

BUILD THE WHOLE STORY



SITUATION

Describe the incident, confirmed impact, uncertainty, urgency, affected services and legal constraints.



TASK

State your role in the incident structure, delegated workstreams, specialist inputs and authorisation boundaries.



ACTION

Explain evidence handling, prioritisation, analysis, coordination, challenge, communication and recovery decisions.



RESULT

Show containment or recovery, evidential limitations, improvements, exercises and later assurance.



PRACTITIONER

Investigate and escalate

SHOW: hands-on response to routine incidents with limited supervision; secure evidence handling; use of playbooks; recognition of common patterns; objective analysis; clear escalation when complexity exceeds authority.

EXAMPLE: investigated unusual authentication activity. Acquired identity and application logs through approved channels, built a timeline, worked with identity and application specialists, separated confirmed facts from assumptions and documented telemetry gaps. Recommended containment to the incident lead.

RESULT: compromise was limited to one confirmed account, subject to stated limitations. Sessions were revoked, credentials reset and stronger authentication enabled.

PROVE IT

A later exercise confirms that analysts can retrieve the required records.

PRINCIPAL

Coordinate complex response

SHOW: independent incident coordination, an action plan, named workstream leads, prioritisation under pressure, senior communication and balanced containment and recovery. Explain how advice remained objective and within executive authority.

EXAMPLE: led technical response to ransomware. Delegated host, identity, network and recovery work; maintained situation reports and a decision log; prioritised privileged access, persistence and recovery integrity; challenged premature restoration until an identity dependency was validated.

RESULT: priority services restored without confirmed reinfection. Separate administrator identities, emergency credential rotation and security checks before reconnection were introduced.

FOLLOW UP

The next exercise meets recovery objectives and validates controls before reconnection.

CHARTERED

Direct significant incidents

SHOW: strategic leadership across organisations and complementary disciplines. Delegate to specialists, review outputs, resolve conflict, communicate with all levels, manage legal and public-interest direction, and enable authorised collective decisions under uncertainty.

EXAMPLE: established strategic, tactical and technical groups during a nationally significant incident. Required evidence, confidence, dependencies and residual risk in recommendations; integrated specialist outputs; presented restoration options; ensured executives authorised residual risk.

RESULT: essential services restored under monitoring, temporary governance became permanent, supplier responsibilities clarified and multi-agency exercises tested the model.

SUSTAIN IT

Repeated exercises and assurance reviews show sustained multi-agency improvement.

TURN "IMPROVED" INTO VERIFIABLE EVIDENCE

WEAK

"The incident was resolved and national resilience improved."



SUBSTANTIATED

Strategic, tactical and technical roles were incorporated into the permanent framework with named decision authorities. Later exercises measured partner notification, governance mobilisation, containment and production of a common operating picture; failures received owners and were retested.

THE EVIDENCE TEST

A result is strongest when the change is owned, checked and sustained.

1

WHAT CHANGED?

Control or method

2

WHO OWNED IT?

Test lead + action owner

3

HOW CHECKED?

Retest or peer review

4

WHAT RESULT?

Attack path closed

5

SUSTAINED?

Later QA sample