Completed application form – a perfect example

The following is an example of what good looks like in a completed application form. The individual provided clear, structured STAR evidence appropriate to the level applied for (in this case ChCSP), against each of the professional competencies.

A: Knowledge, Understanding & Experience

A1: Have led, managed, or carried out activities that have a degree of complexity within their Specialism or across a number of Specialisms and understand how skills should be applied across a number of projects and to different environments.

Example: OT Testing for large Fast-Moving Consumer Goods (FMCG) manufacturer

Situation: Company was approached by a large FMCG manufacturer. We were asked to help them identify what assets they had on their operational technology production lines and assess the overall security of the organisation. This included a detailed risk assessment and penetration testing.
Task: I led multiple asset discovery exercises and penetration tests against their production lines. The results of this needed to feed into the detailed risk assessments our Risk team was compiling for the wider business.

Action: Testing in OT environments is complex. There is a generally higher risk of causing costly disruption due to the nature of the equipment within the networks. This is largely due to the use of legacy equipment which expects only given inputs and break if unexpected data reaches them.
I took appropriate precautions when connecting to each production line in line with my specialist training and experience. This included selecting suitable tools for the task based on my knowledge of how different tooling may affect the OT network.

I started by running passive tooling to understand the network and the risks that I was likely to pose to its operations. I progressed to very targeted active techniques against certain low-risk assets in agreement with the system owners. Some of the activities I conducted included:

- Establishing what "normal" looked like on the network.
- Understanding what protocols and devices were transmitting data across the network.
- Understanding what devices were likely to pose the highest risk if they were to receive malformed packets/unexpected data.
- Taking a manual and very cautious approach to probing the network to identify any other devices and attempting to identify any potential routes to other networks/the internet in line with the penetration testing scope.

Result: As a result, the organisation was able to:

- Gain a detailed understanding of what assets they had connected to each production line across their factories.
- Gain an understanding of where potential means to traverse production lines/networks was possible, including where assets had direct internet connectivity.
- Gain an understanding of the physical- and cyber-risks to their business operations.
- Obtain a detailed risk assessment. This helped the organisation to understand where the highest risk failings from a technical and procedural standpoint lay, and what the financial impact of these were likely to be for the business.

The client commissioned us for future engagements.

A2: Applied analytical problem solving in meeting customer / organisational requirements.

Example: Determining alternatives when risks of active testing are too great.

Situation: I was conducting a recent test of a production financial system. Testing indicated that it may be vulnerable to a critical vulnerability.

Task: Verification of the presence of the vulnerability via exploitation posed a real risk of causing a denial-of-service condition for legitimate users of the system. As such, I needed to apply my analytical problem-solving skills to find a different approach to verifying the vulnerability for my customer.

Action: I discussed the risks of exploitation with the client, and agreed with them that active exploitation posed a higher risk than either of us were comfortable with. As such, I used my analytical problem-solving skills to identify two potential alternative methods of verification with them:

- If they had a pre-production system, I could attempt exploitation of that system.
- I could hop on a screen share with them. I could then direct them through various configuration files on the host machine, to verify the exact versions of the technology in use.

Result: We agreed to proceed with the second option. I managed to identify the exact version numbers in use, and check other configuration settings to determine whether their system was vulnerable to the identified issue. I determined that whilst they were indeed running a vulnerable version of the software in question, other configuration settings meant that they weren't vulnerable to the specific exploit I had identified.

As such, I was able to raise an issue in the final report regarding the software version in use but confirm that they were not affected by the currently known vulnerability affecting said software. This helped the customer to better understand their exposure and minimised the risk of me causing an outage on their system, per their customer requirements.

A3: Have led, managed, or coordinated continuous improvement to cyber security.

Example: On a long-term project for a bank, I was embedded in the team developing their commercial online banking platform.

Situation: For a period of approximately 3 years, I was allocated to work with a major bank on a continuous security project. This project helped them with the secure development of their commercial online banking platform.

Task: My primary task with the bank was to conduct the security testing function of their agile development workflow. This included penetration testing any code changes and security fixes which had been implemented in the previous sprint. I was also tasked with conducting code reviews and helping to define security requirements for upcoming changes to the platform and new products and features within the team. This was all part of their continuous development lifecycle.

