



Chartered Institute of Information Security

CII Sec Guidance for Continuing Professional Development (CPD)

October 2024

V1.0

Contents

1. Introduction	3
2. Understanding Professional Development Requirements	3
2.1 CPD Cycle	3
3. CIISec CPD Requirements	5
3.1 Membership Level	5
3.2 Category requirements	5
4. Categories	6
5. Submission requirements	6
6. Audit	7
7. Validation	7
8. Revocation	7
9. Appeals	8
Annex A	9

1. Introduction

CIISec promotes, develops, and represents the professionalism, integrity and excellence of those operating within cyber, digital and information security.

Accredited membership seeks to formally recognise the excellence that exists amongst cyber, digital and information security individuals, in the same way that many other professions accredit skills and standards.

Having completed the accreditation process, Continuing Professional Development (CPD) is the members route to show continued commitment to maintaining and developing their competency in a variety of skills related to the profession.

The purpose for completing CPD is to encourage individuals to look forward; to identify opportunities to learn something new; refresh existing knowledge; improve skills or aid the development of personal qualities; to maintain and develop workplace performance; aid future career opportunities and professional recognition.

Learning through CPD should be reflective and should relate to specific objectives even if these are limited to maintaining a professional competence.

2. Understanding Professional Development Requirements

Individual members are best placed to determine their development needs and how to meet them and the best way is to set this out in a CPD Plan. It is recommended that this is reviewed at a minimum annually, but as development needs are met, others may be added. It is likely that in some cases employers or experienced colleagues will play a part in the development and execution of an individual's CPD; but ultimately it is the individual member's responsibility to identify their professional development needs, opportunities and to understand and meet the requirements to maintain a professional membership or registration.

2.1 CPD Cycle

The first step in establishing future professional development is to take the time to reflect on what has been accomplished to date.

This should then help to identify development needs for the next CPD period. Thought should be given to identifying and recognising knowledge gaps, strengths and weaknesses.

After identifying the needs, a CPD plan can be developed. This is where goals and objectives are set and ways to fulfil them can be identified.

The next step is to complete the plan by attending and engaging in activities to meet the needs that were identified and added to the plan.

An important part of any CPD plan is to update the plan with the learning outcomes from undertaking the various activities. Whilst this can be subjective it will be of benefit as they

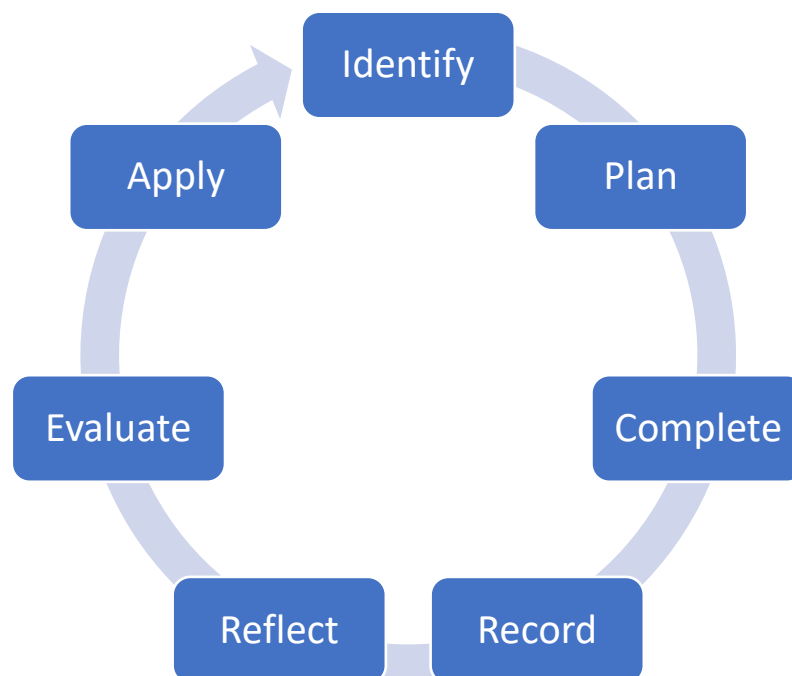
CIISec Guidance for Continuing Professional Development (CPD)

should show what knowledge, skills and abilities can be demonstrated upon completion of the learning experience or activity.

