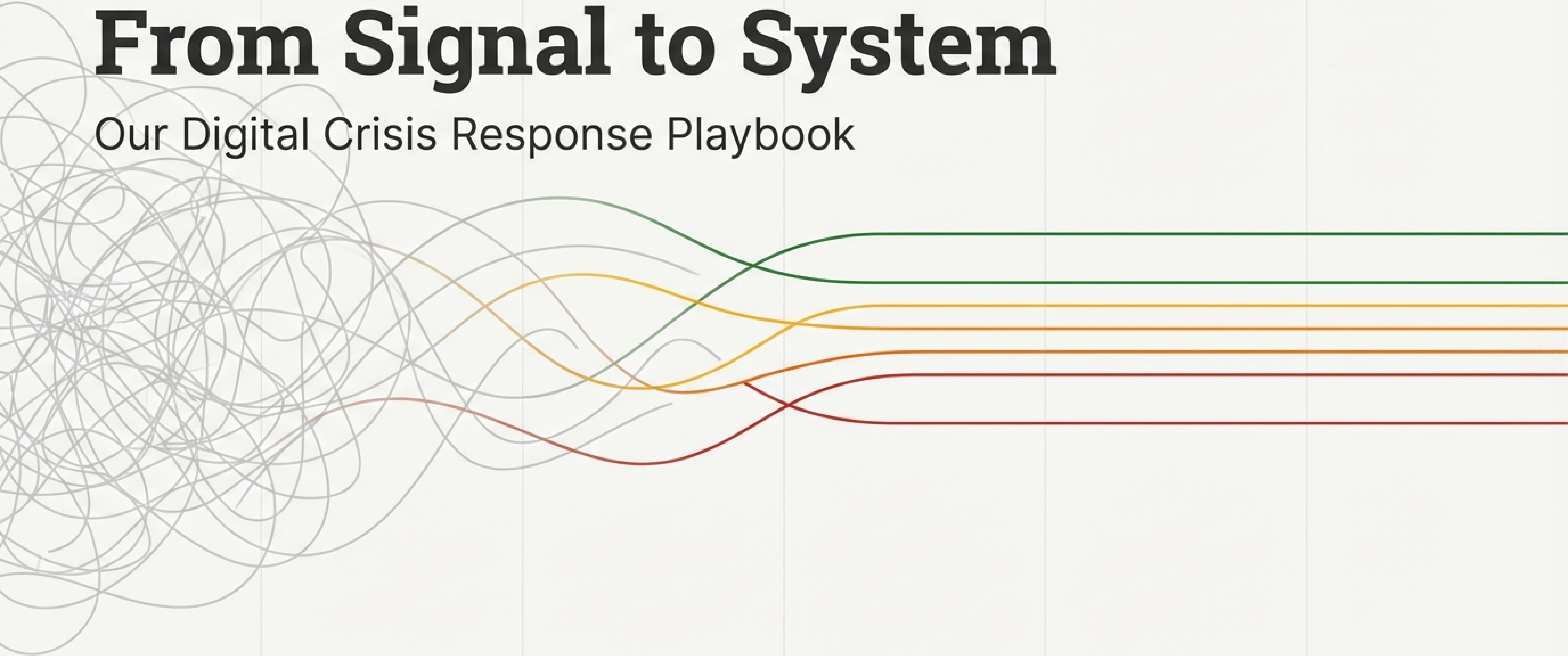
From Signal to System

Our Digital Crisis Response Playbook



Part of The Social Listening System™ | The DPRI Method™

We classify every threat to ensure our response matches the risk.

Our system categorises potential issues into four distinct levels, moving from minor incidents to existential threats. This allows us to allocate the right resources, at the right speed, every time. Each level has a specific owner, timeline, and escalation protocol.

🟢 LEVEL 1: MINOR ISSUE

Localised negative sentiment with limited reach and no escalation risk.

🟡 LEVEL 2: MODERATE ISSUE

Emerging negative pattern requiring monitoring and coordinated response.

🟠 LEVEL 3: MAJOR CRISIS

Significant reputation threat requiring immediate cross-functional response and potential public statement.

🔴 LEVEL 4: EXISTENTIAL CRISIS

Severe threat to brand reputation, customer trust, or business viability requiring all-hands response.

The anatomy of a crisis: How we measure severity.

