OUTLIERS RISK MANAGEMENT CENTRE™

Crisis Management Toolkit™

Lead through acute crises with speed, control and credibility

Executive / Crisis Team / Board · Access Tier T2 · Flagship Edition 2026

Publication-ready resource for the Outliers Resource Library

1. Full Guide

A crisis is an acute, high-impact event that threatens the organisation and demands rapid, coordinated executive response. This toolkit provides a five-stage model, crisis team structure, decision protocols and communications.

The five-stage crisis model

1. Prepare — team, plan, scenarios, training
2. Detect — early warning & activation
3. Respond — command, decisions, containment
4. Recover — restore operations & confidence
5. Learn — post-crisis review & improvement

Maturity model

L1 Fragile	L2 Functional	L3 Disciplined	L4 Strategic	L5 Resilient
Informal / reactive	Basic, siloed	Standardised & governed	Integrated & quantified	Predictive & embedded

2. Templates

2.1 Crisis team & RACI

Role	Responsibility
Crisis Sponsor (CEO/Exec)	Overall command and key decisions
Crisis Manager	Coordinates response and the crisis room
Communications Lead	Internal/external communications
Operations Lead	Operational containment and recovery
Legal/Compliance Lead	Legal, regulatory and reporting obligations
Scribe	Decision and action log

2.2 Crisis activation & severity

Severity	Definition	Authority to activate
Level 1 (Major)	Enterprise-threatening	CEO / Board notified
Level 2 (Significant)	Material but contained	Crisis Manager
Level 3 (Minor)	Localised disruption	Function head

2.3 Crisis communications templates

- Holding statement (first hour)
- Staff notification
- Customer notification
- Regulator notification
- Media statement
- Post-resolution update

2.4 Decision & action log (template)

Time	Decision/Action	Owner	Status
10:05	Activate crisis team (Level 1)	Crisis Mgr	Done
10:20	Issue holding statement	Comms	Done
10:40	Isolate affected systems	IT	In progress

3. Registers

Capture the event in the Incident Register (XLSX); log all crisis decisions in the action log; feed lessons into the Enterprise Risk Register.

4. Checklists

Crisis readiness checklist

- ☐ Crisis plan documented and accessible offline
- ☐ Crisis team and deputies named with contacts
- ☐ Activation triggers and severity levels defined
- ☐ Decision protocol and authorities clear
- ☐ Communications templates pre-drafted
- ☐ Crisis room / virtual bridge ready
- ☐ Simulation exercised in last 12 months
- ☐ Post-crisis review process defined

Governance Structure

Risk is governed through three lines of defence under board oversight:

Layer	Role	Responsibility
Board	Oversight	Approves policy, appetite; oversees the risk profile
Risk / Audit Committee	Focused oversight	Reviews top risks, appetite, assurance
1st line — Management/owners	Own & manage	Identify, assess, control and report risk in operations
2nd line — Risk/Compliance	Oversee & challenge	Set framework, monitor, challenge, aggregate reporting
3rd line — Internal Audit	Assure	Independent assurance over the risk and control system

Reporting Templates

Standard crisis-readiness report structure

- Executive summary & key messages
- Profile vs appetite (RAG)
- Top risks & movement
- KRIs and breaches
- Incidents & losses in period
- Actions & overdue items
- Decisions / escalations sought

KRI reporting table (example)

KRI	Current	Threshold	RAG	Trend	Action
Crisis plan currency	Current	Current	Green	Stable	Maintain
Last simulation	4 mo ago	≤12 mo	Green	—	Schedule next
Open post-crisis actions	2	0	Amber	Down	Close out

Board Reporting Example

Illustrative one-page board summary (replace with live data):

Item	Status	Commentary
Crisis readiness	Green	Plan current; simulation completed 4 months ago
Recent activations	Green	No Level 1 crises this period
Improvement actions	Amber	2 actions from last simulation still open

Decisions sought	—	Note readiness; approve annual simulation calendar

Disclaimer

This toolkit is a professional management resource, not legal, regulatory or audit advice. Calibrate scoring scales, appetite, limits and governance to your organisation, sector and applicable regulation. Sector-specific requirements (e.g. prudential, data-protection, HSE) must be confirmed against current local regulation.