Action: I fed back any identified security and functional weaknesses I identified within the system, logging defects directly into the bank's bug tracking system. I also attended regular meetings with

key project stakeholders to alert them to the trends I was identifying. I relayed what actions they should be taking to improve the overall security of the software, as well as acting as an expert adviser on the approaches they should be taking with their testing strategy. When identifying security issues, I would provide detailed advice to the development team on the root cause of the defect and the actions they could take to avoid introducing the same defects in future. This was a continuous process with me spending one week a month embedded in the bank's team for about three years.

Result: I identified a clear downward trend in the quantity and types of defects I was identifying throughout the lifecycle of the project. This was backed up by internal data compiled by the bank which showed that security defects were being identified and addressed in a much quicker manner than before my engagement. They also identified a much lower rate of repeat defects as the developers learned from the advice I provided. This demonstrated a continual improvement in their secure development practices. The bank's data also showed a clear reduction in their costs of remediating security defects based on the earlier identification and remediation of the defects.
At each annual contract renewal, I was specifically named by the client as the requested resource. This was due to the real impacts my work was making for the organisation's cyber security. My engagement with the client on their continual improvement only ended due to me changing employers.

B: Communication & Interpersonal Skills

B1: Have the ability to question and listen, summarise and explain cyber security appropriately.

Example: Client Moving Penetration Testing In-House

Situation: In date, a client in the manufacturing sector informed us that they wanted to move their Industrial Control Systems penetration testing in-house to reduce costs.

Task: The client asked for a half-day workshop to allow us to explain the risks and challenges with training up their in-house Operational Technology (OT) team to conduct penetration tests.

Action: Having listened to the client's brief, I broke the workshop into a few key areas:

- Our Experience
- The Key Risks & Advantages of moving testing in-house
- Potential Training Courses

- Further Advice.

Having listened to the client's concerns about the cost of penetration testing, and around them getting trained up suitably, I started by explaining the levels of experience which I ensure our consultants have before letting them loose on an OT network. This includes:

- Having several years of penetration testing experience.
- Dedicated training in ICS.
- A competency sign-off from a suitably qualified and experienced colleague.

This was used to set the groundwork to explain that they couldn't train up their existing OT engineers to be safe and competent penetration testers overnight and without significant initial investment in time and cost.

I questioned the client on their existing knowledge of penetration testing, and then explained the key risks of moving the penetration testing in-house based on this information. Primarily this was that it would not be feasible for their in-house engineers to get the level of skill that dedicated OT penetration testers have in the short timeframes they were requesting. This is due to them also performing other roles in the business. I highlighted that any mistake which knocks production lines offline could be very costly to the business. I explained how good OT penetration testers need to both understand penetration testing tools and techniques and understand how to apply these safely in often-unstable production OT environments.

I explained that if their OT engineers could learn the penetration testing tools and techniques effectively, then they would ultimately make great OT penetration testers as they work with OT every day. This would garner them a depth of understanding that a full-time penetration tester can only hope to gain. However, I highlighted that the journey to get them to a level where I would be happy letting them loose on production OT systems would be a long and costly one.

I wanted to leave them on a positive note. As such, I moved on to explain the training journey I would put a junior consultant through to bring them from almost no knowledge of penetration testing to becoming an OT penetration tester. This included discussing some entry-level penetration testing courses and certifications, before progressing to some more specialist courses such as certification body xx course.

I let the client know that it is a risky move to train up their in-house engineers in penetration testing without exposing them to the fundamentals of wider penetration testing. However, if it was a journey they were adamant to go on, I would attempt to support them by recommending training and CPD opportunities that could help the team to slowly build up their skills.

Result: At the end of the workshop, the OT engineers thanked me and my team for clearly summarising the challenges and risks associated with moving testing in-house. They expressed that they didn't feel that they have the time or skillset to proceed in-house. They felt that the information which I had provided had given them clear evidence to raise with their board-level-contact about the risks to the business of using inexperienced in-house staff. I let them know that I would be willing to have discussions to explain the challenges with the board if it helps. I also said that they could come back with any questions, and I always want more people to pursue penetration testing, so would support them if the board does insist on the decision.