	Level 1 (🟢)	Level 2 (🟡)	Level 3 (🟠)	Level 4 (🔴)
VOLUME (Negative Mentions)	<10	10-50	50-500	>500+
VELOCITY (% increase in 24h)	Stable	50-100%	100-500%	>500% (Viral)
SENTIMENT (% Negative)	<30%	40-60%	60-80%	>80%
REACH (Account Influence)	Low (<1k followers)	Medium (1k-10k)	High (10k-100k)	Major Influencers / Mass Media
RESPONSE TIMELINE	Within 4 hours	Within 2 hours	Within 1 hour	Immediate (minutes)

Stage 1: Detection – How we find the signal in the noise.

Our first line of defence is a comprehensive monitoring protocol. We combine automated alerts for high-risk signals with a disciplined manual review process to ensure nothing is missed.

Automated Alerting

🔴 **CRITICAL ALERTS (L3-4):** Immediate SMS, Phone Call, Slack. For keywords like “lawsuit,” “data breach,” “fraud.”

🟡 **HIGH-PRIORITY ALERTS (L2):** Slack & Email. For keywords like “terrible experience,” “switching from [brand].”

🟢 **STANDARD ALERTS (L1):** Digest every 4 hours. General brand and competitor mentions.

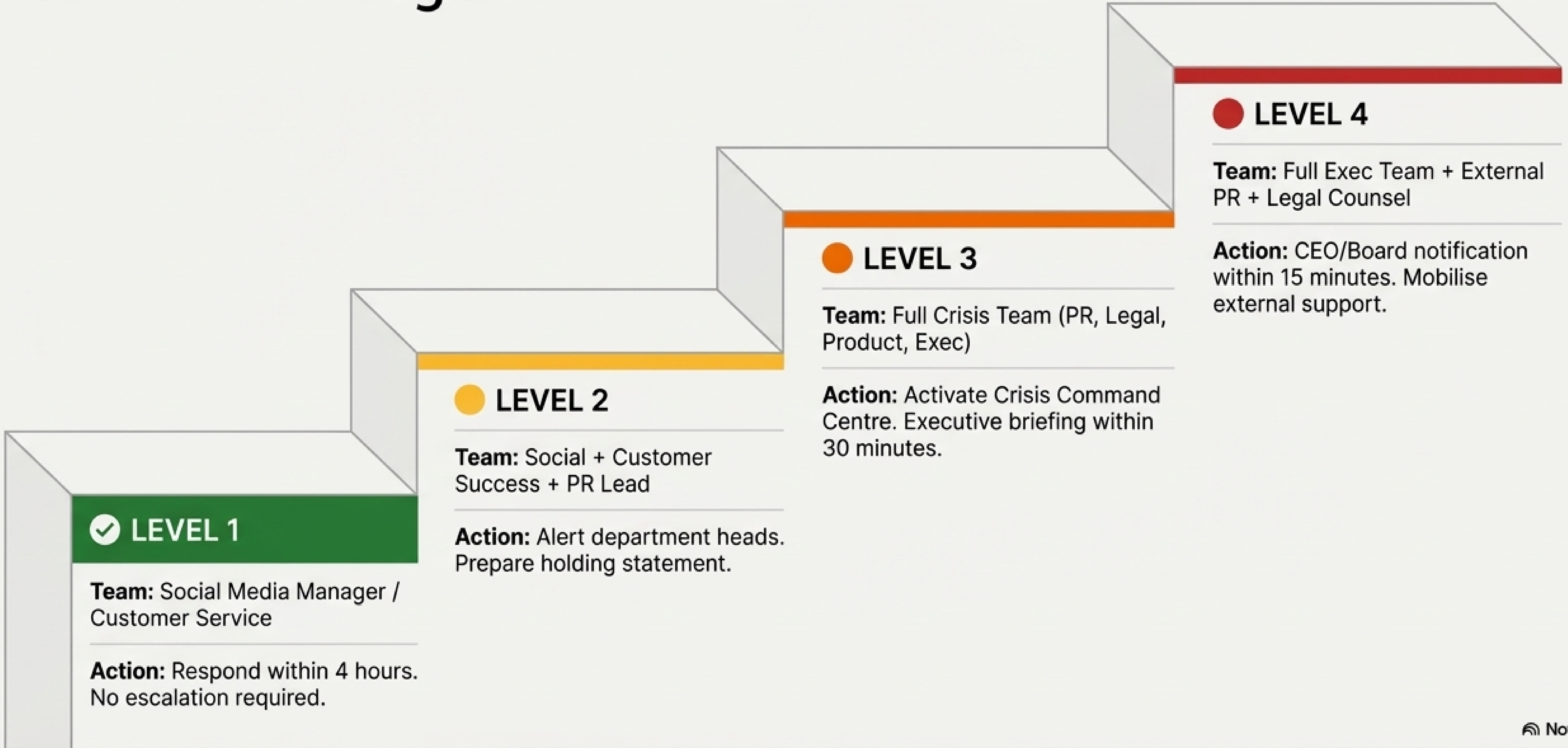
Manual Monitoring

DAILY CHECKLIST (Before 9 AM): Scan top mentions, review sentiment trends, check overnight alerts.

CONTINUOUS CHECKLIST (Every 4 Hours): Review new mentions, monitor crisis keywords.

END-OF-DAY CHECKLIST (Before 6 PM): Final review, brief overnight team.

Stage 2: Escalation – Activating the right team at the right time.



✓ LEVEL 1

Team: Social Media Manager / Customer Service

Action: Respond within 4 hours. No escalation required.

● LEVEL 2

Team: Social + Customer Success + PR Lead

Action: Alert department heads. Prepare holding statement.

● LEVEL 3

Team: Full Crisis Team (PR, Legal, Product, Exec)

Action: Activate Crisis Command Centre. Executive briefing within 30 minutes.

