GRCForce

The Incident Response Governance Stack: Readiness Checklist & Simulation Guide

A practical playbook for incident response, crisis command and regulatory notification readiness.

Use this playbook before your next exercise, regulatory review or resilience assurance conversation. It is designed to help CISOs, Heads of GRC, incident leads and senior management test whether the governance above the technical response will hold under pressure.

What is included

- Incident Response Governance Stack Canvas
- Readiness Checklist
- Regulatory Notification Reference
- Incident Severity Classification
- Prioritised Simulation Guide
- Five Questions to Ask in the First Hour
- One Thing You Can Do This Week
- Next Step CTA

One Practical Model for Incident Response, Crisis Command and Regulatory Notification

In a crisis, organisations fall to the level of their preparation.

Most organisations have an incident response plan. Far fewer have tested whether the governance above the technical layer actually works: who has command authority, who communicates externally, who makes the trade-offs between containment and continuity, and whether the regulatory notification window can actually be met.

This playbook is designed to help you answer those questions before you need them.

Use it for:

- Testing whether your incident response plan is operationally realistic.
- Preparing for an NIS2, DORA or sector-specific regulatory incident notification exercise.
- Designing or improving your crisis command structure.
- Planning and scoping a tabletop or simulation exercise.
- Reviewing post-incident governance actions after a real event.
- Assurance conversations with boards, clients or regulators.

The objective is not to create more documentation. The objective is to know whether your response model would actually hold when the pressure is real.

Page 1 — The Incident Response Governance Stack Canvas

Use this canvas to score your response model across the five layers.

Layer	Prepare	Respond	Learn	Evidence owner	Status
1. Command	Roles named, backups defined, escalation structure documented	Incident lead active, command cadence clear, decision rights understood	Command gaps reviewed after exercises and incidents	Incident Commander / CISO	Green / Amber / Red
2. Decisions	Approval thresholds and backup decision-makers defined	Critical decisions made at the right layer without delay	Decision bottlenecks analysed and corrected	Incident Commander / Executive team	Green / Amber / Red
3. Communications	Internal, client, media and staff templates prepared	Messages approved and issued in the right sequence and channel	Communication delays and confusion captured for improvement	Communications / Legal	Green / Amber / Red
4. Notification	Regulatory obligations, windows, contacts and templates documented	Notification approval chain works under time pressure	Notification failures or delays lead to process improvement	Compliance / Legal	Green / Amber / Red
5. Learning	Post-incident review method and ownership agreed	Evidence gathered during the event to support review	Actions tracked to closure and fed back into the model	GRC / Risk owner	Green / Amber / Red

How to score quickly

- Green: the layer is documented, owned, current, and has been tested.
- Amber: the layer exists but is stale, incomplete, or unclear under pressure.
- Red: the layer is missing, unowned, or likely to fail in a real event.

If you have more than two Red layers, do not wait for the next exercise. Fix the model first.

Page 2 — Readiness Checklist and Notification Reference

1. Command Authority Is Assigned

- [ ] A named individual holds incident command authority at the operational level

- [ ] A senior named individual holds crisis ownership at the executive level
- [ ] Escalation from incident to crisis level is formally documented and understood
- [ ] Backup role-holders are named for all critical response roles
- [ ] The command structure has been tested in the last twelve months

Common failure: Command authority described in a document, but not understood by the people expected to use it.

2. Decision Rights Are Explicit

- [ ] The technical team knows what it can approve without escalation
- [ ] Management knows which decisions require executive involvement
- [ ] Board notification thresholds are documented
- [ ] Payment, shutdown, and major communication decisions have pre-agreed escalation paths
- [ ] No critical decision relies on a single unavailable person

Common failure: The response plan says what should happen, but not who is allowed to decide it.

3. Communications Are Ready

- [ ] Internal crisis communication templates are prepared and accessible
- [ ] Client and partner holding statements exist for likely scenarios
- [ ] Out-of-band communication channels are available if corporate systems fail
- [ ] Media wording exists where relevant
- [ ] The communication approval chain has been tested

Common failure: The first external message is written from scratch under maximum pressure.

4. Regulatory Notification Is Operationally Ready

- [ ] Applicable obligations under NIS2, DORA, GDPR or sector-specific rules are documented
- [ ] Contact details and submission channels are current
- [ ] Templates exist for initial, intermediate, and final reporting where relevant
- [ ] Approval paths are agreed and tested
- [ ] Legal, compliance, communications, and executives know their role in the process

Common failure: Detection is fast, but notification is late because no one owns the approval chain.

5. External Relationships Are Ready

- [ ] External incident response or forensics support is confirmed
- [ ] Legal counsel with incident experience is identified
- [ ] Cyber insurance process and contacts are known
- [ ] PR or crisis communication support is identified where needed
- [ ] Supplier and cloud escalation paths are documented for critical services

Common failure: Critical third parties are called for the first time during the incident.