B2: Provide and explain cyber security advice, direction and/or expert opinion, in a way that can clearly be understood by the intended audience.

Example: Scoping Complex Penetration Tests

Situation: I am regularly asked to scope complex penetration tests, such as IT Health Checks.

Task: We recently received a tender document from a local government organisation, looking for penetration testing. I was the technical lead for the bid, assisting the sales team in its preparation.

Action: I started by analysing the provided documentation from the client, which suggested that they required a range of services, including:

- Internal and External Infrastructure vulnerability assessments, with targeted in-depth penetration testing in certain areas
- Build & Configuration Reviews
- A Wireless audit
- Unauthenticated web application assessments of several public websites.

As part of this tender, we were required to submit a detailed project plan that included the number of days on each element, as well as example reports for each service.
Based on my reading of the requirements (both technical and documents required for submission), I created a checklist of tasks that would aid our submission.
I then proceeded to prepare the example reports required as part of the bid. I also wrote up the required parts of the bidding document to explain exactly what services we would provide, and how they would align to their requirements.

Result: We scored high marks on the technical section of the bid when receiving the tender results. This was due to my write-ups clearly explaining that we fully understood their requirements and providing the client with a direction for their testing requirements.
Our example reports also demonstrated that they would easily be understood by the intended audience. This was due to us providing detail on our findings in a format that can clearly be understood by their target audience:

- The executive summary by the board
- The technical summary by a project manager
- The detail by the technical team tasked with implementing the fixes.

B3: Have good personal and social skills that demonstrate empathy, diversity, and inclusivity.

Example: Exercises at Cyber event xxx

Situation: When the certification body xx first launched, I had a friend who was involved in running the scheme for QA on behalf of NCSC. They asked if I would be interested in holding workshops and presentations for the events.

Task: I was asked to host an interactive workshop at one of the Cyber xxx events. These events aim to encourage more school-aged people to consider a career in cyber security, helping improve a lack of diversity in the sector.

Action: I strive to make Cyber Security as diverse and inclusive an industry as I can, and so decided to devise a workshop which would combine a little of three main areas:

- A potential real-world scenario.
- Something familiar to the students.
- Something that demonstrates the simplicity of some types of attacks.

As such, I setup a simulated-insecure WiFi network (access was restricted to authorised IPs to prevent accidental connections from legitimate devices), and a cloned Instagram login page.
I asked a volunteer student to connect a device to the WiFi, and attempt to login to a pretend account.
Once this had been done, I ensured the wider audience was included by asking the room to take a closer look at the website, to see if they noticed anything wrong with it. This was designed to get the students thinking about how to identify malicious or untrustworthy sites. It included simple checks like:

- Ensuring that the URL is typed correctly
- That a trusted certificate has been issued for the application
- A wider discussion around connecting to untrusted wireless networks.

I used three approaches to help the participants cement their understanding of the potential attacks, and ensure the session was fully inclusive:

- Using a familiar setup simulating a website many of them access daily, and a coffee-shop setting
- Group discussion, encouraging the students to point out potential issues
- The use of a quiz platform to allow shyer students to still get their voices heard.

Result: The Cyber events xxx workshop was a success. The participants started lively discussions about the issues presented, what they could do to be more secure themselves, and the advice they could pass onto friends and family. I feel that I played an important role in helping a group of female students realise that the world of cyber security can be interesting, enticing, and welcoming. This helped the industry to become more diverse and inclusive. I was invited back for the subsequent couple of events, until I moved across the country and couldn't be as hands-on anymore.

B4: Have excellent oral and written communication skills for both technical and non-technical audiences.

Example: Writing Pen Test Reports

Situation: In a recent penetration test, I found a number of critical vulnerabilities which could have a devastating impact on the client's business if exploited by an unauthenticated attacker. As the application had previously been tested by another vendor, the client was initially adamant that it was a secure system.
Note, I also conveyed the issues identified, including both the business and technical impacts to the client verbally in meetings and over email messages. However, I have tailored this response specifically to the written (report-writing) aspect of the communications.

Task: I needed to use my excellent written communication skills to convey the seriousness of the issues and how to identify and remediate them in a report which persuaded the board to take decisive action. I also needed to provide the technical detail required for their development team to take remedial actions.