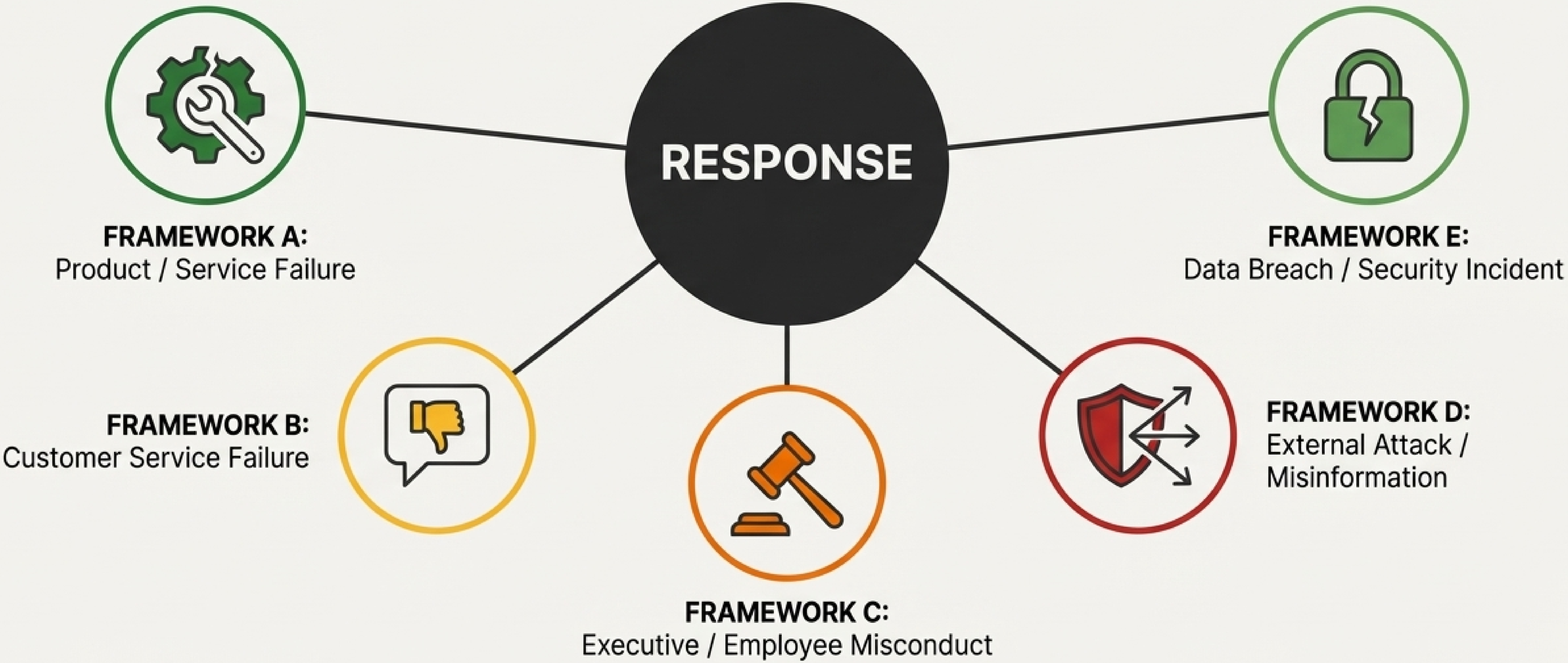
● LEVEL 4

Team: Full Exec Team + External PR + Legal Counsel

Action: CEO/Board notification within 15 minutes. Mobilise external support.

Stage 3: Response – We have a specific framework for every crisis.

A crisis is not a single event; it's a category of problem. We have developed five distinct response frameworks, each with a unique sequence of actions, key principles, and communication templates tailored to the specific situation.



RESPONSE

FRAMEWORK A:
Product / Service Failure

FRAMEWORK B:
Customer Service Failure

FRAMEWORK C:
Executive / Employee Misconduct

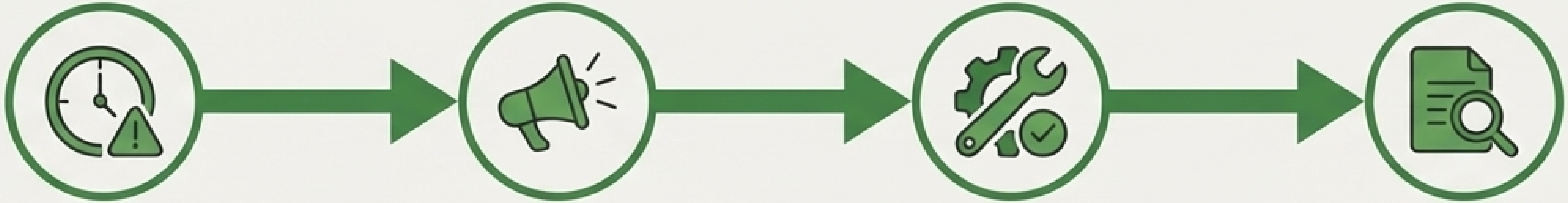
FRAMEWORK D:
External Attack /
Misinformation

FRAMEWORK E:
Data Breach / Security Incident

Responding to Product & Service Failures (Frameworks A & B).

