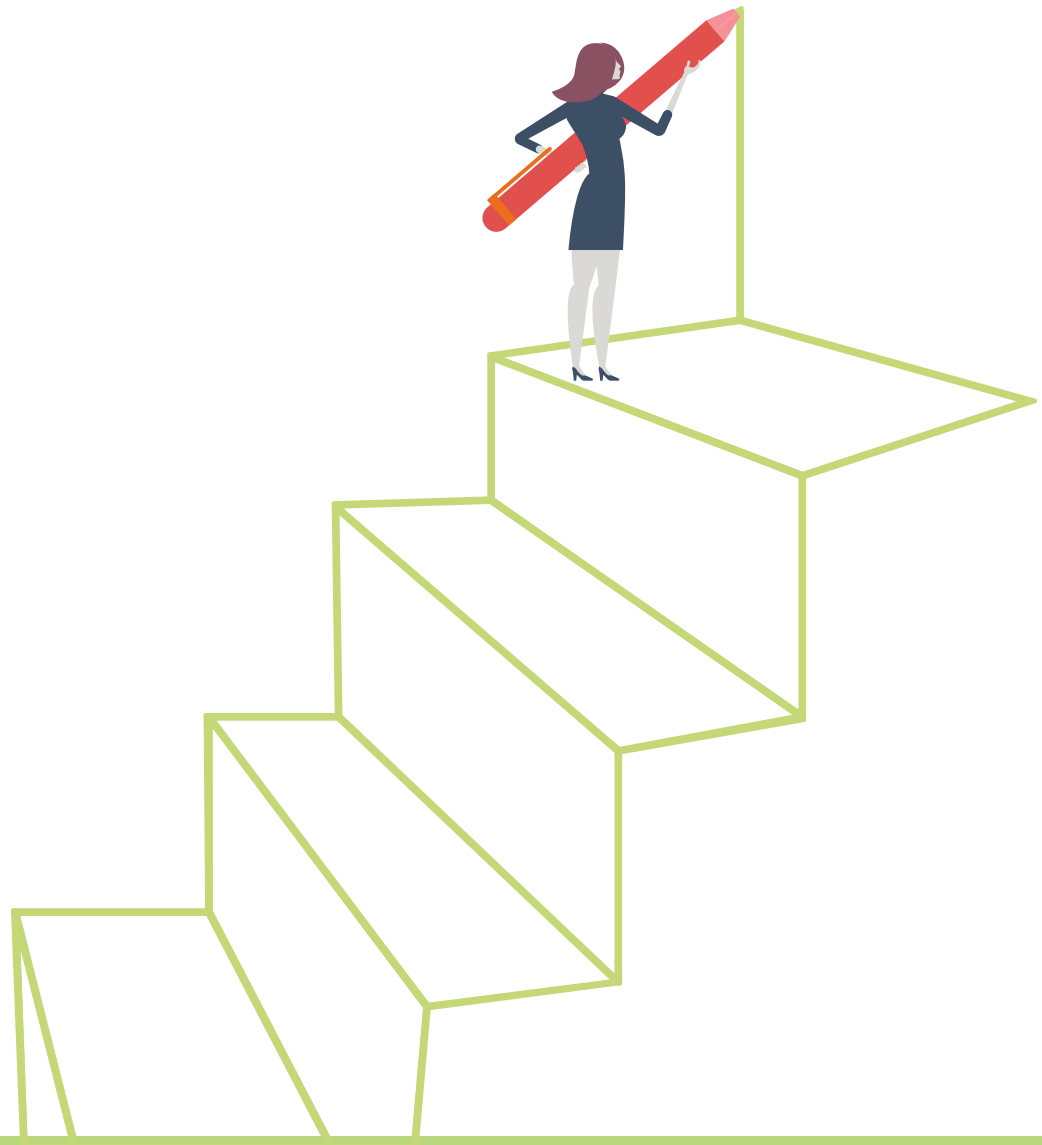
Licensed Body

UK CYBER SECURITY COUNCIL®



CONTENTS

WRITING EVIDENCE THAT DEMONSTRATES YOUR PROFESSIONAL COMPETENCE

Applying for a professional title is not about listing responsibilities, qualifications or technologies you have used. Assessors need evidence of how you applied your knowledge, judgement and professional skills in real situations.

This guide explains how to use the STAR approach - Situation, Task, Action and Result - to structure strong evidence while protecting sensitive information. The examples are anonymised and adapted from genuine application patterns. They are models of structure and evidential depth, not wording to copy. Applicants must use their own verifiable experience.

Important: "weaker evidence" describes wording that gives an assessor insufficient evidence. It does not imply that the applicant, the work, or the application outcome was weak.

SPCC v4.2 context

The UK Cyber Security Council Standard for Professional Competence and Commitment, version 4.2, sets the overarching competence and commitment expectations for Practitioner, Principal and Chartered registration. The examples below use the SPCC progression as a level check, while remaining grounded in the relevant specialism. Applicants should map each example to the precise competence statements requested in their application form.

THE STAR APPROACH: SHOWING YOUR CONTRIBUTION

Strong applications help assessors understand the professional context, your personal responsibilities, the decisions you made, how you worked with others, the outcome achieved and how success was verified. A common weakness is describing activities rather than demonstrating professional judgement, responsibility and impact.

Situation

Explain the professional context, why it mattered, the scale of the work, and the factors that made it sensitive, uncertain or complex.