Action: I opened the executive summary of my report, aimed at a non-technical audience, by highlighting that I had identified a number of critical and high-severity findings. These could cause an unauthenticated internet-based attacker to gain access to the client's systems. The attacker could add, amend, or delete entire customer bookings, and gain access to compromise sensitive personal information. I then highlighted the regulatory, operational, and reputational risks associated with exploitation. This summary was aimed at getting the attention of non-technical senior leadership so that they could understand the severity of the identified issues.

I then ensured that I had detailed-yet-clear attack chains and root cause analyses within a separate section of the report. This was aimed at the more technical leadership within the organisation. Its aim was to help them to gain additional understanding into the vulnerabilities present and the key changes that could be implemented across the development process to minimise the risks of these issues reoccurring.

I had a detailed section for each identified vulnerability, aimed at a technical audience. This outlined in technical detail the location of the vulnerability within the application, the likely cause behind the vulnerability, step-by-step instructions to allow the developers to reproduce the vulnerability. It also had detailed remediation advice including example code snippets and references to suitable additional documentation as necessary.

Result: The information contained in my report was persuasive and clearly presented in a manner suitable to the required audience. This allowed senior leadership to quickly dedicate resources to remediating the most pressing identified issues. It also allowed the developers tasked with implementing the fixes to identify the source of the identified issues and implement fixes based on the detailed advice contained in my report. After completing a major programme of changes to the system, the client commissioned a retest where I was able to confirm that effective fixes had been put into place. I received confirmation that some of the advice contained within my root cause analyses had been actioned to help prevent such vulnerabilities being reintroduced in the future. This demonstrates how my experience and report influenced the organisation to make major changes.

C: Collaborative Management, Leadership & Mentoring

C1: Are able to manage resource, people, budgets in complex and/or high pressure cyber security environments

Example: Establishing and leading a penetration testing team.

Situation: In joining my current employer, I built and established a new penetration testing team, where I became Head of Penetration Testing. I am required to manage resources, people, and budgets for the team.

Task: I had to work with management, team members and the wider business to ensure that a successful penetration testing team was established. This team needed to function well, deliver on our requirements of providing a high-quality service to customers, and ensure the continual professional development of team members.

Action: I report directly to the Managing Director and regularly attend senior leadership meetings with members at board level within the business. Through these meetings, I advise senior leadership on the progress of the penetration testing team. I provide technical leadership on the direction and requirements of the team to enable it to continue to grow and provide an outstanding service to our clients. This includes advising on certifications, standards and professional memberships which the organisation should be achieving (such as membership of CHECK). It also includes requesting access to relevant training to enable the team to continue to professionally develop. I additionally advise the board on our own internal penetration testing requirements to help ensure that the organisation remains secure.
I line manage the penetration testing team and ensure that the team has the right resources and tools available to effectively perform their job. Alongside, I also perform my duties as a penetration tester myself, resulting in a high-pressure cyber security environment.

Result: The penetration testing team has continued to grow in both new business and headcount since the team was established approximately 3 years ago. I have mentored and witnessed the continued professional growth of both our junior team members and more senior members of the team. I influenced the formation of a strong, competent and highly effective team. I have been appointed as the formal head of the penetration testing team within the organisation. I also liaise with the board to influence our own internal testing programme.

C2: Are able to lead, manage and develop people through coaching and mentoring. Creates and leads formal or informal teams and / or creates collaborative links with teams. Provides support and feedback to encourage and develop colleagues. Advises and influences others.

Example: Junior Pen Tester training

Situation: I was given two junior consultants to join the penetration testing team which I manage, one of which is an Apprentice (0.5 FTE with 0.5 focussed on university).

Task: Neither new junior had any prior experience in penetration testing (although both had limited IT/security experience), so I needed to establish a training plan for the new team members, balancing the lack of availability of senior consultants to deliver bespoke training in the short term versus the need to train the consultants up in a timely manner.

Action: I started by researching publicly available training courses to give the two juniors an initial baseline level of knowledge and start off their development. After thorough research, I booked them onto a training course aimed at new entrants into industry. This would provide them with a baseline knowledge of both application and infrastructure security. I also set them up on our Hack the Box e-learning platform.

