A. Knowledge, Understanding & Experience Practitioner Cyber Security Professionals shall use their knowledge, understanding and experience relating to their Discipline / Specialism including some understanding of cyber security in its wider sense and should be able to demonstrate practical experience within their Discipline / Specialism.	**A-1: Are engaged in a role or have practical experience of activities within their discipline / specialism.** I am currently employed as the Cyber Security Team Lead at InfoSecCo. In this role, I oversee the cyber security team, managing and directing our efforts to protect the organisation and its clients from cyber threats. My daily responsibilities encompass a broad range of cyber security tasks, including threat analysis, vulnerability management, and the implementation of security measures tailored to our specific needs and challenges. This position requires a deep understanding of cyber security principles and practices within our discipline, and I utilise my practical experience daily to ensure the safety and integrity of our information systems. **A-2: Engaged in problem solving to meet a customer / organisational requirements:** Situation: During a 365-security review, I identified several potential vulnerabilities in a client's Microsoft 365 environment. The client relied heavily on this cloud platform for their daily operations, making it critical to address these issues promptly without disrupting their business processes. Task: My primary objective was to audit the client's Microsoft 365 setup comprehensively, identify security weaknesses, and provide clear, actionable recommendations that could be implemented within the constraints of their current setup and business model. Action: I conducted an audit of their Microsoft 365 environment, using a combination of automated tools and manual checks to assess their security posture. Following the audit, I compiled a report detailing my findings, which included issues related to access controls, admin centre controls, and threat protection features. I then presented this report to my client, outlining a series of tailored recommendations that leveraged Microsoft 365's built-in security features and best practices to bolster their security without hindering their operations. Result: The client implemented the recommended changes, resulting in a significantly strengthened security posture for their Microsoft 365 environment. This not only protected them from potential threats but also enhanced their confidence in our services.

	A-3: Have contributed and implemented continuous improvement to cyber security. Situation: At InfoSecCo., part of my role involves contributing to the monthly information security policy review. This task is to ensure that our security measures evolve in line with emerging threats and industry best practices. Task: My responsibility was to assess our current cybersecurity stance, identify any gaps or areas of risk, and provide recommendations for improvements. This involved a thorough analysis of our existing policies, procedures, and technical controls. Action: I conducted a review of our current cybersecurity policies and practices, I identified several key areas where improvements could significantly reduce our risk profile, including enhancements to our incident response, monitoring, and device management. I compiled my findings and recommendations and presented it during our monthly security meeting. Result: My recommendations were well-received and led to the implementation of several updates to our cybersecurity policies and practices. These changes have contributed to a stronger security posture for InfoSecCo., reducing our vulnerability to cyber threats and reinforcing our commitment to continuous improvement in cybersecurity.
B. Communications & Interpersonal Skills Practitioner Cyber Security Professionals should demonstrate that they have reasonable communications and interpersonal skills.	**B-1: Have the ability to discuss cyber security effectively to both technical and non-technical audiences**. In my role, especially when consulting on Cyber Essentials, I regularly engage with a diverse range of stakeholders, from technical staff within IT departments to non-technical staff. This requires a flexible communication style that can be adapted based on the audience's level of expertise. For instance, when discussing technical security measures, I use technical language and concepts to ensure clarity and precision with IT professionals. Conversely, when explaining cyber security principles to non-technical staff, I prioritise simplicity and relevance, using analogies and relatable examples to foster understanding and engagement. This dual approach ensures that all stakeholders are adequately informed about their roles in maintaining cyber security and feel encouraged to contribute to our collective security posture. **B-2: Have good personal and social skills and awareness of diversity and inclusivity.** My tenure as a Rank xx in the Army, where I was responsible for managing diverse teams, was a testament to my interpersonal and leadership skills. This role demanded not only managerial expertise but also a profound understanding of team dynamics and individual motivations. Managing diverse teams, especially in high-