Task

Explain your personal responsibility and how it sat within the wider delivery. Identify the team, partners or governance groups involved; what you owned; what you delegated; where you collaborated; who directed or authorised the work; and which decisions remained outside your authority. This is especially important at Chartered level, where evidence should demonstrate leadership through others rather than suggesting the applicant operated alone.

Action

Explain what you personally did and how those actions contributed to the broader delivery. Include your analysis and decisions, but also show how you allocated work, collaborated with peers and specialists, took direction from authorised leaders, integrated others' outputs, resolved disagreements and assured delivery. At Chartered level, the evidence should show how personal leadership enabled collective performance and defensible organisational decisions.

Result

Explain what changed, how the change was verified, and how your contribution affected the team, organisation or profession. Avoid unsupported claims such as "security improved". Refer to retesting, audit, exercises, risk decisions, performance measures, adoption, feedback or recurring follow-up activity.

Follow-up and continued improvement

Where follow-up occurred, include it. For Principal evidence this demonstrates that improvement extended beyond project closure. For Chartered evidence it is often critical because it shows sustained governance, assurance, learning and institutional change.

DEMONSTRATING EXPERIENCE WITHOUT DISCLOSING SENSITIVE INFORMATION

Certain organisational, operational and technical details have been anonymised or omitted because of legal, contractual or security obligations. The example accurately reflects my responsibilities, collaborative contribution, decisions and outcomes. The core claims can be verified by an authorised referee or attestor where appropriate.

Anonymise the organisation, system, incident and exact figures where necessary, but retain meaningful evidence of scale, complexity, personal accountability, wider team involvement, decision-making, standards, impact and verification. Never invent metrics. If exact figures cannot be disclosed, use accurate relative wording or describe the verification mechanism.

Instead of naming an organisation, system or supplier, describe its function and significance. Instead of publishing an exact vulnerability or attack path, describe the control weakness, authorised validation and business consequence. Instead of identifying a threat actor or incident, describe the observed capability, confirmed impact, evidential limitations and response decisions. Instead of saying "security improved", state the control implemented, who owned it, how it was tested and whether later review showed that the improvement was sustained.

Examples of safer wording

Certain organisational, operational and technical details have been anonymised or omitted because of legal, contractual, regulatory, classification or security obligations. The example accurately reflects my responsibilities, the contribution of the wider team, the work I delegated, the direction and authority under which I operated, the decisions I made and the outcomes achieved. I have retained sufficient context to demonstrate scale, complexity and professional judgement. The core claims and supporting outcomes can be verified by an authorised referee or attestor, and by protected records where appropriate.

A fuller confidentiality statement

If exact figures cannot be disclosed, do not invent replacements. Use a verifiable range, relative movement or the assurance mechanism instead. For example: "a later access review found no remaining shared privileged accounts", "the next exercise completed the required security checks before reconnection", or "two subsequent governance reviews confirmed that every high risk had an owner and review date".

Use accurate measures and avoid invented precision

Where evidence was incomplete, say so. Distinguish confirmed facts, professional assessment, assumptions and unresolved questions. Explain how uncertainty affected your recommendation, what additional assurance was requested, and who accepted any residual risk. Honest limitation statements often provide stronger evidence of judgement and integrity than unsupported certainty.

Be explicit about uncertainty and limitations

Refer to the existence and purpose of supporting artefacts without reproducing protected content. Suitable evidence may include an authorised referee or attestor, redacted reports, risk records, decision logs, test plans, audit results, exercise records, change tickets, access reviews, remediation trackers, governance minutes, quality-assurance records and subsequent review results.

Use evidence that can be verified without disclosure

State who authorised the work, who owned the business risk, who supplied specialist input, what you delegated, where you collaborated, and which decisions remained outside your authority. This is especially important at Principal and Chartered levels. Strong evidence demonstrates leadership through others and respect for legal, operational and governance boundaries, rather than implying that the applicant acted alone.

Show authority, collaboration and boundaries

You can normally explain the class of weakness, event or governance problem without publishing exploitable detail. Describe the security objective, affected control area, business consequence, analytical method, decision point and validation mechanism. Avoid live indicators, credentials, exact architecture, unpatched product versions, classified capabilities, attribution detail, protected evidence, personal data or information covered by legal privilege.

Describe sensitive technical and operational detail proportionately

Replace names and exact identifiers with accurate functional descriptions. For example, use "a regulated financial services organisation", "a nationally important service", "a distributed cloud platform", "a material supplier", or "a privileged identity service". Replace exact numbers only where necessary, using truthful relative descriptions such as "several business units", "a high-volume service", or "a substantial user population". Do not make the example so generic that the assessor cannot judge significance.

Anonymise identifiers, not competence

Confidentiality does not remove the need for evidence. An assessor should still be able to understand the professional problem, why it mattered, the scale and complexity, your accountability, the contribution of the wider team, the decisions made, the standards applied, the outcome and how that outcome was verified.

Common mistake

Many applications describe "what I do". Strong applications demonstrate "what I did, why it mattered, how I approached it and what happened as a result".

SECURITY TESTING

Specialism contextualisation

Use the Security Testing contextualisation alongside the overarching SPCC. It indicates that evidence should address the lifecycle and scope of testing engagements, relevant legal and regulatory frameworks, business risk, suitable test platforms, accurate and repeatable records, proportionate notification and clear reporting. Principal evidence may be demonstrated through strong leadership of a complex CTL-style engagement. Chartered evidence should show greater breadth, influence and assurance of team quality, but a governance-heavy example should be supported elsewhere by multiple examples of advanced and current technical testing practice.

