



HARPONIAN

INTERNATIONAL

AI Incident Response for Executives

Roles, Escalation, and Decision-Making

Format	Duration	Audience	Deployment	LMS / SSO	PO
Live / Recorded	60 min	Executives / Board	Enterprise licensing	N/A	Supported

Executive Overview

AI Incident Response for Executives is a live or recorded, scenario-based executive briefing that prepares leadership for AI-related incidents before they occur. It explains what can happen when AI systems or AI use go wrong, including errors, misuse, reputational harm, regulatory exposure, and operational disruption. The briefing clarifies executive roles, escalation expectations, and decision points so leaders can respond with less confusion and more defensible judgment.

Briefing Outcome

Equip executives, board members, and crisis management leaders with a clear response model for AI incidents, including who should be involved, when issues should escalate, and how key decisions should be documented.

Why This Matters

AI incidents can move quickly across legal, operational, communications, security, compliance, and reputational domains. Leadership needs a shared playbook before an incident occurs so the organization can act consistently, preserve trust, and support reviewable decision-making.

Enterprise Risk Exposure Addressed

- Delayed escalation when AI misuse, errors, or unexpected outputs are discovered
- Unclear executive ownership during incidents involving AI tools or AI-generated decisions
- Reputational, regulatory, or customer-impact exposure from inconsistent response actions

What the Organization Receives

- **Executive AI Incident Response Briefing:** Scenario-based leadership discussion covering roles, escalation, and decision-making expectations.
- **AI Incident Roles and Escalation Map:** Practical guidance on who should be involved and when an AI-related issue should be raised for executive review.
- **Decision-Making Framework:** A structured approach for assessing severity, business impact, legal or regulatory exposure, and communications needs.
- **Crisis Coordination Notes:** Guidance for aligning executive leadership, legal, compliance, information security, operations, and communications teams.
- **Defensible Response Documentation Guide:** Prompts for recording key facts, decisions, approvals, follow-up actions, and lessons learned.