For operational issues, our priority is speed, transparency, and empathy. The goal is to acknowledge the problem, manage customer expectations, and fix both the individual issue and the underlying system.

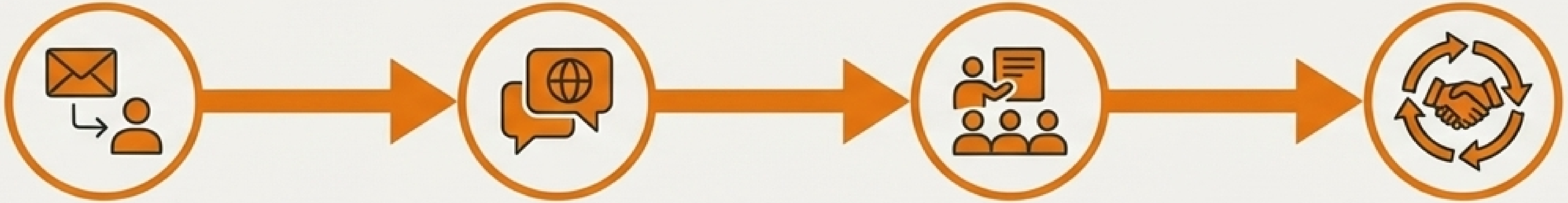
Product Failure (e.g., Service Outage)



1. Acknowledge (<1hr)
2. Update (every 2-4hrs)
3. Resolve
4. Post-Mortem (48-72hrs)

Key Principle: Acknowledge quickly, even without all the answers. Set and meet update expectations.

Customer Service Failure (e.g., Poor Support Experience)



1. Private Outreach (DM)
2. Public Acknowledgment
3. Internal Review
4. Close Loop Publicly

Key Principle: Take the conversation private first. Empathise first, explain second.

Responding to Misconduct & Misinformation (Frameworks C & D).