PRACTITIONER CYBER SECURITY PROFESSIONAL

SPCC v4.2 alignment

SPCC v4.2 level focus: applied professional practice, sound problem-solving, communication, integrity, standards and continuing development. The applicant should show independent delivery within authorised boundaries and appropriate collaboration or escalation.

Good STAR evidence

Situation

I conducted a two-day internal infrastructure assessment for an e-commerce organisation supporting its payment-security obligations. The client wanted to establish whether access from a standard user network could lead to compromise of the cardholder environment.

Task

I owned the technical assessment and reporting within the agreed Rules of Engagement. A client security contact approved higher-risk actions, while an internal reviewer independently checked my high-severity findings. I was responsible for keeping both informed and for pausing where operational risk exceeded my authority.

Action

I confirmed the scope, exclusions and escalation route before connecting. An access control prevented my device obtaining a normal network configuration, but I established that it relied on a replicable identifier and demonstrated an authorised bypass. I combined network enumeration with manual validation of name-resolution, credential and directory-certificate weaknesses. After obtaining standard-user access, I identified a certificate-service misconfiguration that could support privilege escalation. I paused before the higher-impact step, explained the proposed action and safeguards to the client, and continued only after approval. I maintained timestamped records and supplied reproducible evidence to the reviewer. My report separated technical remediation from the executive explanation of the combined attack path.

Result

The client corrected the certificate configuration, hardened name resolution and replaced the ineffective access control. My retest confirmed that the original route from ordinary network access to privileged directory control could no longer be reproduced. The report also supported additional investment in monitoring and technical capacity.

Weaker STAR evidence

Situation: I regularly test client networks. Task: I identify vulnerabilities and write reports. Action: I use Nmap, Nessus and other tools, then tell the client about serious issues. Result: The client improves its security posture.

Why it is weaker

It names tools and routine duties but does not show a specific problem, validation, collaboration, authorisation, judgement or a verifiable outcome.

Weak and substantiated improvement statements

- Unsupported claim "*The client improved its network security*".
- Substantiated statement "*The client corrected the certificate-service configuration, disabled the vulnerable name-resolution behaviour and replaced identifier filtering with authenticated network access control. During retesting, I confirmed that the original privilege-escalation chain no longer worked*".

PRINCIPAL CYBER SECURITY PROFESSIONAL

SPCC v4.2 alignment

SPCC v4.2 level focus: expert practice in complex activity, leadership of delivery, adaptation of methods, management of people or resources, improvement and contribution to the specialism. Principal evidence need not resemble an enterprise-wide programme; a strong CTL-style engagement can demonstrate the level.

Good STAR evidence

Situation

I led a five-day CHECK-style infrastructure assessment for a public-sector client. The scope covered several network segments and a small externally hosted service. Access was delayed on the first morning and one production segment had strict availability constraints.

Task

I was accountable for technical delivery, client liaison and report quality. I delegated defined test areas to two team members according to competence, retained the sensitive production segment myself, and worked under the client's change and escalation authority. I also paired a developing tester with the more experienced team member for controlled knowledge transfer.

Action

I converted the scope into a simple coverage plan showing ownership, dependencies and time limits. When access was delayed, I resequenced the work so the team could begin external and low-risk internal testing without losing a day. I held short technical reviews to combine findings across segments and required independent validation of high-severity issues. A potential privileged attack path crossed two testers' areas; I brought their evidence together, directed limited additional validation and agreed a safe stopping point with the client. I reviewed report wording to ensure the executive summary explained business impact while the technical section remained reproducible. I also gave the developing tester structured feedback on evidence quality and remediation writing.

Result

The team completed all critical scope within the original window, with one lower-risk area recorded for follow-up. The client removed the exposed trust relationship and retesting confirmed the route was closed. The coverage plan and review checklist were reused on later engagements, and the developing tester subsequently led a comparable workstream with normal peer review.

Follow-up and continued improvement

At the next quarterly review, I sampled three later reports and confirmed that each high-severity finding contained independent validation, clear scope evidence and actionable remediation. I updated the checklist where reviewers had interpreted impact inconsistently.

Weaker STAR evidence

Situation: I led a large penetration test. Task: I managed two testers. Action: I assigned work, held meetings and reviewed reports. Result: The project finished on time and the client was satisfied.

Why it is weaker

It does not show how work was delegated, how constraints were managed, what technical judgement was exercised, or whether the applicant improved team capability or delivery quality.

Weak and substantiated improvement statements

- Unsupported claim *"I improved the quality of testing"*.
- Substantiated statement *"I introduced a coverage plan and independent review checklist for high-severity findings. The process prevented one unverified automated result from being issued and corrected inconsistent impact wording before release. A follow-up sample of three reports confirmed the checklist remained in use and the evidence standard had been maintained"*.

CHARTERED CYBER SECURITY PROFESSIONAL

SPCC v4.2 alignment

SPCC v4.2 level focus: acknowledged expertise, leadership of significant and complex activity, strategic improvement, influence across organisational boundaries, highest professional integrity and wider contribution. A governance-heavy Security Testing example should be supported elsewhere by multiple examples of advanced, current technical practice.

Good STAR evidence

Situation

I remained an active security-testing practitioner while leading improvement of a consultancy's testing service across web, infrastructure, cloud and operational technology. Client reports varied in quality, senior testers were repeatedly drawn into late-stage corrections, and specialist work depended on too few individuals.