	pressure environments, honed my ability to recognise and respect the unique contributions of each team member, fostering an inclusive atmosphere that valued diversity and promoted unity. These experiences have been pivotal in my professional development, teaching me the importance of empathy, respect, and effective communication in building and leading successful teams. **B-3: Have good oral and written communication skills.** My experience in the Army as and cyber security consulting has significantly contributed to my proficiency in both oral and written communication. Delivering briefings, leading meetings, and consulting with clients have refined my ability to articulate cyber security concepts clearly and persuasively. Additionally, preparing detailed reports, policy documents, and security recommendations has further honed my written communication skills, allowing me to convey information in a manner that is both precise and accessible to the intended audience. This skill set is crucial in my role, as effective communication is foundational to the successful implementation of cyber security measures and policies.
C. Collaborative Management, Leadership & Mentoring Practitioner Cyber Security Professionals should demonstrate that they understand the need to develop management skills and have carried out some supervisory activity within a cyber security environment.	**C-1: Understand the management of resources in a cyber security environment.** Situation: At InfoSecCo., balancing the demands of multiple cybersecurity projects, including consulting and penetration testing, required precise management of both time and resources. Each project has its unique challenges and deadlines, necessitating a strategic approach to resource allocation. Task: My primary responsibility was to ensure that my time and my team's time were optimised across projects to meet deadlines effectively without compromising the quality of our work. This involved not only scheduling and task allocation but also anticipating potential resource constraints before they impacted project timelines. Action: I implemented a dynamic resource management strategy that involved regular project reviews and adjustments to team members' allocations based on project progress and emerging needs. I utilised our internal project management software to track project timelines, milestones, and resource allocations in real-time. This enabled me to identify bottlenecks early and redistribute tasks or adjust deadlines as necessary. Additionally, I put a lot of emphasis on open communication within the team regarding project statuses and encouraged flexibility to adapt to changing priorities. Result: This proactive approach to managing time and resources significantly improved our project delivery efficiency. The strategy also enhanced team satisfaction, as clear communication and realistic project planning reduced stress and workload spikes.

	C-2: Able to supervise and develop people. Situation: Throughout my military career and current role at InfoSecCo., supervising and developing personnel has been a critical responsibility. In the army, I was notably appointed as the regimental career management officer for Army personnel in Location xx. Task: My task was to mentor, develop, and supervise my team members, ensuring their professional growth and readiness to meet both current and future challenges. Action: Leveraging my experience in career development and team leadership, I established a development program. This included personalised training paths, mentorship opportunities, and regular performance evaluations. In Location xx, I focused on career counselling, helping personnel navigate their progression options effectively. At InfoSecCo., I apply a similar strategy, fostering a supportive environment that encourages continuous learning and skill advancement. Result: Through these efforts, team members have achieved notable professional growth, with several advancing to higher roles or gaining specialized certifications. The positive impact on morale and team cohesiveness has also markedly improved our operational effectiveness and job satisfaction levels. **C-3: Have an understanding of the need for organisational and time management skills.** Situation: At InfoSecCo., every minute counts, with all time being accountable. Managing both my time and that of my team is a key responsibility. Task: The essential task was to ensure efficient time management practices were in place to handle our workload, meet project deadlines, and maintain a high standard of our services. Action: I adopted holistic approach to time management, utilising digital tools for scheduling and prioritisation. Daily standup meetings (15 mins max) were conducted to assess workload, redistribute tasks if necessary, and ensure everyone was on track. I also implemented a protocol for reporting delays, fostering an environment where challenges could be openly discussed and addressed promptly. Result: This approach significantly enhanced our team's productivity and cohesion and ability to complete tasks within allocated time frames.