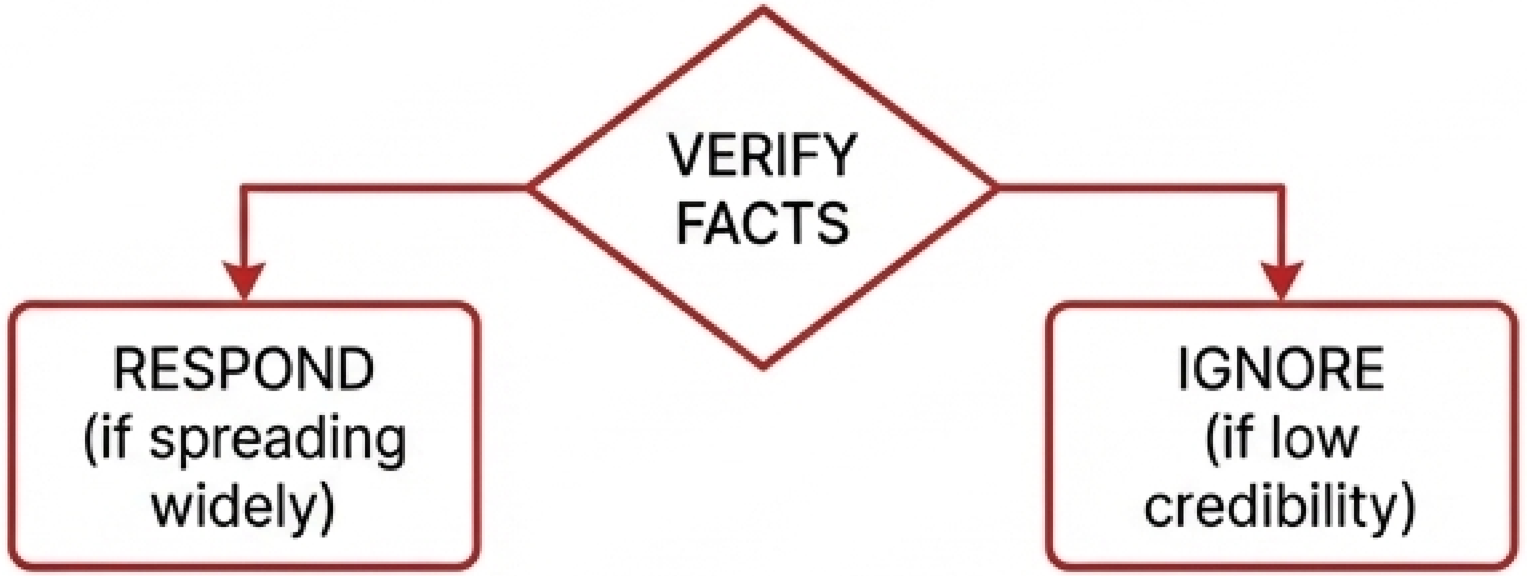
When dealing with reputational threats, our response becomes more deliberate and legally guided. We act decisively on internal matters and lead with verified facts against external attacks.

Executive/Employee Misconduct

1. Immediate Internal Action (Engage Legal)
2. Issue Holding Statement
3. Investigate
4. Resolution Statement

Critical Rule
DO NOT defend the accused, dismiss allegations, or comment on specific personnel matters before an investigation is complete.