This allowed the juniors to gain a baseline level of knowledge. In parallel, I worked to free up some of my time to deliver a more advanced bespoke web application training course, and develop a sign-off test for them.

I set both junior consultants shadowing some of the senior team members. This allowed them to begin to learn the processes we follow when conducting tests, begin to familiarise themselves with our testing methodologies, and learn how to communicate with clients. This formed an informal training path to coach and mentor the juniors alongside the formal training.

After a couple of months of a combination of external training, Hack the Box, and shadowing, I brought the consultants together for a week-long bootcamp I built for web application security testing.

I stepped through each part of our testing methodology in detail, and combined theory, discussions, and practical exercises to ensure that the juniors could learn and develop effectively. This was followed by a 2-week hiatus allowing them to further cement their understanding via Hack the Box labs, before I set a sign-off examination for them.

Result: The full-time junior consultant has passed her sign-off test and has started to deliver client work. Initially this was alongside an experienced senior, and now on her own (although I am still closely auditing her work and making myself or other team members available to support, advise, and feedback as needed). The apprentice (having a slower cycle to facilitate university tasks) is currently sitting his sign-off assessment and will follow the same route to client work.
With a combination of the outsourced training, internal formal training, informal training, and regular one-on-one catchups, the two junior consultants have developed a lot since joining us. Both have successfully passed IASME training to become Cyber Essentials assessors, and one is now delivering penetration tests.
Aware that development is a continual process in penetration testing, I have a plan in place to progress them both to CHECK Team Member level. Further development beyond that will be tailored depending on their preferred specialisations.

C3: Have excellent organisational and time management skills

Example: Managing the Penetration testing team & Client Work

Situation: A colleague and I were brought in establish a new penetration testing team within Company.

Task: I was asked to establish a new penetration testing team in an existing Cyber Security consultancy to help expand their business.

Action: I had to use my excellent organisational and time management skills to balance the tasks involved with establishing a new team versus prioritising commencing client work with a view to becoming profitable.
I started the groundwork before joining the organisation, by identifying the hardware (laptops), software (licensing), and team requirements for setting up a successful team. This allowed us to clearly predict expected setup costs. It also allowed for the laptops to be pre-ordered prior to mine and my colleague's arrival at the business, minimising the lost time before we would be ready for client work.
Once I joined the organisation, I spent a few days building a minimum viable product (MVP) for our standard laptop build, whilst tasking my colleague with producing high-level testing methodologies for us to follow. I also spent time producing processes and procedures for activities such as working on

classified projects, and identified the requirements to get the team certified as a member of membership organisation xxx.

Result: My organisational and time management skills meant that I was able to plan and manage the required setup tasks effectively against the need to start delivering client work. This meant that we were able to start delivering our first projects within a few weeks of the team being established. We quickly became a membership organisation xx member company, and the team turned a profit ahead of the business' forecasts. I was also promoted to formally lead the team last year. We have brought on a further three consultants to the team, including two junior consultants which I have been working to train up. I have also succeeded in getting the organisation CHECK green light status with NCSC.

C4: Maintain a productive, professional, and secure working environment

Example: Working on classified projects

Situation: I was working onsite on a classified project with a colleague.

Task: We were commissioned to conduct an internal infrastructure assessment and desktop breakout testing. Due to the nature of the project, maintaining a secure working environment was essential. All test data was required to stay onsite, and reporting needed to occur onsite.

Action: I ensured that we would have a productive, professional, and secure working environment from the offset. I did this by ensuring that my pen test laptop was fully up to date, with any tooling I believed may be required installed. I ensured that I had the required equipment to allow the full job to be conducted onsite. This included CDs to allow the final report to be passed to the client, and that the latest reporting templates and testing methodologies were on my laptop.
On arrival onsite, I signed us in at reception and asked for our point of contact to be informed of our arrival.
During the course of the test, I maintained a professional and approachable manner with the point of contact, who was very interested in the work we do as penetration testers. I ensured that I completed a thorough job, whilst also explaining my actions to the point of contact as I wented to enable them to gain an insight into our practices.
I ensured both myself and my colleague were professional in keeping detailed and accurate testing notes, logging when we switched networks, and performed other actions during the test. I ensured

that we were productive by regularly checking in with my colleague to ensure that we achieved complete coverage of the target systems without duplicating effort.
At the end of each day, I ensured that our disks were handed to the point of contact for secure storage.
After drafting the final test report, I asked my colleague to read the report to ensure that I had written it completely and accurately, as our standard quality assurance processes could not be followed. I then securely encrypted the report before burning it to a CD for the client's use.