Task

I was accountable for the service improvement within direction set by the executive team. I continued to lead technically complex assessments, delegated methodology work to senior specialists, collaborated with quality, legal and delivery colleagues, and required practice leads to evidence adoption within their domains. Budget and recruitment decisions remained with the executive sponsor, to whom I presented options and risks.

Action

I reviewed a sample of complex engagements and personally led an advanced multi-domain assessment to test whether the proposed standards remained workable in practice. I established minimum expectations for scoping, attack-path evidence, peer review, severity and client communication, while allowing specialist methods to differ. I delegated technical playbook development to recognised specialists, chaired cross-practice reviews and resolved disagreements through evidence and controlled trials. I introduced progression pathways so developing testers could move from labs, through supervised delivery, to independent assessment. For executive leaders, I reported recurring technical themes, capacity risks and investment choices rather than vulnerability counts. I also took direction from legal and operational authorities when testing constraints affected live or regulated environments.

Result

Over two review cycles, material corrections at final QA reduced, high-severity findings consistently showed independent validation, and two previously single-person specialisms gained additional authorised practitioners. Repeat findings were grouped into shared causes, enabling clients to fund systemic remediation. The service standards were incorporated into contracts, induction and performance review.

Follow-up and continued improvement

I commissioned six-month and annual reviews of report quality, skills coverage and recurring findings. Results informed further training and methodology updates. I shared anonymised lessons at professional events while continuing hands-on advanced testing and technical mentoring.

Weaker STAR evidence

Situation: I have led complex tests for many years. Task: I oversee consultants. Action: I review scopes and reports, provide technical escalation and hold advanced certifications. Result: Clients trust me and return for more work.

Why it is weaker

This shows seniority but not strategic technical leadership, collaborative delivery, delegation, sustained improvement or continuing active practice in Security Testing.

Weak and substantiated improvement statements

- Unsupported claim *"Testing quality and team capability improved"*.
- Substantiated statement *"Final-QA records showed fewer material corrections over two review cycles, every high-severity finding sampled had independent validation, and two specialist areas moved from reliance on one practitioner to at least two authorised practitioners. Six-month and annual reviews confirmed continued use of the standards and drove further methodology updates"*.

INCIDENT RESPONSE

Specialism contextualisation

Use the Incident Response contextualisation to show how SPCC competence appears in real incident work. Evidence may cover incident lifecycle knowledge, use and adaptation of action plans and playbooks, objective decision-making, communication under pressure, confidentiality, legal and regulatory constraints, delegation to complementary specialists, review of their outputs, remediation and improvement. Practitioner evidence may show routine incidents with appropriate escalation; Principal evidence should show independent coordination and guidance; Chartered evidence should show direction across complex incidents, final accountability, cross-disciplinary leadership and strategic improvement.

PRACTITIONER CYBER SECURITY PROFESSIONAL

SPCC v4.2 alignment

SPCC v4.2 level focus: applied investigation, problem-solving, communication, integrity, secure handling and standards within established authority.

Good STAR evidence

Situation

I investigated suspicious authentication activity affecting a business-critical web service. The initial alert did not establish whether the activity was unsuccessful probing or a confirmed account compromise.

Task

I owned the initial analysis and evidence record, working within the incident lead's priorities. Identity and application teams supplied logs and system context. The incident lead authorised containment, while I was responsible for making a clear evidence-based recommendation.

Action

I obtained logs through approved channels and recorded source, acquisition time and retention limits. I built a timeline, compared the activity with the user's established pattern and confirmed a successful authentication followed by access to an unusual function. I prioritised checks for privileged access, additional accounts, persistence and movement to other services. I worked with the identity analyst to validate normal behaviour and with the application owner to interpret events, while documenting telemetry gaps. My update separated confirmed facts, assessment, unanswered questions and confidence. Following approval, the team disabled the account, revoked sessions, reset credentials and applied enhanced monitoring.

Result

The confirmed compromise was limited to one account, subject to recorded logging limitations. Stronger authentication was enabled, and relevant log retention was extended. A later exercise confirmed that analysts could retrieve authentication, session and application records across the complete simulated period.

Weaker STAR evidence

Situation: A client had an incident. Task: I investigated it. Action: I checked logs, found a malicious address and helped secure the account. Result: The attacker was removed and the system became secure.

Why it is weaker

It does not show how compromise was confirmed, how others contributed, what evidence was preserved, what remained uncertain or how the improvement was verified.

Weak and substantiated improvement statements

- Unsupported claim "*Logging and authentication were improved*".
- Substantiated statement "*Stronger authentication was enabled for the service, and identity and application logs were retained for the defined investigation period. A later exercise confirmed that analysts could retrieve the required records across the complete simulated timeline*".

PRINCIPAL CYBER SECURITY PROFESSIONAL

SPCC v4.2 alignment

SPCC v4.2 level focus: leadership of complex response, prioritisation, coordination, senior communication, resource management and planned improvement.

Good STAR evidence

Situation

I led the technical response to ransomware affecting a large organisation's critical services. The method of entry, duration of compromise and trustworthiness of recovery assets were initially uncertain, while operational leaders needed restoration options quickly.

Task

I was accountable for coordinating the technical workstreams and advising the CISO. I delegated host, identity, network and recovery tasks to named leads, collaborated with legal, threat-intelligence and service teams, and worked within strategic priorities set by the executive incident group.