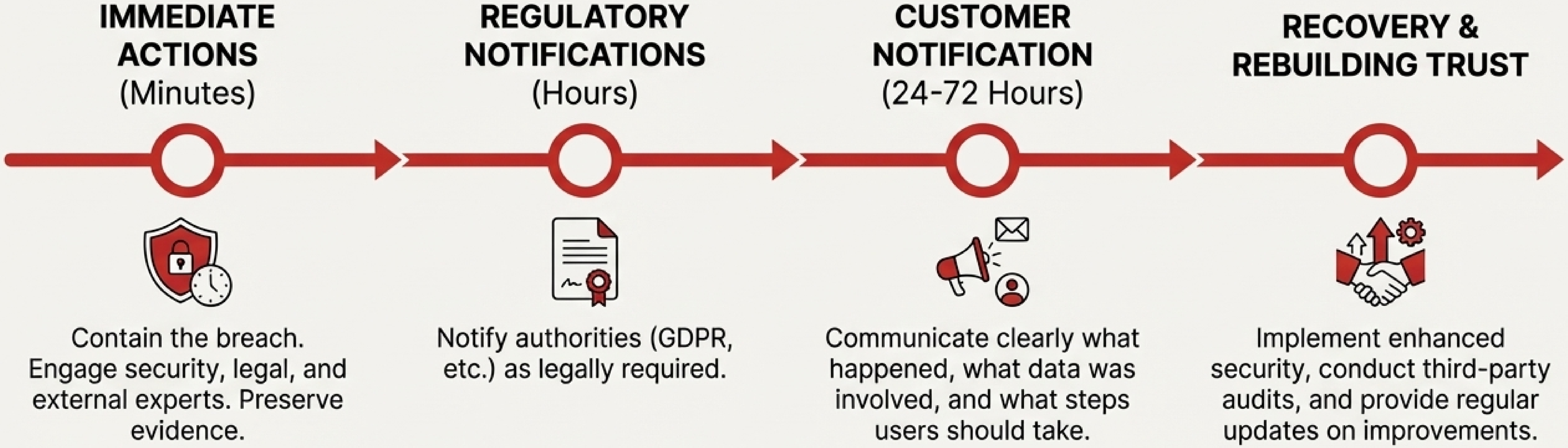
External Attack / Misinformation



Key Principle
Lead with facts, not emotion. Correct once, clearly, then move on. Stay above the fray.

Responding to a Data Breach or Security Incident (Framework E)

In a security crisis, speed matters, but accuracy and legal compliance matter more. Our response is a highly structured, multi-stage process designed to contain the threat, notify stakeholders, and take full responsibility.



IMMEDIATE ACTIONS
(Minutes)

Contain the breach. Engage security, legal, and external experts. Preserve evidence.

REGULATORY NOTIFICATIONS
(Hours)

Notify authorities (GDPR, etc.) as legally required.

CUSTOMER NOTIFICATION
(24-72 Hours)

Communicate clearly what happened, what data was involved, and what steps users should take.

RECOVERY & REBUILDING TRUST

Implement enhanced security, conduct third-party audits, and provide regular updates on improvements.

Key Principle: Over-communicate with affected users. Rebuild trust through sustained transparency and concrete actions.

Our Communication Toolkit:
The right message for every moment.

We use a suite of pre-approved templates to ensure our communications are fast, consistent, and on-tone. Each template serves a specific strategic purpose in the crisis lifecycle.

Immediate Acknowledgment

Use When:
Crisis detected, investigation underway.

Tone:
Serious, accountable, action-oriented.

Progress Update

Use When:
Investigation ongoing, providing new details.

Tone:
Transparent, detailed.

Resolution Announcement

Use When:
Crisis is over, explaining what was learned.

Tone:
Accountable, forward-looking.

Apology Statement

Use When:
Company is at fault and must take full responsibility.

Tone:
Humble, genuine, accountable. (Key element: No "buts" or blaming).