Next, it's time to reflect, consideration should be given as to whether the learning or activity has met any of the gaps identified.

Having completed some or all of the plan, time should be taken to evaluate, by gauging the effectiveness of the learning and the impact of all activities.

Finally, applying what has been learnt, putting into practice the new skills and knowledge and sharing it with others.



3. CIISec CPD Requirements

Having gone through the cycle and developed a CPD plan, the points below set out the requirements that are expected by CIISec.

3.1 Membership Level

CIISec have several different membership levels and the CPD requirements reflect this.

With effect from the release of this document CPD **must be completed annually** to maintain CIISec membership going forward.

Membership Level	CPD Requirement
Associate, Full and Fellow	Should complete a minimum of 25 hours annually . It is acknowledged that most members will complete more than this.
Accredited Affiliate	Should complete a minimum of 10 hours annually.
Retired (accredited) members	Are expected in their first year (having notified CIISec of their change in status) to complete a minimum of 10 hours CPD. After this period, providing membership is maintained then the requirement will be confirmation that they have completed Category 1 (detailed below).
Student and Affiliate members	Will be expected to confirm on an annual basis that they have completed Category 1 (detail below) of the CIISec CPD requirements.
All levels	CPD should be completed at least 2 months prior to the membership lapse date. However, if the minimum hours required have been met then the CPD form can be submitted earlier.
All levels	If a member upgrades within their annual CPD period, CIISec will expect the CPD requirements from the higher membership level.

3.2 Category requirements

The following table details the mandated CPD submission requirements.

Membership Level	Mandatory Requirement
Accredited Affiliate, Associate, Full and Fellow and those holding Professional Registration through the UK Cyber Security Council (UKCSC)	provide evidence of reading and understanding the CIISec Code of Conduct and Ethics (and the UK Cyber Security Council ethics statements if the CPD also covers Professional Registration).
	ensure at least 2 hours of CPD each year, relate directly to Category 2 (CIISec Essential skills: Policy and Standards (A2); Legal and Regulatory Environment and Compliance (A6); Risk Management (B2); Data Protection (G1); Privacy (G2)); and for the specialism(s) held under their Professional Registration (as applicable).
	provide CPD from at least 3 different categories.

4. Categories

The following details the top-level categories, more detail of the activities related to the categories can be found in the table in Annex A.

As previously highlighted categories 1 and 2 are mandatory, providing 4 further categories to provide evidence from.

Category 1	Codes of Conduct and Ethics	Max 1 hour
Category 2	CIISec Essential Skills and/or Professional Registration Specialism	Min 2 hours
Category 3	Professional Contribution – Volunteering	Max 20 hours
Category 4	Development (Role Related)	Max 20 hours
Category 5	Management, Leadership, Business and Communications	Max 10 hours
Category 6	Events and Conferences relating to Cyber Digital and Information Security	Max 10 hours

5. Submission requirements

We are introducing a new form to be completed. Whilst we understand that many will complete CPD for other certifications and accreditations we do have specific CIISec requirements which need to be fulfilled.

Section 1 relates to the member's personal information. We are looking for name, e-mail, membership ID, membership level and the period the CPD form covers.

Section 2 covers the 6 categories that members can claim CPD against. We are expecting to see the hours and details of the activity along with the learning outcome.

For category 1 by inserting a date, the member is confirming that the category has been completed as this is a mandatory category. Category 2 is also a mandatory category.

For the remaining categories we are expecting the member to enter total hours claimed as a number, noting that if a particular category is not being claimed then a zero will still need to be entered. Please remember to check the table above, as we may have restricted the number of hours that we will accept for a chosen category.

Then we are looking for the detail related to the activity undertaken and the learning outcome and/or benefit to continued professionalism.

For example, if it is attendance at an event, then enter the title of the event, the date attended and what was gained from attendance. Similarly, if the activity is a course, detail the name of the course, organisation running it, number of days and the knowledge/learning gained by attending.

CIISec Guidance for Continuing Professional Development (CPD)

Currently, we are not expecting members to attach/load up any documents to validate any of the activities listed. This will only be required if the member is audited, but it should be noted that it is the member's responsibility to ensure this evidence is retained and available on request.

Finally, we are looking for the total hours for all categories claimed to be entered.

