

PUBLIC SAMPLE / FICTIONAL ENGAGEMENT

Readiness exercise and improvement plan

Prepared for Northline Studio

A fictional organization used solely to demonstrate reporting. No client information, live indicators or actual evidence is included.

Report reference	Reporting cutoff	Intended reader
TRN-001	07 Oct 2026 / 23:59 UTC	Executive sponsor, marketing, IT and support leads

EXECUTIVE ASSESSMENT

In a fictional 90-minute tabletop, participants recognized the simulated role-loss incident but did not immediately identify who could authorize platform reporting. The group produced a usable situation summary, while the evidence-transfer route and deputy coverage remained unclear. Scores reflect observed exercise behaviors, not certification or real-incident performance.

DECISION REQUESTED

Appoint reporting authority and deputies, approve a secure evidence route, and repeat the two incomplete decisions in a shorter follow-up exercise.

Inside this report

02 Scope and method / 03 Findings / 04 Evidence and chronology / 05 Action plan / 06 Handover and limitations

Illustrative format only. Final scope, response cadence, authorized recipients and local requirements are agreed for each engagement. No service outcome or legal determination is promised.

02 / HALDEN INTELLIGENCE

Scope, coverage & method

AGREED QUESTION AND COVERAGE

Facilitated tabletop for six role representatives using a social-account takeover scenario. Evaluate escalation, authorization, evidence handling, communications and recovery readiness. No live phishing, access changes or customer messages.

OUTSIDE THIS ASSESSMENT

Employee performance ranking, certification, technical penetration testing, production response-time commitments and conclusions about behavior outside the exercise.

Asset / record	Accountable owner	Coverage
AS-01 / Exercise group	Sponsor	Six role representatives; no personal scores
AS-02 / Playbook	Operations lead	Draft escalation and reporting process
AS-03 / Scenario injects	Facilitator	Three fictional developments over 90 minutes

REPORTING METHOD

Define authority and scope; register supplied material; separate direct observations from statements; assess alternative explanations; review findings against source limitations; assign actions with acceptance evidence.

CONFIDENCE IS NOT SEVERITY

High: the cited material directly supports this narrow observation. Moderate: the observation has support but an important gap remains. Low: it is a lead or statement requiring corroboration. Confidence never establishes identity, intent or legal liability.

PRIORITY AND TIME

High: address promptly because of potential material harm or dependency. Medium: assign a near-term owner. Low: review in the agreed cycle. These are qualitative priorities, not CVSS ratings. All times are UTC; event times and receipt times are distinct.

03 / HALDEN INTELLIGENCE

Findings & interpretation

F-01 / HIGH PRIORITY / HIGH CONFIDENCE

Reporting authority is ambiguous

Observation. At minute 25, marketing and IT each assumed the other could approve a platform report. The playbook did not resolve the question.

Why it matters. An actual incident could be delayed or produce conflicting submissions.

Alternative / uncertainty. Existing informal practice may work for experienced staff but was not evident to the exercise group.

Recommended action. Name one accountable role, a deputy and a written approval record for reporting.

Evidence: E-01, E-02

F-02 / HIGH PRIORITY / MODERATE CONFIDENCE

Evidence transfer route is not operationally clear

Observation. Two participants proposed sending captures through ordinary email. No approved secure upload destination could be identified during the exercise.

Why it matters. Sensitive material could be dispersed across channels without controlled access or retention.

Alternative / uncertainty. A secure tool may already exist but lack a clear owner or onboarding instructions.

Recommended action. Select the authorized channel and rehearse access using harmless sample files.

Evidence: E-01, E-03

F-03 / LOW PRIORITY / HIGH CONFIDENCE

Situation summaries separate facts from unknowns

Observation. The final group summary explicitly separated role loss from unconfirmed attacker identity and did not promise restoration.

Why it matters. This behavior supports clearer decisions and reduces misleading communications.

Alternative / uncertainty. Performance under a scripted scenario may not generalize to an unplanned event.

Recommended action. Retain the summary structure in the playbook and include it in the follow-up exercise.

Evidence: E-03

04 / HALDEN INTELLIGENCE

Evidence & chronology

Evidence register

ID / source	Receipt time (UTC)	Known limitation
E-01 / Fictional facilitator observation log	2026-10-05 10:30 UTC	Observations, not a recording or individual appraisal
E-02 / Fictional draft escalation playbook	2026-10-04 12:00 UTC	Version used in exercise only
E-03 / Fictional group outputs and debrief	2026-10-05 11:00 UTC	Self-reported confidence is not measured competence

Event chronology

Event time (UTC)	Recorded event	Source
05 Oct / 09:00	Role-loss scenario introduced	E-01
05 Oct / 09:25	Reporting authority decision stalled	E-01
05 Oct / 10:30	Exercise ended; improvements agreed in debrief	E-03

HANDLING AND PROVENANCE

The entries above are invented descriptions, not evidence attachments. In a real engagement, assign a unique evidence ID; record collector, authority, source, collection and receipt times, method and limitations; retain the original in approved storage; and log access, transformations and transfers. Calculate digests on actual files where appropriate. Never invent a digest or custody event.

SOURCE BOUNDARIES

A screenshot can support what was visible in that copy. It does not, on its own, prove origin, completeness, authorship or the full history of an event. Preserve contradictions and distinguish client-reported events from independently verified observations.

05 / HALDEN INTELLIGENCE

Action plan & service register

When	Owner	Completion evidence	State
Within 7 days	Executive sponsor	Approve reporting owner and deputy	Open
Within 14 days	IT + privacy lead	Demonstrate approved evidence transfer with test data	Open
Within 21 days	Operations lead	Issue playbook revision and record acknowledgement	Planned
Within 30 days	Facilitator	Retest incomplete decisions with changed scenario	Planned

Observed exercise rubric

Capability	Score / 2	Observed basis
Escalation	2	Correct internal lead identified
Authorization	0	No decision owner established
Evidence handling	1	Need recognized; route not demonstrated
Communications	2	Facts and uncertainty separated
Deputy coverage	0	Absent role had no agreed alternate

0 = not demonstrated; 1 = partial; 2 = demonstrated in this exercise. The 5/10 total is a local exercise result, not an industry benchmark.

CLOSING AN ACTION

Record the actual completion time, responsible person and evidence reference. A request, recommendation or platform submission is not completion. Keep unresolved dependencies visible and agree the next review date with the client.

Limitations & handover

LIMITS ON RELIANCE

A single facilitated session cannot prove operational readiness. Follow-up closure requires observable evidence, not attendance alone.

DISTRIBUTION AND RETENTION

This fictional sample is public. A live report requires an approved recipient list, secure delivery method, retention schedule and disposal owner agreed with the client and, where relevant, counsel. Do not place real evidence or personal data in public website assets.

Release checklist for a live engagement

Required check	Record to complete before issue
Authority and scope	Approved instruction reference and authorized assets
Analyst and peer review	Named preparer, reviewer, review date and corrections
Client decisions	Decision owner, accepted actions and unresolved objections
Delivery and acceptance	Approved recipients, transfer receipt and acceptance date
Follow-up and retention	Next review, retention basis and disposal responsibility

These fields are deliberately unsigned. No real review, instruction, client approval or evidence transfer is represented by this sample.

Method references

Background guidance only; these publications do not validate fictional findings or certify this report. Apply current platform procedures and engagement-specific legal advice separately.

NIST SP 800-61 Rev. 3 — Incident Response Recommendations and Considerations for Cybersecurity Risk Management (2025)
<https://csrc.nist.gov/pubs/sp/800/61/r3/final>