Requirements applicable to E-learning Activities

as mentioned in para 30 – 31 of Annex 1 to **GL24**: **Guideline on Continuing Professional Development for Licensed Insurance Intermediaries**

This document aims to set out the requirements applicable to E-learning Activities to be recognized as Type 1 or Type 7 Qualified CPD Activities under **GL24**: **Guideline on Continuing Professional Development for Licensed Insurance Intermediaries** ("CPD Guideline") issued by the Insurance Authority ("IA"), and should be read in conjunction with the CPD Guideline.

For the avoidance of doubt, the requirements set out in this document are not applicable to E-learning Activities which form a part of a Type 2, 3, 4, 5, 6 or 8 Qualified CPD Activities.

Unless otherwise specified, words and expressions used in this document shall have the same meanings as given to them in the CPD Guideline.

1. Introduction

1.1. According to the CPD Guideline, individual licensees can earn up to 5 CPD hours (in aggregate) for each Assessment Period through participation in E-learning Activities recognized as Type 1 or Type 7 Qualified CPD Activities.

1.2. E-learning Activities can only be recognized as Type 1 or Type 7 Qualified CPD Activities if the E-learning Activities:

(a) have a proper login and identity-checking system to prevent abuse and unauthorized logins;

(b) provide continual verification and assessment elements;

(c) have a proper audit trail which keeps track of participants' login time[1], idle-time[2] and activities undertaken; and

(d) can meet the other requirements applicable to E-learning Activities as specified by and posted on the IA's website.

1.3. This document aims to set out the requirements applicable to E-learning Activities as mentioned in para 1.2 (d) above.

[1] "login time" generally means the date and time at which the users logged on to an E-learning Activity as well as the total time the users logged on to the E-learning Activity.

[2] "Idle-time" generally means the period of inactivity on the part of the users of an E-learning Activity, e.g. time during which the users are not clicking or inputting anything using the keyboard/mouse, users may also pause the E-learning activities during the learning process. However, the time during which a short video or an audio clip being played in an E-learning activity should not normally be regarded as "idle-time".

2. Definition

2.1. "E-learning Activities" refer to activities in the form of online courses. Online courses are learning programmes whose delivery involves the use of technology and are delivered through a digital learning platform via the Internet or intranet to provide structured teaching, learning and assessment. They can be undertaken by users anytime and anywhere with no time or geographic limitation.

2.2. "E-learning Activity Providers" refer to CPD activity providers who offer E-learning Activities which are Type 1 or Type 7 Qualified CPD Activities.

2.3. "Users" refer to the learners who undertake an E-learning Activity.

3. Requirements applicable to E-learning Activities

3.1. All E-learning Activities which are Type 1 or Type 7 Qualified CPD Activities are required to comply with the following requirements:

3.1.1. Secured login and continual identity authentication system

3.1.1.1. E-learning Activities should have in place a secured login to verify the identity of the users at the beginning of the E-learning Activities to avoid unauthorized logins. E-learning Activity Providers should ensure that the data input by the users (such as the user name, password, etc.) is accurate by verifying it against the data in the record of the E-learning Activity Providers via a login system.

3.1.1.2. E-learning Activity Providers should also be able to ensure that the users claiming the CPD hours are in fact the users registered for and participated in the E-learning Activities (i.e. they are who they claim to be) to avoid abuse. To this end, they should utilize appropriate identity authentication technology to uphold the integrity of E-learning Activities. Detailed requirements in this regard are set out below.

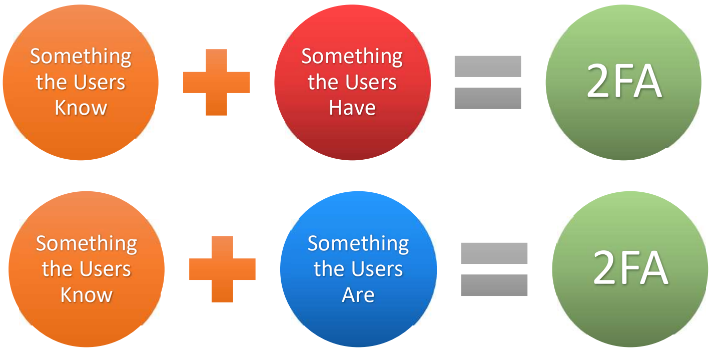
3.1.1.3. In general, there are three types of recognized factors for user identity authentication:

(a) something the users know (such as username, password, personal identification number (PIN), etc.);

(b) something the users have (such as a mobile phone for receiving a secondary one-time password); and

(c) something the users are (biometrics such as fingerprint, iris, retinas, face, speech, keystroke, etc.).