6. Audit

CIISec will conduct random audits of submitted CPD forms. It is an important process that upholds the integrity of CIISec's credentials and ensures compliance with contractual requirements put on CIISec.

If an individual is selected for an audit, they will receive an email with instructions about the necessary documentation required to validate the activities which have been declared on the initial CPD submission. To maintain membership, it is expected that members will respond to audit requests and provide the required information within 90 days.

7. Validation

Proof of CPD claimed may be in the form of course transcripts, awarded diplomas, certificates or evidence of attendance, e-mail or Teams invitations, research/prep notes for speaking or teaching, copies of official meeting minutes, or rosters/documentation of registration materials etc.

When validating CPD with respect to a book and/or magazine, please provide details such as a purchase receipt, invoice etc. At a minimum, the proof should include the title and author for a book and if it's a magazine, the publisher.

It is the **members responsibility to retain documentation** and keep proof of CPD for at least 12 months beyond the expiration of membership/professional registration in the event of an audit. **CIISec will not** retain any documentation provided once the audit has been completed.

8. Revocation

Members who fail to comply with the CIISec requirements for CPD face having their membership and use of the CIISec post-nominal revoked and will no longer be allowed to present themselves as a CIISec member. Individuals who have their accreditation revoked will be required to complete a reaccreditation application against the CIISec Skills Framework to regain membership.

Those members who also hold a Professional Registration should note that CIISec are obligated as a Licensee to inform the UKCSC if an individual does not comply with the CPD requirements (25 hrs annually and 75 hours over a 3-year period). By not meeting the CPD requirement, the individual risks removal from the Council Register and therefore the ability

CIISec Guidance for Continuing Professional Development (CPD)

to continue to use the Councils titles and post-nominals. The names of professionally registered individuals removed from the Register due to non-compliance with the published CPD requirements will be made available to other Licensed Bodies, as necessary.

9. Appeals

Individuals whose accredited membership has been revoked due to noncompliance with the CIISec CPD requirements and appeal for reinstatement may incur an additional reinstatement fee. It should be noted this may be in addition to any back or current fees required to reinstate the individual. Appeals undertaken by an individual are undertaken at the discretion and cost of that individual.

For further details of the appeals process contact: membership@ciisec.org

CIISec Guidance for Continuing Professional Development (CPD)

Annex A

The following table details recognised activity and the category it relates to.

Category 1 - Code of Conduct and Ethics
Reading of the CIISec Code of Conduct & Ethics and if applicable UK Cyber Security Council Guiding Principles for Individuals
Category 2 - CIISec Essential Skills and Professional Registration Specialisms
Learning specifically related to CIISec Essential Skills: A2 - Policy and Standards; A6 - Legal and Regulatory Environment and Compliance; B2 - Risk Assessment; G1 - Data Protection and G2 - Privacy
Learning specifically related to the Professional Registration Specialisms of: Cyber Security Audit and Assurance; Cyber Security Governance and Risk Management and Secure Systems Architecture and Design
Category 3 - Professional Contribution - Volunteering
Assessor/Interviewer/Accreditation Committee Member/Training Course Assessor/EPQ Independent assessor/moderator
Mentor/Hub lead or coordinator/Associate or Full Development Programme Speaker/panel member
Masterclass presenter/CIISec Live Speaker or Panel member/CIISec Working groups
Article, Blog (official) or White paper – author/co-author/editor
Book – author/co-author/editor/chapter author
Training Course Preparation
Unpaid participation in International, Government or Industry working groups
Unpaid skill related support to businesses, universities etc.
Category 4 - Development (Role Related)
Learning specifically related to any of the other CIISec A-I Skills
Learning through practical work experiences/Unique work experience/Receipt of guidance and/or support from colleagues
Job/work related courses which are part of a members ongoing development, where the learning outcomes directly relates to their role
Category 5 - Management, Leadership, Business and Communications
Leadership training/Project management training/Courses on interpersonal communications etc.
Category 6 - Events and Conferences relating to Cyber Digital and Information Security
Attendance at events relevant to the profession (e.g. CIISec Live, Internet Intelligence & Investigation (III) Conference, CyberUK etc.)

NOTE: If members have published papers, written articles, given internal and/or external presentations and/or lectures. When using these they should only be counted once unless there have been substantial updates made.