Version 1
February 2024

Guide to Good

Continual Professional Development (CPD)

Introduction

Continual Professional Development (CPD) refers to the ongoing process of enhancing and updating an individual's professional skills, knowledge, and competencies throughout their career. In the context of cyber security professionals, CPD is even more important due to the dynamic and constantly evolving nature of the field. As technology advances, so do cyber threats, requiring practitioners to stay ahead of new vulnerabilities, attack techniques, defence strategies, frameworks and new technologies. In this context, the adoption of good CPD practice ensures that cyber security professionals remain capable of addressing current and emerging challenges and strengthens their effectiveness in protecting information and communication systems, operational technologies and critical national infrastructure.

Through a combination of certifications, workshops, hands-on experiences, peer collaboration, and staying informed of industry trends, CPD empowers experts to adapt swiftly and contribute to the performance of robust cyber security tactics that can protect individuals, organisations, and critical infrastructure from cyber risks. By investing in CPD and actively seeking out opportunities for skill development and learning, cyber professionals not only improve their own careers prospects but also contribute to the broader security of our information and communication systems. This helps ensure that they remain well-equipped to address emerging cyber threats and technological advancements.

A proactive approach to CPD involves setting clear professional development goals, regularly reviewing and updating an individual's skill set, staying informed about industry trends, and consistently seeking new challenges to refine and expand expertise. When adopting good CPD practices and taking a proactive approach towards their career development, professionals continually strengthen their competence and foster a resilient and adaptable mindset that is crucial for effectively navigating the cyber security profession.

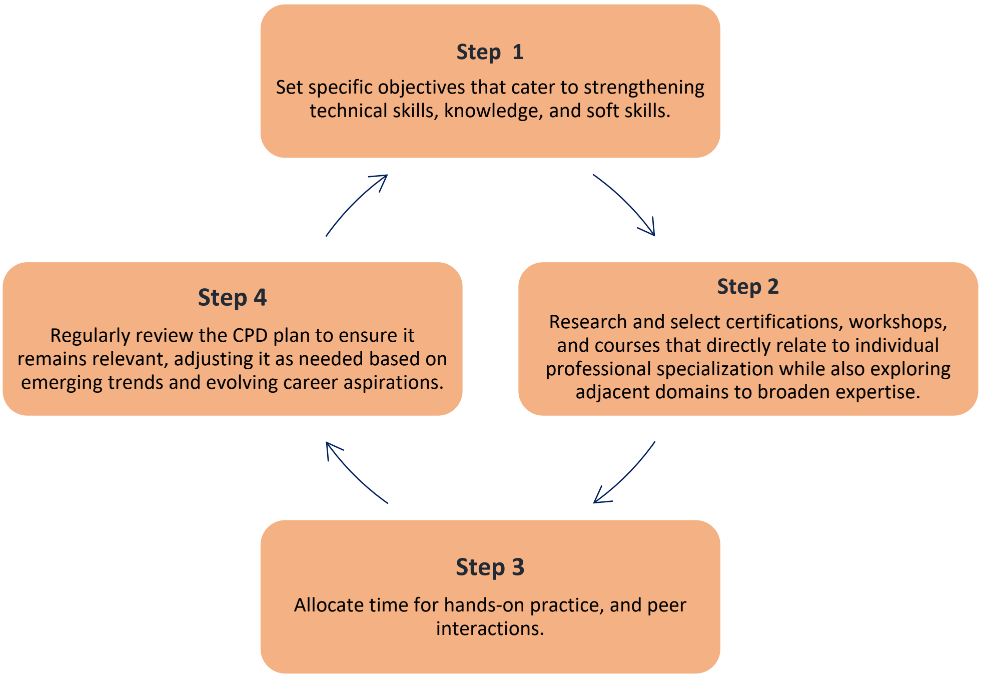
As stated in the UK Cyber Security Council (the Council) CPD Policy, the *demonstration of commitment to CPD is an integral and mandatory part of the competency requirements for all cyber security practitioners irrespective of role or specialism*. Furthermore, *it is vital that professionals remain competent and, therefore, are required to demonstrate that their knowledge and professional skills are being kept current. This is particularly important because of the continual advances and growth in cyber security. This growth means that there is an increasing need to understand the changes and implement advances as they are identified, developed, and become mainstream. This is particularly important whether considering the system as a whole or interfacing with other disciplines providing non-functional requirements*. For this reason, the Licensed Bodies of the Council are required to check the CPD requirements from a registered member every 3 years. Within this time frame, all professionally registered individuals are expected to carry out a minimum of 25 hours per year of CPD across various sources, and report this to the

Licensed Body they are registered with on a 3-year basis. More information regarding the specific requirements on individuals and specific requirements on the Licensed Bodies can be found in the CPD Policy.

Given the need to guide registered cyber security professionals towards adopting CPD, this document seeks to provide examples of what constitutes good CPD practice. With the support of this guide alongside explicit guidance from their respective Licensed Bodies, professionals will know what should or shouldn't be accepted when undertaking the CPD audits every 3 years. Additionally, this document should enable suitable guidance for individuals to carry out their CPD activities in between the audits. Some typical examples of CPD could include training courses, work experience, academic study, volunteering engagements, participation in events and seminars, self-study, and other activities. Essentially, the key aspect of good CPD practice is to ensure a balance between technical knowledge, soft skills, and practical application activities to develop a well-rounded skill set.

