Cybersecurity Incident Response TTX
2 July 2026

1. Exercise Framework & Objective

This exercise is designed to simulate a high-consequence operational disruption to evaluate the strategic decision-making, regulatory compliance posture, and inter-agency coordination of the South East Energy Agency (SEEA) Board. The goal is to move beyond routine operational updates and test how the Board exercises its corporate governance, fiduciary duties, and public accountability under severe time constraints and incomplete information. Furthermore, it will evaluate the Board's capacity to recognise systemic risks to Critical National Infrastructure (CNI) and formulate post-incident organisational resilience strategies.

2. Agenda

- [00:00 - 00:15] **Briefing**: Ground Rules & Regional Risk Landscape
- [00:15 - 00:45] **Inject 1**: Operational Interruption & Trusted System Data Breach
- [00:45 - 01:25] **Inject 2**: Financial Gridlock, NIS2 Accountability & Public Fallout
- [01:25 - 01:50] **Board Strategic Deliberation & Action Matrix Plan**
- [01:50 - 02:00] **Chairperson's Wrap-Up & Core Recommendations**

3. The South East Strategic Context

The SEEA operates as a critical institutional intermediary driving the regional energy transition across Carlow, Kilkenny, Wexford, and Waterford. The agency manages sensitive energy performance metrics, coordinates massive retrofitting deployment programmes, and processes millions in capital grant funding pipelines via the Sustainable Energy Authority of Ireland (SEAI). Crucially, SEEA serves as a trusted municipal hub, maintaining direct data links and shared digital pathways with all four partner Local Authorities. Because the agency sits at the intersection of public funding, local authority infrastructure, and private contracting supply chains, any compromise to its digital integrity instantly poses a systemic risk to the wider public sector network and regional climate targets.

3.1. The Modern Regulatory Environment (2026)

As a public body playing a pivotal role in regional infrastructure coordination, the SEEA operates under enhanced statutory responsibilities. The Board must navigate:

- Strict Statutory Reporting Timelines under the General Data Protection Regulation (GDPR) and the Irish Data Protection Act 2018, the agency must comply with mandatory reporting timelines enforced by the Data Protection Commission (DPC).
- Evolving corporate liability thresholds mandated by the national transposition of the Directive (EU) 2022/2555 Network Information Security (NIS2) (National Cyber Security Bill 2026), which places direct accountability on corporate boards for the cyber resilience of essential and critical entities.

4. Board Persona / Role Matrix

Rather than using technical IT roles, Board members should approach the scenario through their authentic professional governance mandates:

- **The Chairperson & CEO**: Leading regional strategic positioning, coordinating directly with the Department of the Environment, Climate and Communications (DECC), and maintaining ministerial communications.
- **Local Authority Representative Directors (Carlow, Kilkenny, Wexford, Waterford Councils)**: Managing localised public fallout, localised council resource impacts, and civil defence intersection points.
- **Audit, Risk & Legal Committee Chair**: Navigating strict compliance, data protection reporting timelines under the Data Protection Commissioner (DPC), and identifying corporate liability vulnerabilities.
- **Communications & Stakeholder Lead Director**: Directing crisis PR to mitigate severe reputational damage among trusted community groups, businesses, and Sustainable Energy Communities (SEC).

5. Ground Rules

1. **Do Not Read Ahead**: This document contains only your briefing context. Do not attempt to guess or preempt the technical injects.
2. **Accept the Premise**: The scenario constraints are realistic. Accept them as facts rather than fighting the technical nuances.
3. **No Solo Decisions**: No single director holds full control; an effective response depends entirely on integrating your legal, financial, communication, and local authority perspectives.

6. Scenario: Trusted Intermediary

6.1. Inject 1

The Integrity Breach (30 Mins)

- **Incident**: On a morning during peak grant-application cycles, SEEA regional energy monitoring, auditing database, and ISO 50001 Energy management systems - client management cloud environments are locked by an external ransomware intrusion.
- **Escalation**: The cyber threat actor targets the agency's data connections linking local authorities and the Sustainable Energy Authority of Ireland (SEAI). Proprietary financial records, localised commercial infrastructure audits, and residential upgrade pipelines across all four counties are actively compromised.
- **Strategic Board Dilemma**:
    1. At what exact point does an infrastructure operational crisis transition into a mandatory Board-level data breach notification?
    2. How does the agency protect its position as the region's Trusted Intermediary if client infrastructure audits are leaked or held hostage?

Notes:

6.2. Inject 2

Financial Freeze & Regional Contagion (40 Mins)

- **Escalation**: Capital project pipelines halt. Over €20 million in pending regional grant funding and capital projects (including joint local authority climate initiatives and community retrofits) are frozen mid-transaction due to compliance holds.
- **Public Crisis**: Local media outlets begin reporting that multi-million euro clean energy project delays are threatening county-level carbon emission targets. Concurrently, the NCSC suggest that the breach targets broader weaknesses across European municipal support networks.
- **Strategic Board Dilemma**:
    1. How does the Board manage the sudden legal and financial liability of stalled community and commercial contractor works across the South East?
    2. How should local authority directors insulate their respective County Councils from systemic network contagion risks?
    3. What are the downstream impacts of this disruption on regional Critical National Infrastructure (CNI) (e.g., smart grid integration, localised grid stability), and how does the Board define its minimum viable operational resilience during a prolonged outage?

Notes:

7. Board Deliverables (The Output)

By the conclusion of the 2-hour exercise, the Board will ratify a 4-Point Strategic Response Directive:

1. **The Legal & Regulatory Compliance Line**
    - An explicit consensus on notification steps regarding national frameworks (e.g., NCSC, SEAI, and the DPC) under Irish and European legal constraints.
2. **Financial & Business Continuity Plan**
    - An approved emergency framework to address frozen grant pipelines, protect local authority co-funders, and ensure ongoing regional project management viability.
3. **Joint Stakeholder Communication Strategy**
    - A unified public and internal communications protocol to manage information gaps, address community panic, and preserve institutional trust across the public and private sectors in the South East.
4. **Post-Incident CNI & Operational Resilience Framework**
    - A forward-looking governance strategy mapping SEEA's digital dependencies on Critical National Infrastructure. This must outline the post-incident architectural upgrades and resource allocations required to guarantee regional climate infrastructure resilience against future cascading failures.

Notes: