed margin payments, and the authorization of emergency contingency budgets.
Chief Information / Security Officer (CIO/CISO)	Translates technical realities into business risk. Must prepare to communicate containment status without jargon, manage the influx of threat intelligence, and advise the CEO on the technical feasibility of recovery options versus ransom payment.
Chief People Officer / HR	Monitors the status, safety, and well-being of all staff. Must prepare for trauma counseling, fatigue management for responders, and deploying "safe and well" procedures.
Legal & Compliance	Provides real-time counsel on regulatory breach reporting, data privacy cross-border issues, and liability. Must ensure the team understands how to operate under Legal Privilege.
Head of PR / Communications	Controls the creation and delivery of all internal and external messaging. Must prepare holding statements, monitor social media sentiment, and coordinate media relations.
Business Line Heads	Considers the operational impact on services and products. Must prepare to implement manual workarounds, manage client expectations, and balance commercial decisions.

05 Best practice framework: the three-tiered response structure

In the accelerated reality of the RAID threat landscape, a crisis demands a highly disciplined organizational structure to preserve executive decision-making bandwidth and prevent the C-suite from becoming bogged down in tactical execution.

Global best practices, including those outlined in ISO 22361, consistently advocate for a three-tiered response architecture.

While naming conventions vary around the world, such as the Incident Command System (ICS/NIMS) in North America or Gold/Silver/Bronze designations in the UK, the core objective is universally consistent: unequivocally separate strategic command from operational coordination and tactical resolution.



To illustrate this architecture in action, we leverage the Orchid Corp Strategic Response Model. Orchid Corp is a fictitious, globally distributed enterprise utilized within Immersive's exercises.



The Orchid Crisis Management Plan is designed to represent a proven, best-practice structure that organizations can confidently adopt and adapt.

Establishing a three-tiered architecture on paper is essential for keeping every responder in their proper lane, preventing the CEO from managing firewall rules and stopping the SOC analyst from drafting press statements.

However, a documented structure is only theoretical until it is pressure-tested. To ensure seamless communication and rapid decision-making across the Strategic, Operational, and Tactical tiers during an actual event, organizations must move from static planning to dynamic, continuous validation—and use performance under pressure as evidence of readiness.

ILLUSTRATIVE EXAMPLE: THE ORCHID CORP CRISIS RESPONSE MODEL

01

The Strategic Team (Executive/Board Level)

Objective: Focus entirely on the What and the Why. The Strategic Team is responsible for the overall strategic direction, prioritizing organizational viability, safeguarding reputation, and setting the parameters within which the lower tiers must operate.

Composition: C-Suite executives and key senior leaders (with designated liaisons responsible for regular Board briefings).

Key Duties: Making enterprise-threatening decisions (e.g., paying a ransom, halting global operations), authorizing emergency budgets, managing major stakeholder relations.

The Rule: The Strategic Team must remain strictly hands-off regarding technical or operational fixes.

02

The Operational Team (Management Level)

Objective: Focus on the How. The Operational Team translates the strategic intent set by the Strategic Team into actionable plans and coordinates the resources required to execute them.

Composition: Department heads, regional directors, and functional leads.

Key Duties: Developing the tactical action plan, allocating resources to the Tactical teams, managing inter-departmental conflicts, determining operational workarounds, and filtering information up to the Strategic team.

The Rule: The Operational Team must act as the filter, protecting the Strategic Team from tactical noise, while ensuring the Tactical Team has the specific resources it needs to execute.



03

The Tactical Team (Responder Level)

Objective: Focus on the Doing. The Tactical tier is the "hands-on" level where the physical or digital work is executed to resolve the crisis.

Composition: Subject Matter Experts (SMEs), front-line responders, engineers, SOC analysts, and facility managers.

Key Duties: Executing the tactical plan (e.g., isolating infected servers, repairing physical damage, patching vulnerabilities) and reporting upward to the Operational Team.

The Rule: The Tactical Team must focus exclusively on technical resolution and real-time reporting, leaving all broader strategic consequences and decision-making for the Operational and Strategic teams to manage.