	C-4: Able to identify and implement appropriate standards. Situation: During my time at InfoSecCo., a significant portion of my role involved consulting with various businesses to assess their needs. Each business presented a unique set of challenges and requirements, necessitating a customised approach to selecting and implementing a standard. Task: My task was to analyse the specific needs of each business we consulted with, determining which standards were best suited to their operational context and industry regulations. Action: For each consultation, I started by conducting a review of the business's current cybersecurity posture and identifying any regulatory requirements specific to their industry. Based on this analysis, I carefully selected the most relevant standards, such as ISO/IEC 27001 for information security management, or cyber essentials for initial improvements, I would then guide the businesses through the process of aligning their cybersecurity practices with these standards, providing tailored recommendations to bridge any gaps. Result: By implementing the appropriate standards, the businesses we worked with were able to significantly enhance their cybersecurity defences, ensuring compliance with regulatory requirements and reducing their risk. This not only improved their security posture but also built stronger trust with their customers and partners. Our consultancy's success in this area led to repeat engagements and referrals, cementing our reputation as a trusted advisor.
D. Integrity Practitioner Cyber Security Professionals should demonstrate that they understand and apply integrity, morals, and ethical values.	**D-1: Have personal and professional honesty and integrity.** Situation: Throughout my career, both in the military and at InfoSecCo., upholding honesty and integrity has been paramount. These values are especially relevant in cyber-security, where trust and ethical standards form the backbone of effective security practices. Task: My continuous task has been to demonstrate personal and professional honesty and integrity in every aspect of my work, from daily interactions with my team to managing sensitive client data and information security. Action: I have consistently prioritised transparency in my communications and decision-making processes. This includes admitting to and learning from mistakes, providing honest and constructive feedback to team members, and maintaining confidentiality with sensitive information. I also ensure that all security practices and recommendations are in the best interest of our clients.

	Result: My commitment to honesty and integrity has fostered a culture of trust within my team and with our clients. It has led to strong, lasting relationships, enhanced team morale, and a reputation for reliability and ethical conduct within my client base. **D-2: Comply with codes of conduct of their professional membership organisation.** Situation: Being a part of a professional cybersecurity organisation requires adherence to a specific code of conduct in this case Org A and Org B, which outlines standards for professional behaviour and ethical practices. Task: As a leader and team member, my task was to fully understand and comply with these codes, ensuring that my actions and the actions of my team aligned with the high standards expected by the organisation and the cybersecurity profession as a whole. Action: I took proactive steps to integrate these codes of conduct into our team's operations by incorporating them into our training sessions, policy documents, and daily practices. I also encouraged open discussions about ethical dilemmas and potential conflicts of interest to reinforce the importance of these standards. Result: This led to a team that was not only well-versed in technical skills but also deeply committed to upholding the ethical standards of our profession. It enhanced our professional reputation and contributed to the broader goal of maintaining public trust in cybersecurity professionals. **D-3: Understanding and compliance with appropriate legal and regulatory requirements.** Situation: The cybersecurity field is regulated, with various laws and regulations governing data protection, privacy, and misuse. Navigating these requirements is essential for our work at InfoSecCo., especially when consulting with clients across different industries. Task: My task was to ensure that both I and my team had a thorough understanding of these legal and regulatory frameworks and that our work complied with these requirements. Action: I initiated a internal training program focused on relevant legal and regulatory standards, such as GDPR, CMA, PJA and others pertinent to our operations. This program included regular updates on legislative changes, workshops on compliance strategies, and audits to ensure our practices remained in line with current laws and regulations.

	Result: Our proactive approach to understanding and complying with legal and regulatory requirements greatly minimized compliance risks for our clients and ourselves. It established InfoSecCo. as a knowledgeable and trustworthy partner in cybersecurity, capable of guiding clients through the complexities of compliance in an ever-evolving regulatory landscape. **D-4: Able to identify and implement appropriate standards.** Situation: As a Cyber Security Professional, I encountered a scenario where a client, seeking to expedite their Cyber Essentials certification process, approached me with a request to bend the rules and overlook certain security measures in their systems, regarding local administrators and the use of MFA. Task: My task in this situation was not just to ensure the technical integrity of their systems but also to uphold my personal integrity and ethical standards in dealing with such requests. Action: Understanding the gravity of the situation and the potential consequences of compromising security standards, I politely but firmly refused to comply with the client's request. I explained to them the importance of adhering to the established security measures outlined in the Cyber Essentials framework to safeguard their organisation against cyber threats. Rather than simply rejecting their request, I took the time to empathise with their concerns and understand the underlying reasons behind their desire to expedite the process. I then engaged in a constructive dialogue with the client, highlighting the risks associated with cutting corners in cybersecurity and stressing the long-term benefits of following the prescribed guidelines. Using my knowledge and persuasive communication skills, I presented alternative solutions and strategies that would enable them to achieve their goals while maintaining the integrity of their systems and adhering to best practices. I assured them that prioritising security measures would not only enhance their resilience to cyber-attacks but also strengthen their reputation as a trustworthy and responsible organisation. Result: By standing firm in my commitment to personal integrity which was deeply engrained in me by the military and advocating for ethical, I was able to convince the client to reconsider their approach and adhere to the established security standards. This decision not only protected the client from potential security breaches but also reinforced the importance of integrity and ethical conduct in the cybersecurity profession. Ultimately, the client appreciated my honesty and set the tone for all future work.