Action

I established twice-daily technical coordination, concise situation reports and a decision log that separated confirmed evidence from hypotheses. I prioritised the earliest confirmed compromise, privileged access, persistence and recovery-asset integrity. Lower-value analysis was deferred where it would not affect immediate containment or recovery decisions. When leaders requested a restoration date, I integrated forensic, threat and service evidence into several options showing operational benefit, confidence, re-compromise risk and additional monitoring. I challenged one proposed rapid restoration because the identity dependency had not been validated, then agreed a staged approach after the responsible service executive accepted the residual risk.

Result

Priority services were restored without confirmed reinfection. Separate administrator identities, stronger privileged authentication and emergency credential-rotation procedures were introduced. Recovery instructions were updated to include dependencies and security checks before reconnection.

Follow-up and continued improvement

In the next exercise, a priority service was restored within its recovery-time objective and remained isolated until identity, endpoint and network checks were complete. Lessons were assigned owners and reviewed by the incident governance group.

Weaker STAR evidence

Situation: I managed ransomware. Task: I coordinated responders and briefed the CISO. Action: I held calls and helped plan recovery. Result: Services were restored and resilience improved.

Why it is weaker

It omits delegation, competing risks, decision authority, the evidence informing recovery and proof that capability improved.

Weak and substantiated improvement statements

- Unsupported claim "*The organisation improved recovery capability*".
- Substantiated statement "*Recovery procedures identified service accounts, infrastructure dependencies, trusted restoration points and mandatory security checks. In the next exercise, the team restored a priority service within the target time and completed identity, endpoint and network validation before reconnection*".

CHARTERED CYBER SECURITY PROFESSIONAL

SPCC v4.2 alignment

SPCC v4.2 level focus: strategic leadership of significant and complex activity, cross-organisational influence, disciplined decision-making under uncertainty, sustained improvement and contribution to the profession.

Good STAR evidence

Situation

I held strategic responsibility during a nationally significant incident affecting essential services. The response involved the affected organisation, government stakeholders, specialist responders, legal advisers, regulators, suppliers and recovery teams. Critical systems had incomplete telemetry, but service decisions could not wait for every forensic question to be resolved.

Task

I was accountable for establishing response governance and a common operating picture. I delegated tactical coordination and technical workstreams to suitably experienced leads, collaborated with legal, regulatory and communications specialists, and operated within strategic public-interest direction. My role was to enable authorised collective decisions, not to substitute for every specialist or accountable executive.

Action

I established strategic, tactical and technical groups with clear decision rights and need-to-know information sharing. I required recommendations to state evidence, confidence, dependencies, operational consequences and residual risk. I directed priority towards privileged control paths, persistence, recovery-asset integrity and consequences for dependent services. Tactical leads integrated technical outputs; I resolved cross-workstream conflicts and presented restoration options against urgency, forensic confidence, re-compromise likelihood and monitoring requirements. Where government or regulatory direction constrained options, I made those dependencies explicit. I ensured executives authorised residual risks and that communications used confirmed, caveated information rather than speculation.

Result

Essential services were restored under enhanced monitoring. The temporary structure became a permanent coordination model with named roles and escalation thresholds. Revised playbooks required confidence ratings and decision logs, and supplier responsibilities were clarified.

Follow-up and continued improvement

Multi-agency exercises later measured notification, governance mobilisation, containment and production of a common operating picture. Actions had owners, deadlines and assurance tests. Results were reviewed at subsequent exercises, and authorised learning was shared through sector forums without exposing the organisation.

Weaker STAR evidence

Situation: I have led nationally important incidents. Task: I was responsible for response and recovery. Action: I led large teams, briefed boards and coordinated government stakeholders. Result: Services were restored and national resilience improved.

Why it is weaker

It asserts scale but does not show delegation, collaboration, strategic authority, decision structures, uncertainty management or sustained evidence of improvement.

Weak and substantiated improvement statements

- Unsupported claim *"Multi-agency response arrangements improved"*.
- Substantiated statement *"Strategic, tactical and technical roles were incorporated into the permanent framework with named decision authorities. Later exercises measured partner notification, governance mobilisation, selected containment actions and agreement of a common operating picture. Failures were assigned owners and retested at the next exercise"*.

GOVERNANCE & RISK MANAGEMENT

Specialism contextualisation

Use the Governance and Risk Management contextualisation to connect the SPCC to business need, governance, risk assessment, treatment and assurance. Evidence should show how assets and consequences were identified with stakeholders, how qualitative or quantitative analysis was used and bounded, how appetite and tolerance affected decisions, and how treatment options were prioritised. Higher-level evidence should show governance forums, competing organisational risks, standards and legislation, business-to-security traceability, selection of effective controls and sustained assurance.

PRACTITIONER CYBER SECURITY PROFESSIONAL

SPCC v4.2 alignment

SPCC v4.2 level focus: applied risk practice, communication, integrity, use of standards, improvement and clear escalation within delegated authority.

Good STAR evidence

Situation

I completed a cyber risk assessment for a new cloud service processing sensitive customer information and permitting administrative access by an external support provider.

Task

I was responsible for analysing risk and proposing treatment before production approval. The service owner owned the business risk, specialists supplied technical and privacy advice, and only the designated risk owner could accept exposure above appetite or tolerance.

Action

I facilitated workshops with the service owner, technical lead, supplier and data-protection representative. I mapped data flows, administrator roles, dependencies, threats, controls and business consequences. Using the approved method, I compared the exposure with the organisation's cyber risk appetite and the service's defined tolerance for outage and unauthorised disclosure. I identified persistent third-party privilege and password-only administration as outside tolerance. I proposed named accounts, stronger authentication, time-limited privilege, supplier assurance and restoration testing. I recorded treatment owners and dates and escalated the residual risk rather than implying that my assessment amounted to acceptance.