06

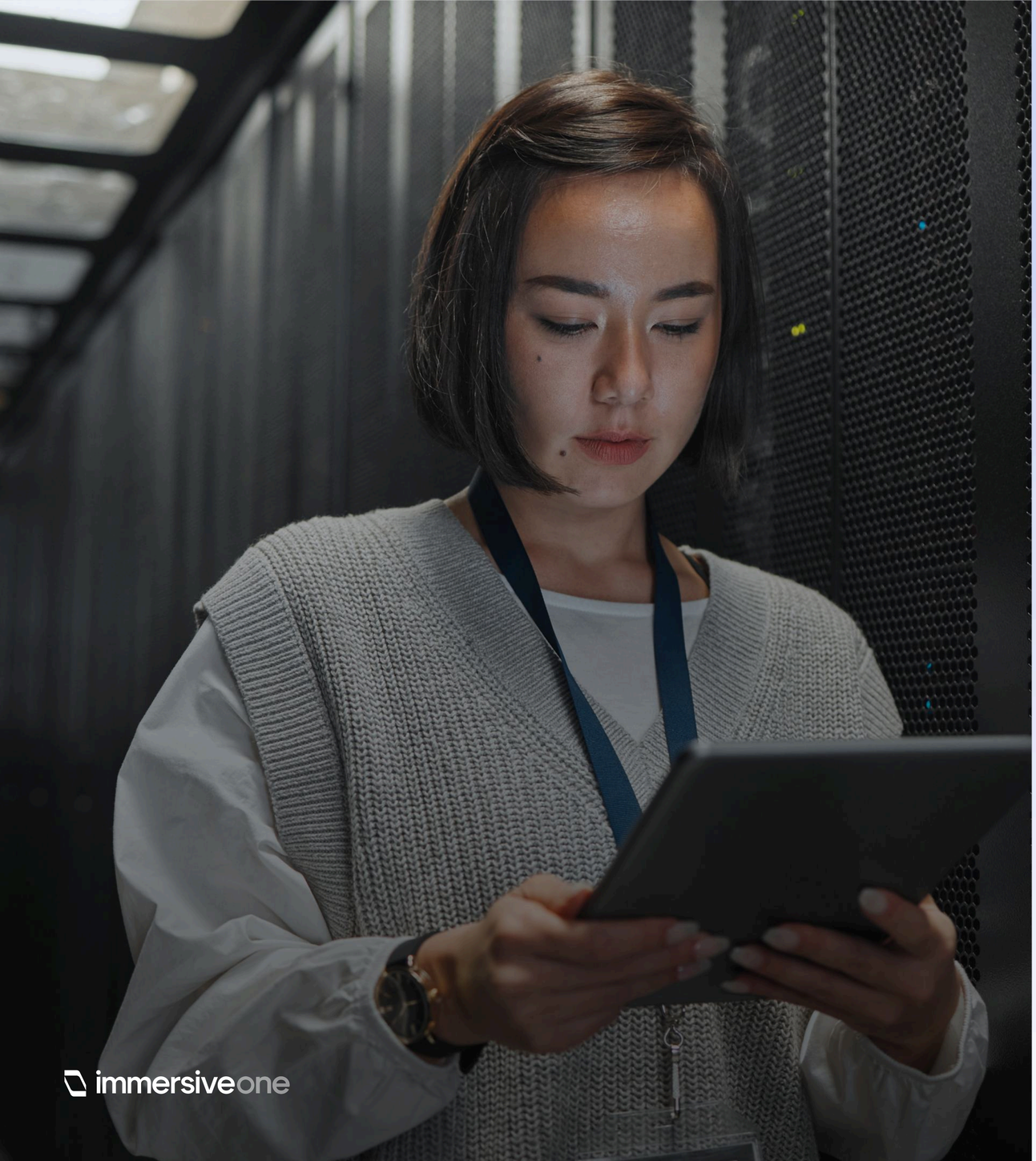
The Immersive approach: **proving resilience** in a dynamic world

Traditional crisis preparation has heavily relied on static, slide-driven tabletop exercises spaced at arbitrarily timed intervals.

Because organizations are now operating in a continually evolving, all-hazards risk landscape that extends far beyond cyber threats, legacy methods struggle to replicate the speed, noise, and chaos of a real-world crisis. The result can be a readiness gap where confidence outpaces demonstrated capability.



immersiveone



Immersive turns organizational readiness into evidence the business can use through a continuous PIBR model:

Prove:

Run live-fire, software-driven crisis simulations featuring dynamic storylines, real-time crisis feeds, and AI-driven actors. Test whether teams and leaders can perform securely and effectively under realistic pressure.

Improve:

Use data-driven insights to identify gaps in decision pathways and cross-functional coordination, then turn those exposed gaps into targeted improvement and repeatable readiness.

Benchmark:

Align crisis response strategies against global industry standards and frameworks (such as ISO 22361 for Crisis Management and the NIST Cybersecurity Framework), peer context, and historical response timelines to understand where readiness stands and where it must improve.

Report:

Translate performance data into board-ready evidence leaders can use to demonstrate oversight, justify investment, support regulatory conversations, and show progress over time.