Result: The testing was completed to a high standard within the allocated timeframes. The point of contact thanked us for engaging with their barrage of questions about penetration testing. They stated that they were considering a career move into pen testing, and that my willingness to talk to them throughout had helped them better understand the role. I ensured that my team maintained a secure, professional, and productive working environment throughout.

D: Integrity

D1: Have personal and professional honesty and integrity

Example: Telling clients when they don't really need a penetration test.

Situation: A client approached us for penetration testing after they had suffered a breach.

Task: A client approached us having suffered a breach, asking for penetration testing. I was asked to advise them on the types of testing required.

Action: I discussed the incident which had occurred with the client to gain a better understanding of their cyber security posture and maturity, as well as identify the status of the remediation work following the breach.
As part of this, I determined that the client had performed very limited remediation work and had no plans in place on how to detect, respond, or remediate future breaches.
I demonstrated my personal and professional honesty and integrity and advised the client that whilst it may be possible to identify the route of entry via a penetration test, they would be more effective in engaging the services of an incident response (IR) firm in the immediate term. An IR firm would be better placed to help identify what had gone wrong and where, whereas penetration testing takes a broader approach in attempting to identify all potential weak points in a system.

Result: The client agreed with my advice and thanked me for my honesty. They conducted further incident response and recovery work initially, before then returning for penetration testing. We then agreed to a test plan which would prioritise the most likely targets (externally facing assets), before building a more robust testing programme.

D2: Comply with codes of conduct of their professional membership organisation

Example: Banking mobile application issue

Situation: Whilst conducting a routine mobile application penetration test for a global banking client in recent date, I identified that every touch of the screen was being logged alongside screenshots and sent to a third-party analytics site.

Task: I needed to identify the risks posed by this and escalate it within my organisation and the client organisation as appropriate.

Action: I conducted research into the third-party analytics platform and found a statement on their website stating that organisations should not send them sensitive screenshots.
I raised the issue as a "critical" issue with my client point of contact. He was not concerned about the issue at all, even when I detailed the risks of sending every keypress in online banking along with screenshots to an untrusted application. The point of contact threatened to fire us from the job stating that it was not an issue.
I was aware of my moral obligations, as well as those under the membership organisation xx's Code of Conduct - particularly the Code of Ethics within that code, of which I am a signatory. I escalated this issue internally to our board of directors, and discussed a way forward, including whether we needed to report the issue higher within the client organisation or with the European banking regulators.
As we were preparing to file a report with the regulators, one of our board members managed to arrange a call with the bank's European CISO where we discussed the identified issue in more detail.

Result: The client's European CISO agreed that the issue was of major concern. They instructed the client contact to prioritise a remediation effort, and to issue us with an unreserved apology for their actions in trying to bury the identified issue. Me and my colleagues involved in the project were recognised within our workplace for acting professionally and properly during the project.

D3: Understand and comply with the appropriate legal and regulatory requirements

Example: Working onsite in international territories

Situation: As part of my work with company, I was required to conduct a penetration test for a financial institution based in city, Country.

Task: Prior to travelling to Country, I needed to ensure I had a basic understanding of Country data laws, and the laws which would affect my work. I then needed to ensure that my work was conducted in compliance with this legislation.

Action: I liaised with colleagues who had previously conducted work in Country, and conducted my own research into the applicable laws and regulations which would affect my work. In doing so, I came to understand that Country has robust laws and regulations in place to protect their citizens' data, particularly in relation to the financial sector. I passed the knowledge I had gained to the colleague who was accompanying me on the job to ensure that he also understood his obligations.

Result: I ensured that we both had newly imaged operating systems to conduct our testing on prior to heading out to Country. I also agreed with the client that we would conduct our reporting whilst onsite in the country and leave all data that we collected behind for them to safely store and process. This ensured that we were fully compliant with our legal and regulatory requirements under Country law.