Result

Production approval was made conditional on treatment. Shared accounts were removed, and an access review confirmed every privileged account had a named owner and stronger authentication. Quarterly supplier reviews required assurance evidence and remediation status. A restoration exercise identified an undocumented service-account dependency, which was corrected before final approval. The risk owner then accepted the reduced residual risk as within appetite and tolerance.

Weaker STAR evidence

Situation: A cloud service needed a risk assessment. Task: I identified risks and ensured compliance. Action: I reviewed ISO 27001, NIST and GDPR and updated the register. Result: The service became compliant and went live.

Why it is weaker

It does not explain appetite, tolerance, ownership, control selection, collaboration or who accepted residual risk. It also makes an unsupported compliance claim.

Weak and substantiated improvement statements

- Unsupported claim "*Supplier monitoring was improved*".
- Substantiated statement "*Critical supplier reviews were scheduled quarterly and required current assurance evidence, incident contacts and remediation status. Missing evidence and overdue high-risk actions were recorded centrally and escalated to the service risk owner*".

PRINCIPAL CYBER SECURITY PROFESSIONAL

SPCC v4.2 alignment

SPCC v4.2 level focus: expert risk and governance practice, leadership, framework adaptation, management of stakeholders, planned improvement and contribution to organisational capability.

Good STAR evidence

Situation

Different business units used inconsistent cyber-risk definitions. Duplicate records, conflicting ratings and actions without owners limited executive oversight. Technical findings were rarely connected to business services, and there was no consistent forum for decisions above appetite.

Task

I was responsible for designing and piloting a common risk and governance process. Business risk owners retained acceptance authority. I delegated analysis of existing registers to risk analysts, collaborated with audit, legal, technical and service teams, and reported design decisions to the security governance committee.

Action

I reviewed risk registers, incidents and audits and identified confusion between inherent and residual risk, informal acceptance and repeated recording of common weaknesses. I designed a model linking technical findings to services, defining likelihood and impact, requiring evidence for control effectiveness and separating risk owners from action owners. I also established governance: monthly operational reviews, escalation thresholds, formal acceptance records, review dates and a quarterly committee view of risks above appetite. When teams resisted standardisation, I retained mandatory ownership, scoring and escalation while allowing specialist evidence. I trained risk owners and facilitated the first reviews rather than simply issuing a template.

Result

The initial exercise consolidated overlapping records into a smaller set of business-service risks. Every high risk obtained a named owner, and exposures above appetite required a recorded treatment or acceptance decision. The committee identified privileged-access weakness across several services and sponsored an organisation-wide response.

Follow-up and continued improvement

Two quarterly reviews later, no high risk lacked an owner or review date. Internal assurance sampled accepted risks and confirmed that evidence and authority were recorded. Feedback informed updated guidance and refresher training.

Weaker STAR evidence

Situation: Risk management needed improvement. Task: I managed the risk register. Action: I updated risks, attended meetings and advised on ISO 27001. Result: Risk ownership and reporting improved.

Why it is weaker

It does not demonstrate governance design, delegated analysis, committee authority, stakeholder influence, or follow-up assurance.

Weak and substantiated improvement statements

- Unsupported claim "*Risk ownership became clearer*".
- Substantiated statement "*Every material risk was assigned a business owner with acceptance authority, while treatment actions had separate delivery owners and dates. At two subsequent quarterly reviews, no high risk remained without an owner or review date, and internal assurance confirmed that acceptance decisions recorded the correct authority*".

CHARTERED CYBER SECURITY PROFESSIONAL

SPCC v4.2 alignment

SPCC v4.2 level focus: enterprise or sector leadership, integration of cyber risk with organisational decision-making, sustained governance, highest integrity and wider professional influence. This example deliberately avoids relying on a Three-Lines model and instead uses accountable ownership, independent challenge and proportionate external assurance.

Good STAR evidence

Situation

I was appointed to transform cyber governance across an organisation operating in several regulated markets. Business units used different control frameworks, supplier assurance was inconsistent and executive reports counted findings rather than explaining exposure. Assurance was duplicated in some areas and absent in others.

Task

I was accountable for integrating cyber risk with corporate decision-making. I delegated control mapping and supplier analysis to specialist leads, collaborated with business executives, legal, procurement, internal assurance and external assessors, and operated under board-approved objectives. Risk acceptance remained with authorised executives; independent assurance providers retained their objectivity and scope.

Action

I established board-approved cyber risk appetite and tolerances, a common control-outcomes framework and explicit ownership for risks and treatments. Rather than imposing a Three-Lines model, I defined who owned each risk, who delivered controls, who provided internal challenge and where independent external assurance was required. I chaired cross-functional governance and redesigned board reporting around risk movement, exposure above appetite, control effectiveness, evidence gaps and decisions. Supplier assurance was tiered by service criticality, data access and substitutability, with external evidence used where it provided stronger assurance than self-attestation. Investment proposals had to identify the risk addressed, expected reduction, dependencies and verification method.

Result

Every risk above appetite received an executive owner, treatment or acceptance decision and review date. Common evidence requirements removed duplicated requests, while external testing was commissioned where internal evidence was insufficient. Committee records showed investment redirected towards shared identity, logging and supplier weaknesses.