Creating a personalised CPD plan

To create a personalised CPD plan, individuals need to engage in a dynamic cyclical process that involves key steps to ensure ongoing professional growth and alignment with their individual career objectives. These steps encompass setting clear and specific goals, researching and selecting relevant learning opportunities, allocating time for practical experience and networking, and maintaining flexibility through regular reviews and adjustments. By following this structured approach, individuals can tailor their CPD journey to address their unique strengths, weaknesses, and interests within their professional specialisation. The process below suggests the four main steps that can be taken to create an effective personalised CPD plan.



Step 1
Set specific objectives that cater to strengthening technical skills, knowledge, and soft skills.

Step 2
Research and select certifications, workshops, and courses that directly relate to individual professional specialization while also exploring adjacent domains to broaden expertise.

Step 3
Allocate time for hands-on practice, and peer interactions.

Step 4
Regularly review the CPD plan to ensure it remains relevant, adjusting it as needed based on emerging trends and evolving career aspirations.

It is important to emphasise that regularly reviewing and adjusting the personalised CPD plan is essential to ensure its ongoing effectiveness. The dynamic nature of the cyber security landscape demands flexibility and adaptability. By routinely revisiting their personalised CPD plan, individuals can assess their progress, identify any gaps in their skill set, and accommodate shifts in industry trends or personal career aspirations. This iterative process allows professionals to fine-tune their learning objectives, incorporate new technologies or methodologies, and remain aligned with the rapidly evolving demands of the field. Embracing a habit of continual evaluation and refinement ensures that their CPD efforts remain targeted, relevant, and instrumental to their professional growth as a cyber security professional.

Typical categories of CPD activities followed by examples

1. Technical Learning

   a. Certifications
      - Pursue one major cyber security certification (e.g., CISSP, CISM) or multiple smaller certifications (e.g., CompTIA Security+, CEH).

   b. Online courses and webinars
      - Complete online courses on threat hunting, incident response, secure coding, etc.

   c. Hands-on labs and CTF challenges.
      - Engage in practical exercises to simulate real-world cyber security scenarios.

   d. Vendor-specific training.
      - Participate in training programs for specific security tools your organisation uses.

2. Knowledge enhancement

   a. Reading and research.
      - Example: regularly read cyber security blogs, research papers, and news articles. Licensed Bodies may ask for a written reflection on the research material reported as CPD.

   b. Threat intelligence updates.
      - Example: subscribe to threat intelligence feeds to stay informed about emerging threats.

3. Professional and soft skills

   a. Industry conferences and workshops.
      - Example: attend cyber security conferences to learn about trends and network with peers.

   b. Peer learning and networking.
      - Example: participate in online forums and communities to discuss industry topics.

   c. Undergoing mentorship and coaching.
      - Example: seek guidance from experienced cyber security professionals for career advice.

   d. Becoming a mentor.

   - Engage in mentoring programs to cultivate soft skills such as effective communication and leadership.

e. Leadership and Management Training.
   - Example: Engage in workshops, seminars, training programmes, and/or conferences focused on trends, best practices, skills development, and innovations in leadership and management. This includes skills capacity development across different areas of business management, including human resources management, finance, project management, etc.

f. Board, panel, or advisory services:
   - Acting as an external advisor to relevant organisations (such as local cyber clusters), outside of the applicant's typical day-job.

4. Practical application

a. Become an assessor for a licensed body.
   - Example: register as an assessor for a licensed body and start assessing applicant applications.

b. Regulatory and policy knowledge.
   - Example: stay informed about relevant data protection laws and compliance regulations in your region.

Reporting and documentation procedures

Effective reporting and documentation procedures are essential components of maintaining your professional development as a registered cyber security professional. To ensure continual improvement and adherence to industry standards, it is recommended that professionals engage in a robust reporting process every three years, accompanied by comprehensive documentation. The reporting process serves as a critical checkpoint for assessing and enhancing professional competence. It involves a thorough review of your CPD activities and accomplishments during this period. The types of documentation required for this reporting process may vary depending on the specific internal procedures of the Licensed Body to which professionals are registered. These documents often include certificates, training records, project reports, and any other evidence of CPD activities completed.

In line with good CPD practice and to meet approval criteria, registered professionals are strongly advised to maintain a CPD portfolio throughout the three-year cycle. This portfolio should meticulously record completed activities, highlighting their relevance to their professional growth, what they learned and how they will put it into practice. It serves as a valuable resource during the reporting process, helping professionals to demonstrate their commitment to continual learning and improvement.

While the format of reporting may vary across different organisations, the main objective remains the same: to provide detailed insights into CPD activities. The specific details of what to report and how often to report can be tailored to align with the requirements of each Licensed Body and to individual professional development goals. This flexibility allows each professional to choose a reporting format that best suits their preferences, organisational needs, and career aspirations.

It is important to keep in mind that the reporting and documentation procedures aim to capture the essence of the CPD journey, showcasing the individual’s dedication to maintaining high professional standards as a registered cyber security professional. By adhering to these practices, professionals not only fulfill their obligations but also contribute to the ongoing improvement of the cyber security field while ensuring that they continue to meet the rigorous standards set by the UK Cyber Security Council along with our Licensed Bodies.