6. The Model Reflects Operational Reality

- [ ] The plan has been reviewed in the last twelve months
- [ ] The plan reflects current systems, suppliers, and team structures
- [ ] Priority services are clearly defined
- [ ] Key assumptions in the plan have been tested at least once

- [ ] At least one ransomware, one availability, and one notification-pressure scenario are covered

Common failure: The plan still describes the environment as it was two reorganisations ago.

Regulatory Notification Reference

Framework	Initial notification window	To whom	Trigger
NIS2 (EU)	24 hours (early warning)	National CSIRT / competent authority	Significant incident
NIS2 (EU)	72 hours (incident notification)	National CSIRT / competent authority	Significant incident
GDPR Article 33	72 hours	Supervisory authority	Personal data breach with risk to individuals
DORA (EU financial)	4 hours (initial)	Competent authority	Major ICT incident
DORA (EU financial)	72 hours (intermediate)	Competent authority	Major ICT incident
UK GDPR	72 hours	ICO	Personal data breach with risk to individuals
Sector-specific	Varies	Sector regulator	Sector-defined significant event

Action: Confirm which of these apply to your organisation. Document the competent authority contact, the notification channel, and the approval process for each.

Incident Severity Classification

Level	Description	Examples	Response action
Level 1 — Event	Suspicious activity detected, no confirmed impact	Unusual login, failed access attempts, anomalous traffic	SOC investigation, no escalation required
Level 2 — Incident	Control breach confirmed, impact limited and contained	Malware on isolated endpoint, credential compromise without data access	Incident team activation, management notification
Level 3 — Significant	Material impact on systems, services or data	Ransomware deployment, confirmed data exfiltration, extended service outage	Crisis command activation, regulatory assessment required
Level 4 — Crisis	Critical services impaired, major regulatory, reputational or commercial impact	Widespread ransomware, major data breach, multi-system outage	Full crisis command, regulatory notification triggered, executive leadership active

Note: The classification trigger for regulatory notification is usually Level 3 or Level 4. Confirm thresholds with legal and compliance.

Page 3 — Prioritised Simulation Guide

The scenarios most worth testing are usually the ones that make the team most uncomfortable. That discomfort shows where assumptions have not been tested and where the model depends on conditions it may not find.

Prioritise based on your threat model: a manufacturer should test physical security; a SaaS provider should prioritise cloud outage scenarios.

Priority	Scenario	What it tests	Why it matters
High	Ransomware with encrypted backups	Whether recovery survives removal of IT availability	Common serious threat, often reveals false recovery assumptions
High	Data exfiltration with regulatory notification pressure	Whether approval chain and templates are ready	Direct regulatory and reputational exposure
High	Third-party or cloud provider outage	Whether critical services can operate in degraded mode	Growing dependency risk across sectors
Medium	Insider threat with privilege abuse	Whether audit logs, HR, legal, and security coordination are ready	Hard to detect and often politically sensitive

Priority	Scenario	What it tests	Why it matters
Medium	Concurrent failure: cyber plus supply chain disruption	Whether command structure handles multiple crises at once	Good test of resilience limits
Medium	Executive communication failure during a public incident	Whether communication governance survives public pressure	High reputational risk during fast-moving events
Low	Ransomware payment demand	Whether board has a decision framework	Less frequent, but high pressure if it occurs
Low	Regulatory audit during an active incident	Whether organisation can manage parallel demands	Uncommon, but governance-heavy if triggered
Low	Phishing compromising finance team	Whether finance and security respond as one model	Tests business and cyber coordination
Low	Physical security failure at a sensitive site	Whether physical and cyber response are joined up	Useful for firms with sensitive premises or prototype data

Five Questions to Ask in the First Hour

1. What happened? — What has been confirmed so far, and what is still assumed?
2. Is it contained? — Is the threat still active or still spreading?
3. Who needs to know? — Which internal and external parties must be informed now?
4. What is the priority service? — Which critical service needs to be protected first?
5. What is the clock? — Which regulatory, contractual, or commercial deadlines are already running?

One Thing You Can Do This Week

Test your notification approval chain. Pick a plausible incident scenario. Ask your response team: if this happened at 4 PM on a Friday, who would approve the initial regulatory notification? Is that person available? Is there a backup? Is the template ready? Where is it stored if the corporate network is down?

If the answer to any of those questions is uncertain, you have found a gap worth closing.

Next Step

Use this playbook before your next exercise, regulatory review, or resilience assurance conversation.

If the canvas shows too many Amber or Red layers, or if your organisation has not run a realistic scenario in the last twelve months, GRC Force can support a focused Incident Response Readiness Review covering:

- Command structure and decision rights.
- Regulatory notification readiness.
- Communication model and templates.
- Simulation design and facilitation.
- Post-exercise governance and action planning.

Start here: https://grcforce.com/en/?utm_source=linkedin&utm_medium=social&utm_campaign=linkedin-week5-incident-response-governance-stack-2026-07&utm_content=lead-magnet-final-contact#contact

GRC Force — Practical governance, risk and compliance advisory for organisations that need to hold up under pressure, not just on paper.