

BUILD THE WHOLE STORY



SITUATION

Describe the service, estate, operational issue, affected controls, dependencies and availability constraints.



TASK

Explain your role, operational ownership, specialist teams, delegated checks, change authority and risk owner.



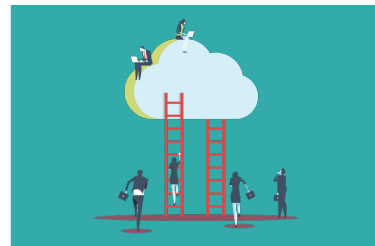
ACTION

Show analysis across logs and systems, secure change, collaboration, prioritisation, compensating controls and assurance.



RESULT

State what operated differently, how it was tested, service impact, exceptions and continued review.



PRACTITIONER

Operate securely

SHOW: hands-on monitoring, configuration and maintenance within approved procedures; understanding of IAM, networking, virtualisation, cloud, evidence handling, SIEM/XDR and change control.

EXAMPLE: investigated privileged sign-ins from unmanaged devices. Correlated identity events, device compliance and support schedules; worked with the identity administrator; tested conditional access in a non-production group; confirmed emergency exclusions and rollback; obtained change approval.

RESULT: routine privileged access required a compliant device and stronger authentication. A controlled test generated the expected SIEM alert and the SOC followed the revised triage procedure.

PROVE IT

Access review and controlled testing verify both control and response.

PRINCIPAL

Lead operational improvement

SHOW: oversight across interconnected systems, adaptation of operational processes, threat-informed prioritisation, resource management, coaching and collaboration with service owners, cloud, suppliers and change management.

EXAMPLE: led vulnerability and configuration improvement across cloud, endpoints and a managed network. Linked assets, findings, exceptions and service criticality; delegated reconciliation; used exploitability, exposure and consequence; established weekly decisions for change, mitigation or escalation.

RESULT: every critical item had an owner, treatment and review date; the greatest exposure was mitigated before patching and then closed through formal change.

FOLLOW UP

Quarterly reviews and assurance confirm decisions and correct authority.

CHARTERED

Transform secure operations

SHOW: strategic integration of SOC, identity, cloud, network, vulnerability, configuration, change and incident processes. Delegate technical design, set outcomes, manage resources and budgets, establish governance, commission independent testing and develop capability.

EXAMPLE: replaced separate priorities and alert-volume reporting with common outcomes for ownership, logging, privileged access, vulnerability treatment and escalation. Specialist leads designed controls; exercises tested hand-offs; options stated threat evidence, business impact and compensating controls.

RESULT: reporting showed service exposure and control effectiveness, priority services achieved defined coverage, exceptions were governed and external assurance identified remaining gaps.

SUSTAIN IT

Six-month and annual reviews drive tuning, supplier obligations and training.

TURN "IMPROVED" INTO VERIFIABLE EVIDENCE

WEAK

"Monitoring, vulnerability management and resilience improved."



SUBSTANTIATED

Defined logging and privileged-access controls were implemented for priority services. Controlled tests confirmed that non-compliant access generated alerts, critical weaknesses had named treatment routes, and exercises tested hand-offs between SOC, identity, network and recovery teams. Follow-up reviews drove further tuning.

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