Follow-up and continued improvement

Six-month and annual reviews tested whether treatments reduced exposure. Internal assurance and external assessments identified remaining gaps, which were tracked to closure or formally re-accepted. The model was embedded into policy, planning and supplier governance, and anonymised learning informed wider professional discussions.

Weaker STAR evidence

Situation: I have extensive GRC experience. Task: I was responsible for risk, ISO 27001 and audits. Action: I advised senior management, reviewed policies and maintained registers. Result: The organisation remained compliant and improved its security posture.

Why it is weaker

It lists senior responsibilities but does not show collaborative governance, decision authority, independent assurance, strategic change or follow-up evidence.

Weak and substantiated improvement statements

- Unsupported claim *"The organisation improved supplier oversight and executive reporting"*.
- Substantiated statement *"Critical suppliers were reviewed against defined evidence and remediation requirements, with independent external assurance commissioned where internal evidence was insufficient. Executive reporting showed risks above appetite, control effectiveness and required decisions. Six-month and annual reviews confirmed which treatments reduced exposure and which required further action"*.

SECURE OPERATIONS

Specialism contextualisation

Secure Operations contextualises the SPCC through the end-to-end operation and management of networks, systems and cloud environments. The specialism includes configuration and maintenance, identity and access management, virtualisation, networking and cryptographic protocols, distributed and multi-cloud environments, forensic awareness, malware and attack environments, firewalls, SIEM/XDR, SOC operations, vulnerability management, configuration management, threat intelligence, change control and collaboration across operational and functional teams. Applicants should select evidence that reflects their actual role rather than treating this list as a checklist.

PRACTITIONER CYBER SECURITY PROFESSIONAL

SPCC v4.2 and contextualised level focus

Applied secure operations within established policies and procedures; hands-on monitoring, configuration and maintenance; understanding of system integrity, IAM, virtualisation, networking, distributed environments and evidence handling; use of SIEM/XDR or related technologies; communication and escalation within authorised boundaries; secure change and lifecycle management.

Good STAR evidence

Situation

I supported secure operations for a hybrid organisation using on-premises identity services, cloud applications and managed endpoints. Repeated privileged sign-ins from unmanaged devices were generating alerts, but the existing procedure did not distinguish approved support activity from potentially unauthorised access.

Task

I was responsible for analysing the alerts, maintaining the evidence record and proposing operational improvements. I worked within the SOC lead's priorities, collaborated with the identity administrator and service owner, and used the approved change process. The service owner retained authority for service risk and the change manager authorised production changes.

Action

I correlated SIEM identity events, device compliance information and support schedules. I confirmed that some activity was legitimate but that two privileged accounts could authenticate without the required managed-device condition. I documented the affected accounts, control gap, logging limitations and potential consequences. Working with the identity administrator, I tested a conditional-access policy in a non-production group, confirmed break-glass exclusions and prepared

rollback steps. I explained the proposed change to the service owner in service-risk terms and escalated the residual exception. After approval, the team deployed the policy, rotated affected credentials and added a triage note so analysts could distinguish authorised support windows from anomalous activity.

Result

An access review confirmed that routine privileged access required a compliant managed device and stronger authentication. A controlled test generated the expected SIEM alert when the condition was breached, and the SOC analyst followed the revised triage procedure. The remaining emergency-access exception had a named owner, monitoring requirement and review date.

Weaker STAR evidence

Situation: I monitor alerts. Task: I keep systems secure. Action: I use SIEM and make configuration changes. Result: Monitoring and access security improved.

Why it is weaker

The wording lists routine activity but gives no specific problem, collaboration, change authority, analysis, control validation or evidence of improvement.

Weak and substantiated improvement statements

- Unsupported claim "*Monitoring and privileged access were improved*".
- Substantiated statement "*A conditional-access policy was introduced for privileged accounts, affected credentials were rotated and a controlled test confirmed that non-compliant access generated an alert. A later access review confirmed that the emergency exception had an owner, monitoring requirement and review date*".

PRINCIPAL CYBER SECURITY PROFESSIONAL

SPCC v4.2 and contextualised level focus

Expert operational practice across interconnected systems; oversight of configuration, monitoring and lifecycle processes; development or adaptation of secure operations procedures; effective use of SIEM/XDR, threat intelligence and vulnerability information; leadership of people and resources; collaboration across technical and non-technical teams; planned improvement and assurance.

Good STAR evidence

Situation

I led a three-month improvement to vulnerability and configuration management for a business service spanning cloud workloads, end-user devices and a managed network. Scanner results were duplicated, asset ownership was incomplete and urgent remediation requests conflicted with agreed maintenance windows.

Task

I was accountable for coordinating the operational work and reporting progress to the security governance forum. I delegated asset reconciliation and control checks to two analysts, collaborated with service owners, the cloud team, the managed provider and change management, and worked within risk priorities set by the service executive. Risk acceptance remained outside my authority.

Action

I created a single operational view linking assets, vulnerabilities, configuration exceptions, service criticality and accountable owners. I adapted the prioritisation method so exploitability, exposure and business consequence were considered alongside technical severity. I established weekly triage with named decision points for emergency change, planned remediation, compensating control or escalation. Where a critical update could not be deployed immediately, I brought together vendor guidance, threat intelligence and service-dependency information, recommended temporary access restrictions and enhanced monitoring, and recorded the residual risk. I reviewed analysts' evidence, coached them on distinguishing duplicate scanner results from separate affected assets, and issued concise operational and senior summaries.