Examples of Two-factor Authentication (2FA)



Non-proctored E-learning Activities

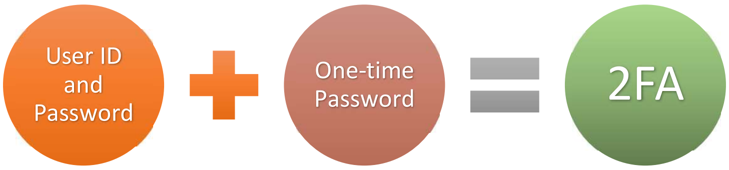
3.1.1.4. For E-learning Activities conducted in an unsupervised environment, i.e. the activities are wholly conducted online and are not proctored, they should at a minimum adopt a **two-factor authentication** to authenticate users' identity. For example, there should be a front-end login by the users using a unique user ID and a personal password (i.e. something the users know), and the users should also input a **secondary one-time password** ("OTP") sent directly to the mobile phone number of the users which is pre-registered with the E-learning Activity Providers (the mobile phone is something the users have).

3.1.1.5. The authentication process of an E-learning Activity should consist of a combination of at least two factors of different types. Two factors of the same types, e.g., both factors are something the users know, is not a two-factor authentication.

3.1.1.6. OTP can be delivered directly to the users' mobile phone through SMS or mobile apps[3]. However, OTP generated by a hardware token, key token or USB token, which can be easily shared, is not an acceptable factor for this purpose. E-learning Activity Providers may adopt other appropriate factor(s) in their two-factor or multi-factor authentication. For examples, **biometric technologies** such as iris or facial recognition, retina or fingerprint scanning, voice recognition, etc. may be deployed for a higher level of integrity.

[3] Examples of such mobile authentication apps include Authy, Duo, FortiToken, Symantec VIP Access, Google Authenticator, etc.

An Acceptable Two-factor Authentication (2FA)



Proctored E-learning Activities

3.1.1.7. If an E-learning Activity Provider does not adopt two-factor authentication in the delivery of its E-learning Activity as outlined in sections 3.1.1.5 – 3.1.1.6, it should either:

(a) allow the users to take the E-learning Activity online but request them to **take a proctored end-of-activity assessment of the E-learning Activity in person at a designated training centre** provided or approved by the E-learning Activity Provider, where the identity of the users is verified in person by a staff member of the E-learning Activity Provider or the training centre (see section 3.1.2 below for the assessment element of E-learning Activities); or

(b) request the users to **take the whole E-learning Activity in person at a designated training centre** provided or approved by the E-learning Activity Provider, where the identity of the users is verified in person by a staff member of the E-learning Activity Provider or the training centre.

Continual authentication of the users' identity

3.1.1.8. There should be continual authentication of the users' identity throughout the E-learning Activities. For example, a user should be prompted to input the personal password or OTP at irregular intervals (i.e. randomly at different points of time) during the E-learning Activity. Apart from the front-end login, a user should be prompted to input the personal password or OTP on at least one separate occasion during an E-learning Activity.

3.1.2. Assessment element

3.1.2.1. All E-learning Activities should contain an end-of-activity ("EoA") assessment component to assess the users' understanding of the learning materials. As an example, users could be requested to answer an appropriate number of MC questions at the end of an E-learning Activity.

3.1.2.2. In order to earn the CPD hours specified for an E-learning Activity, a user must have successfully completed the EoA assessment and achieved the pass mark specified by the E-learning Activity Provider.

3.1.2.3. Users should be allowed to attempt the EoA assessment again if they have failed it. However, they should only be allowed to retake the EoA assessment once in this way. If the users still fail to achieve the pass mark at the second attempt, they should be required to go through the e-learning course again before they are allowed to take the EoA assessment for a third or fourth time. E-learning Activity Providers should set the maximum number of re-attempts of the EoA assessment that they consider appropriate.

