

CII Sec Guidance for Continuing Professional Development (CPD)

September 2026

V3

Contents

1. Introduction	2
2. Understanding Professional Development Requirements	2
3. CII Sec CPD Recommendations	3
4. Categories	4
5. Submission requirements	4
6. Audit	4
7. Validation	5
8. Revocation	5
9. Appeals	5

1. Introduction

CII Sec 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 professional registration process, Continuing Professional Development (CPD) is the member's route to show continued commitment to maintaining and developing their competency in a variety of skills related to the profession.

The purpose of 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.

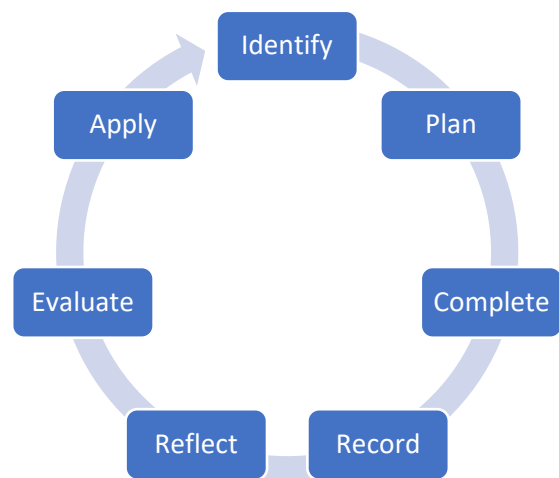
2. Understanding Professional Development Requirements

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. It is the individual member's responsibility to understand and meet the requirements to maintain a professional registration (CII Sec membership; UK CSC or Engineering Council registration).

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.

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 Recommendations

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

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

CPD should be completed in advance of your renewal date, and you will receive reminders from CIISec in advance of your renewal date. Make sure you understand the requirements for other bodies.

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.
Affiliate members	Are encouraged to get used to recording CPD. Whilst no requirement is stipulated, Affiliate members are expected to confirm on an annual basis that they have read the Code of Conduct and Ethics

If you upgrade to an accredited membership grade or above during your membership year, you'll be expected to fulfil the CPD requirements after a full year in that grade.

4. Categories

Recording CPD hours in categories 1 and 2 are expected, members can then choose to record evidence in any of the four further categories up to the maximum.

Category 1	Code of Conduct and Ethics	Max 1 hour
Category 2	CII Sec essential skills (ref Skills Framework); Professional Registration Specialism(s) or skills relevant to registration level (IEng/CEng)	Min 2 hours
Category 3	Professional or voluntary contributions	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

CPD can be submitted via the Trail platform accessed in the member area. Trail can also be downloaded as an app.

You will need to set your CPD objectives, log activities, then when you upload your evidence, i.e. certificates/emails etc, this will automatically map your CPD to the relevant categories.

Trail will track your progress throughout the CPD cycle making it easy to manage.

Please note the onus is on you to ensure CPD is completed as required. CII Sec will not be reviewing or approving CPD unless the member is called upon for audit.

CII Sec understands that from time to time there may be extenuating circumstances that prevent members from completing the full hours recommended. These will be reviewed on a case-by-case basis and may result in the member being exempted from completing CPD for a specific period and from the audit.

For more information, see user guidance for Trail and our membership [Terms and Conditions](#).

6. Audit

CII Sec will conduct random annual audits. It's an important process that upholds the integrity of CII Sec's credentials and ensures compliance with contractual requirements put on CII Sec.

If an individual is selected for an audit they will be contacted with instructions. It is expected that members will respond to audit requests and provide the required information within 90 days.

The audit will be conducted by active professional registrants and feedback will be provided.

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/preparation notes for speaking or teaching, copies of official meeting minutes, or rosters/documentation of registration materials etc. We suggest keeping a note of the url or DOI of journals, books, articles, videos consumed online.

It is your 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

Those members who hold a Professional Registration should note that CIISec is obligated as a Licensee to inform the UK CSC or Engineering Council if an individual does not comply with the CPD requirements (it is recommended that you check the requirements). By not meeting the CPD requirement, or responding to an audit the individual risks removal from the Council Register and therefore the ability to continue to use the Council's 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 professional membership has been revoked due to non-compliance 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