D4: Are able to identify and implement appropriate standards

Example: Working in a global financial organisation to ensure their compliance with PCI-DSS

Situation: I spent approximately 9 months allocated to a global financial organisation on a 2-week on 2-week off rotation. I was conducting penetration testing against their internal assets to ensure compliance with the PCI-DSS standard and their internal security requirements.

Task: Whilst on secondment to this organisation, I was required to conduct penetration tests against systems processing thousands of transactions a second to ensure that they were compliant with PCI-DSS requirements.

Action: As a large financial organisation processing credit card payments, the organisation was required to comply with the PCI-DSS standard. I carried out my security testing and compliance checks in line with PCI-DSS requirements as well as the other legal, regulatory and internal requirements affecting interactions with such high-performance critical systems. This included testing against and following physical, technical, procedural and personnel controls. I had to sign in and out of the data centre floor at the security desk and ensure that all systems under test were compliant with the relevant standards and requirements. This included using only modern cryptography and ensuring that cardholder data was appropriately protected. I was then required to report on any deviations identified and relay my findings to head of the cyber security function within the organisation.

Result: I identified multiple non-conformances with the PCI-DSS standard in the systems I assessed. I flagged these to management as appropriate and ensured that they implemented remediation and risk management plans to mitigate the identified risks. I have also used the information gained around PCI-DSS when conducting testing for other clients in the finance and retail sectors.
Other Examples: Defining and implementing penetration testing team processes to ensure conformance to legal, regulatory, and contractual requirements; Registered as a accredited Expert.

E: Personal Commitment

E1: Carry out and record Continuing Professional Development (CPD) or an acceptable equivalent

Example: As part of my xxxx certification (cert acronym) certification, certification organisation require a CPD log.

Situation: CERTIFICATION ORGANISATION require holders of their certification acronym certifications to obtain 36 CPE credits every four years to maintain certification.

Task: I am required to obtain CPE credits to maintain my certification.
Action: I work to ensure that I regularly obtain CPE credits via attending industry conferences, training, and self-study. I log this into the certification organisation portal as a record of my continuing professional development.

Result: The certification website contains a log of all CPE points I have earned which are related to my certification acronym qualification - primarily continued development within OT security.

E2: Actively participate and promote the cyber security profession

Example: Cyber event, University of xxx

Situation: University of xxx was running an event for schools across the region of England. The aim was to educate secondary school children about how to be more secure online and get them thinking about a potential future career in cyber security.

Task: I was asked to design, develop and present a series of 45-minute sessions to improve awareness of cyber security risks and the behavioural change that the students could make to improve their overall day-to-day security. This was aimed at being a combination of educating the students to be more secure online and to demonstrate some of the fun aspects of working in cyber security.
Action: I actively participated by developing a programme which demonstrated the risks of untrusted WiFi networks, phishing emails and fake websites through an interactive demonstration, interspersed with quizzes and discussion topics. This programme included a demonstration of key aspects of my job as a penetration tester, and common techniques used by attackers to attempt to steal private or personal information. This included social media quizzes that harvest such data.
I offered guidance on how to protect themselves online and in public locations.

Result: The students and teachers found the training sessions both engaging and useful. The feedback I received from both them and the event organisers indicated that it had encouraged the participants to think more carefully about how they behave online and in public locations. This helped to foster behavioural change and cyber security awareness in the students who would shortly be embarking on their careers across a variety of sectors. It also helped to promote cyber security as a potential career path.

E3: Maintain a working knowledge of technological advancements and threat space

Example: As a penetration tester and CHECK Team Leader, I need to continually update my knowledge which I verify via regular examinations.

Situation: Clients and contractual obligations require me to be able to demonstrate my current knowledge and experience through industry certifications.

Task: I am required to undertake NCSC-recognised examinations every three years to demonstrate my continual knowledge.

Action: Throughout the year, I ensure that I am allocated to a variety of client projects which expose me to a mix of legacy, current, and emerging technologies. In the run-up to the industry examinations, I take additional time to ensure that I am fully up to speed on the latest vulnerabilities and public exploits which could be relevant for the examinations.

Result: I have continuously held NCSC-recognised certifications since date, allowing me to demonstrate my working knowledge of the threat space and industry advancements to our clients.