E. Personal Commitment Practitioner Cyber Security Professionals should demonstrate that they carry out and plan for continued development of themselves and the cyber security profession.	**E-1: Carry out and record Continuing Professional Development (CPD).** Situation: At InfoSecCo., part of our annual commitment to excellence involves submitting a comprehensive Continuing Professional Development (CPD) report as part of our CREST accreditation. This process is essential for maintaining our high standards of practice and ensuring our team remains at the forefront of cybersecurity expertise. Task: My responsibility was not only to fulfil my personal CPD requirements but also to coordinate the planning and recording of the entire team's CPD activities. This involved forecasting our training needs 12 months in advance and identifying opportunities for professional development that align with our strategic objectives and the latest industry trends. Action: To meet these objectives, we engaged in a variety of CPD activities throughout the year. The team regularly participated in webinars and online training platforms such as Capture the flag exercise X and Cyber training org Y, which offer hands-on cybersecurity challenges and courses. Personally, I completed the Org X Assessors training and achieved the CSTM certification, further enhancing my expertise and contributions to our team's capabilities. Result: The structured approach to CPD ensured that the entire team not only met but often exceeded our training goals, directly contributing to our collective expertise and maintaining our company accreditation. This commitment to ongoing professional development has kept us competitive and capable of delivering the highest level of service to our clients. **E-2: Actively participate and promote the cyber security profession**. Situation: Given my deep personal and professional interest in cybersecurity, I often find myself naturally inclined to discuss the subject in various settings, including interactions with clients and friends. Task: Leveraging my subject interest and personal passion for cybersecurity, I actively engage in conversations to promote awareness and understanding of cybersecurity principles and practices. Action: Whether I'm conversing with clients during consultations or chatting with friends, I tend to share insights into the fascinating world of cyber. Drawing from my skills, experiences, and personal interest, I discuss topics such as threat intelligence, data privacy, and penetration testing in a way that is relatable and accessible to my audience.

	Additionally, I seek out opportunities to participate in cybersecurity-related events, workshops, by actively participating in these activities, I not only deepen my own knowledge but also inspire others to explore and engage with cybersecurity in meaningful ways. Result: Through my genuine passion and enthusiasm for cybersecurity, I have been able to spark interest and curiosity among clients and friends alike. By sharing my subject interest and personal commitment to the cyber field, I have contributed to raising awareness and fostering a culture of cyber resilience within my professional and social circles. My active involvement in cybersecurity communities has enabled me to connect with like-minded individuals and expand my network, reinforcing my dedication to continual learning and development in the cybersecurity profession. **E-3: Maintain a working knowledge of technological advancements**. Situation: The rapid pace of technological advancement presents both opportunities and challenges in the field of security and tech as a whole. Staying informed about the latest technologies is essential for developing effective security strategies. Task: My task was to ensure that I, along with my team at InfoSecCo., maintained a current and comprehensive understanding of emerging technologies and cybersecurity trends. Action: I implemented a strategy for continuous learning that included subscribing to leading industry publications, attending relevant tech and security conferences, and participating in hands-on workshops. Additionally, I encouraged the team to engage in regular knowledge-sharing sessions where we could discuss new technologies and their implications for cybersecurity. Result: This approach has kept us well-informed of technological advancements, enabling us to anticipate and mitigate potential security vulnerabilities before they could impact our operations or our clients. It has also allowed us to advise our clients more effectively on how to safeguard their businesses against the latest cyber threats.