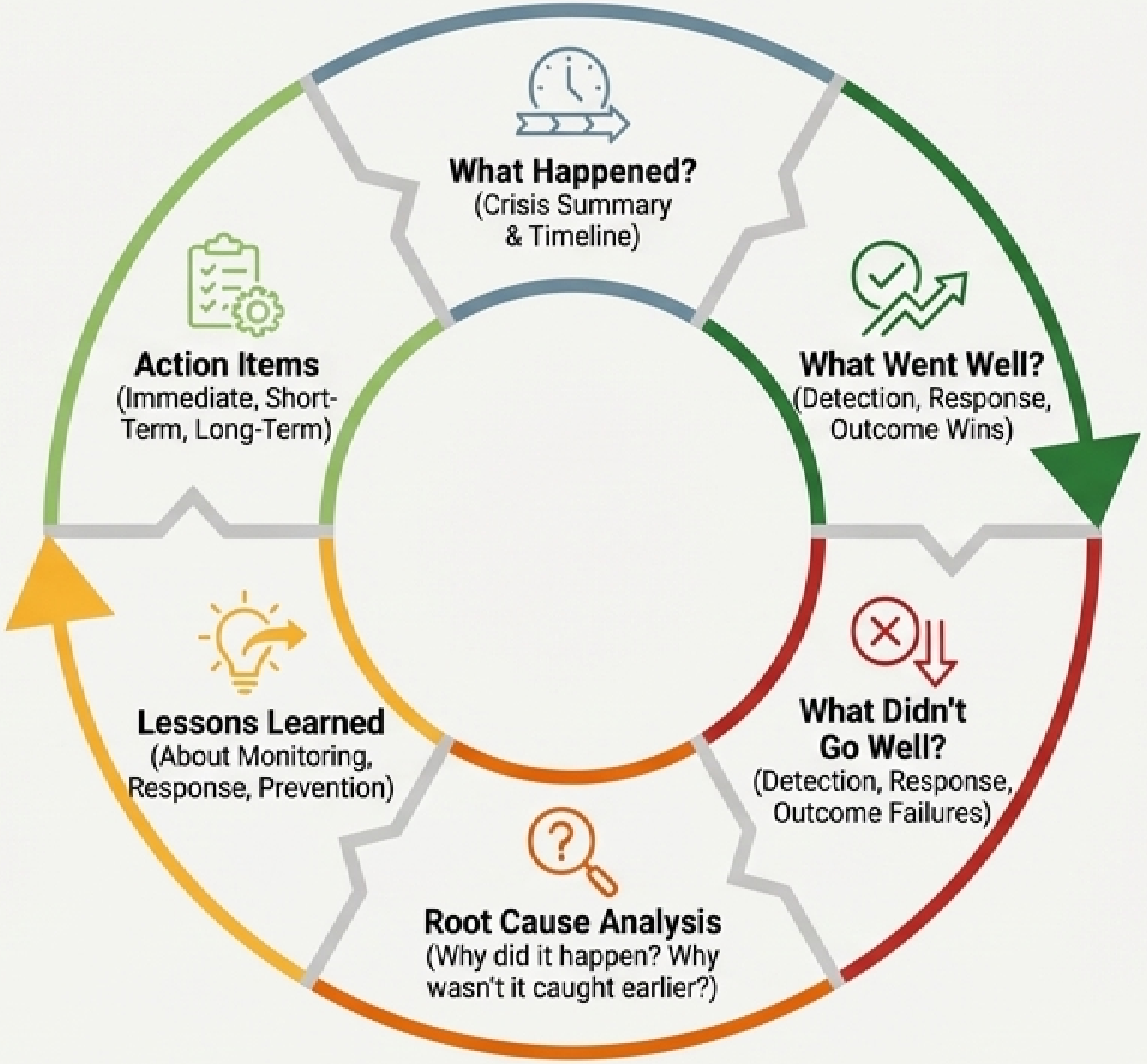
"We Hear You" Statement

Use When:
Acknowledging community feeling on a defended decision.

Tone:
Respectful, firm, open.

Stage 4: Learning – How we get smarter after every crisis.

The crisis is not over when the noise stops. Within 72 hours of resolution, the full response team convenes for a structured **Post-Crisis Review.** The goal is not to assign blame, but to improve our people, processes, and platform.



What Happened?
(Crisis Summary & Timeline)
What Went Well?
(Detection, Response, Outcome Wins)
What Didn't Go Well?
(Detection, Response, Outcome Failures)
Root Cause Analysis
(Why did it happen? Why wasn't it caught earlier?)
Lessons Learned
(About Monitoring, Response, Prevention)
Action Items
(Immediate, Short-Term, Long-Term)

NotebookLM

Measuring what matters: The Crisis Performance Scorecard.

To ensure accountability and track our progress over time, we score every crisis response against 10 core elements. This provides a clear, quantitative assessment of our performance.

Detection Speed.. [___/10]

Severity Assessment... [___/10]

Team Assembly... [___/10]

Internal Communication....................................... [___/10]

Response Quality.. [___/10]

Response Speed.. [___/10]

Resolution Effectiveness...................................... [___/10]

Sentiment Recovery.. [___/10]

Process Adherence.. [___/10]

Learning & Documentation.................................... [___/10]

TOTAL SCORE INTERPRETATION

90-100: "Excellent"

75-89: "Good"

60-74: "Adequate (Needs Improvement)"

<60: "Poor (Requires Overhaul)"

This playbook is a living document.

The best crisis teams are those that learn from every incident and continuously improve their systems. After each crisis, we are committed to updating this playbook with what we’ve learned.

Update

We update templates, adjust alert thresholds, and revise decision trees.

Train

We train the team on new learnings and revised protocols.

Share

We share a case study with the broader organisation to spread knowledge.