PROVE, BENCHMARK, IMPROVE, REPORT

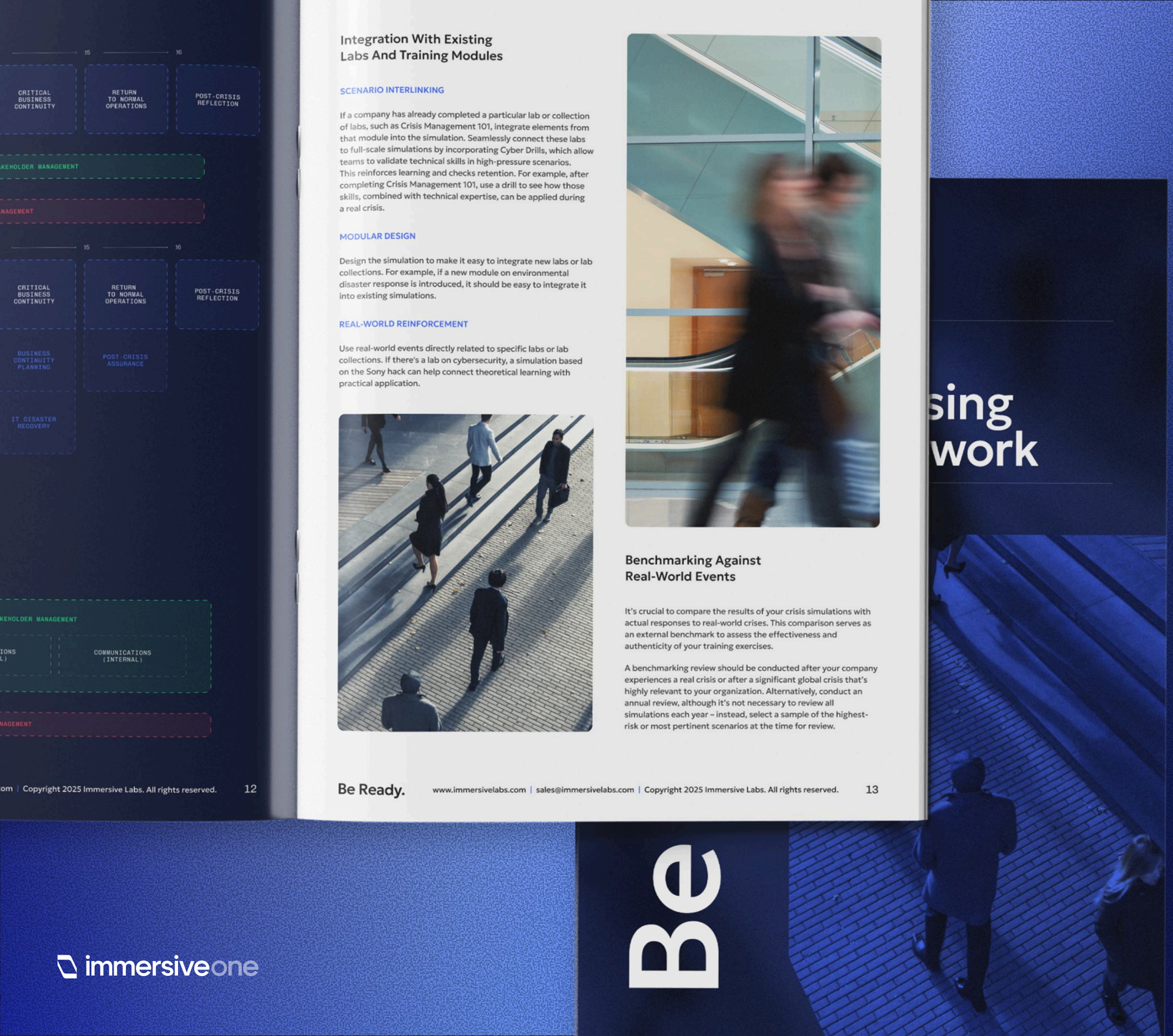
Crisis exercising framework

A structured and systematic approach to exercising roles across the lifecycle of and incident and/or crisis.

The framework structures exercise programs to practice decision-making at the appropriate organizational level. Its application tests and validates preparedness, enhancing overall resilience by identifying opportunities for decision-making improvement and areas requiring greater confidence in processes, knowledge, or skills.

Informed by and aligned with NIST 800-61, ISO 22361, ISO 22301, ISO 27035 and ISO 27001

New After Action Reporting aligned to Crisis Exercising Framework will be released in April 2026



01	02	03	04	05	06
Initial Response Categorization and escalation	Containment	Assessment and Response	Critical Business Continuity	Return to Normal Operations	Post-Crisis Reflection

A Communications and Stakeholder Management

B Resource Management



By prioritizing Immersive, all-hazards exercising across every tier of your response structure, your organization shifts from hoping it is ready to having evidence that it is ready. Ensure your leadership team is prepared to protect the business, your customers, and your reputation when the inevitable occurs.

immersive

Continuously assess, build, and prove your cyber resilience

Our immersive cybersecurity solutions ensure your team is prepared to tackle and defend against the evolving cyber risks of today, and tomorrow.