Result

Every critical item received an owner, treatment route and review date. Duplicate records were consolidated, and service owners could see which exposures affected their services. The highest-risk weakness was mitigated through restricted access and monitoring before the approved patch window, then closed through the formal change process.

Follow-up and continued improvement

Two quarterly reviews later, no critical item lacked an owner or treatment decision. Internal assurance sampled the process and confirmed that emergency changes, compensating controls and risk acceptances recorded the correct authority. Findings informed updated guidance and analyst training.

Weaker STAR evidence

Situation: Vulnerability management needed improvement. Task: I managed the team. Action: I held meetings, prioritised patches and produced reports. Result: Remediation became faster and risk reduced.

Why it is weaker

It does not explain the operating model, delegation, prioritisation method, change constraints, decision authority or follow-up assurance.

Weak and substantiated improvement statements

- Unsupported claim "*The vulnerability-management process improved*".

- Substantiated statement *"Every critical item was linked to a business service, owner, treatment route and review date. Two later quarterly reviews found no critical item without a decision, and an assurance sample confirmed that emergency changes and risk acceptances recorded the correct authority"*.

CHARTERED CYBER SECURITY PROFESSIONAL

SPCC v4.2 and contextualised level focus

Strategic leadership of secure operations across complex estates; integration of networks, identity, cloud, SOC, SIEM/XDR, vulnerability, configuration, change and incident processes; management of people, resources and high-pressure decisions; cross-organisational influence; proportionate assurance; sustained improvement and contribution to professional practice.

Good STAR evidence

Situation

I was accountable for transforming secure operations across a regulated organisation whose SOC, identity, cloud, vulnerability and service-management teams used separate priorities and metrics. Critical telemetry was inconsistent, configuration ownership was unclear and operational reporting counted alerts without showing service exposure or control effectiveness.

Task

I led the operating-model change under objectives approved by the executive risk committee. I delegated detailed SIEM engineering, identity-control design and configuration-baseline work to specialist leads, collaborated with service executives, architecture, incident response, risk, privacy, internal assurance and strategic suppliers, and retained accountability for integration and operational outcomes. Budget and risk acceptance remained with authorised executives, to whom I presented options, dependencies and residual risks.

Action

I defined common outcomes for asset ownership, security logging, privileged access, vulnerability treatment, configuration control and incident escalation. Specialist leads designed detailed controls within those outcomes. I established cross-functional governance with clear decision rights and required operational measures to show coverage, control performance, unresolved exposure and service impact. I commissioned independent testing where internal evidence was insufficient and used exercises to test hand-offs between SOC, identity, network and recovery teams. When service availability conflicted with rapid remediation, I required options to state threat evidence, business impact, compensating controls, recovery implications and the authority needed. I also established progression routes for analysts and required practice leads to review technical currency and capability coverage.

Result

Executive reporting changed from alert volumes to service exposure, control effectiveness and decisions. Priority services achieved defined logging and privileged-access coverage, critical configuration items had named owners, and material exceptions were formally governed. Exercises demonstrated improved coordination across detection, containment and recovery, while external assurance identified remaining gaps for treatment.

Follow-up and continued improvement

Six-month and annual reviews tested whether improvements remained effective. Results drove further tuning, supplier obligations and training. The operating model was embedded into policy, service onboarding, investment planning and performance review, and anonymised lessons were shared through professional forums.

Weaker STAR evidence

Situation: I am responsible for security operations. Task: I oversee the SOC and infrastructure security. Action: I review dashboards, manage suppliers and advise executives. Result: The organisation's security posture and resilience improved.

Why it is weaker

This lists senior responsibilities but does not demonstrate integrated operational leadership, delegation, decision rights, evidence-based assurance or sustained change.

Weak and substantiated improvement statements

- Unsupported claim "*Operational resilience and SOC performance improved*".
- Substantiated statement "*Executive reporting showed service-level logging coverage, control effectiveness, material exceptions and required decisions. Exercises tested hand-offs between SOC, identity, network and recovery teams; actions had owners and assurance tests. Six-month and annual reviews confirmed which controls remained effective and drove further supplier and training changes*".

FINAL APPLICANT CHECKS

Situation

Is the context specific, meaningful and safely anonymised? Have you explained significance, scale and constraints?

Task

Is your personal accountability clear alongside the wider team, delegated work, collaboration, direction and limits of authority?

Action

Have you shown what you did, what others contributed, how work was coordinated, what you decided, what direction you followed and why?

Result

Have you replaced "improved" with implementation, verification and observable impact?

Follow-up

For Principal and especially Chartered evidence, have you shown sustained review, assurance, learning or institutional adoption?

Level

Does the example demonstrate applied delivery at Practitioner, leadership and improvement at Principal, or strategic and sustained influence at Chartered?

Accuracy and authenticity

Do not copy the examples verbatim. Use your own experience, voice and evidence. Do not invent figures, outcomes or follow-up. If exact data is sensitive, describe the verified change accurately without disclosing protected detail. A referee or attestor should be able to confirm the substance of the claim.

References

UK Cyber Security Council. Security Testing contextualisation, version 2.

UK Cyber Security Council. Incident Response contextualisation, version 2.

UK Cyber Security Council. Cyber Security Governance and Risk Management contextualisation, version 3.

UK Cyber Security Council. Secure Operations contextualisation, version 1.1.

UK Cyber Security Council. Standard for Professional Competence & Commitment (UK CSC SPCC), version 4.2, published October 2024. https://www.ukcybersecuritycouncil.org.uk/base/media/docs/the-uk-csc-spcc-4-2-final.pdf