3.1.2.4. As a general rule, the questions used in the re-assessment should be different from those used in the first assessment. Arranging questions and/or answers in different order are not considered sufficient for this purpose. E-learning Activity Providers should adopt a prudent approach in selecting the questions for re-assessment, taking into account of the size of EoA assessment questions bank. Users should be advised if they have answered each assessment question correctly, although the correct answers should not be disclosed to them for questions answered incorrectly.

3.1.2.5. Users are not required to complete the whole E-learning Activity in one sitting. They may choose to take a bite-size module of the E-learning Activity and log out, then resume taking the rest of the activity and complete the EoA assessment on other occasions. The completion date of the E-learning Activity will be the date on which the users obtain a pass mark of the EoA assessment.

3.1.2.6. Prospective users should be informed of the format and type of assessment(s) of the E-learning Activity as well as the required pass mark prior to enrolment.

3.1.3. Audit trail to track users' login time[4], idle-time[5] and activities undertaken

3.1.3.1. A tracking system should be in place to keep track of the users' login time, idle-time and all the activities undertaken during the entire time logged in. Activities undertaken include but not limited to pages viewed, videos watched, the end-of-activity assessments/exercises/quizzes/mini-games attempted and the scores obtained, forums and chatrooms participation, etc. The relevant audit trail records should be generated and maintained for audit purposes.

3.1.3.2. If the tracking system is unable to log the idle-time, the E-learning Activity Provider concerned should ensure that the E-learning Activity will automatically log out the users when there is a certain period of inactivity.

3.1.3.3. Upon request, an E-learning Activity Provider should provide the IA with the relevant audit trail records to confirm if a user has successfully completed a particular E-learning Activity as certified on a certificate/record of completion purportedly issued by the said E-learning Activity Provider.

3.1.4. Expected study hours and the number of CPD hours to be earned

3.1.4.1. An E-learning Activity must last for no less than **30 minutes**; it could be a 30-minute E-learning Activity or an E-learning Activity comprised of several modules (e.g. 2 modules of 15 minutes or 3 modules of 10 minutes, etc.). There is no specific limitation on the course design as such. Users may choose to complete one particular module and log out. When they login again, the learning management system should be able to tell them which module(s) they have already completed. However, in order to earn the CPD hours specified for an E-learning Activity, users must have successfully completed all the modules as well as obtaining a pass mark in the final assessment at the end of the whole activity.

3.1.4.2. An E-learning Activity Provider must specify **the minimum number of study hours** that the users are expected to spend on the whole E-learning Activity in order to master all the learning materials so as to meet the activity objectives.

3.1.4.3. Given that users are free to spend as long (or as short) a time as they wish on an E-learning Activity, an E-learning Activity Provider must also

[4] See footnote 1.

[5] See footnote 2.

specify **the number of CPD hours that the users can earn** upon their successful completion of the E-learning Activity. For instance, if an E-learning Activity Provider specifies that users could earn 1 CPD hour upon their successful completion of a particular E-learning Activity, users can earn 1 CPD hour only in respect of this E-learning Activity, even though they might have in fact spent more than an hour to complete the said activity.

3.1.4.4. Time spent by users on taking the end-of-activity assessment should generally **not** be included in the CPD hour(s) to be awarded to the users upon their successful completion of an E-learning Activity.

3.1.5. Certificate/Record of completion of the E-learning Activity

3.1.5.1. E-learning Activity Providers should issue a **certificate/record of completion,** in hard copy or soft copy (downloadable and printable), to each user who has successfully completed an E-learning Activity. As a best practice, the E-learning Activity Providers could make the certificate/record of completion available in the learning management system for downloading and printing by the users anytime as long as the users remain a subscriber to the e-learning service.

3.1.5.2. Users are advised to download the certificate/record of completion upon their successful completion of an E-learning Activity as they may not be able to log in the learning management system again when they no longer subscribe to its service.

3.1.5.3. E-learning Activity Providers should include all the following information in the certificate/record of completion as far as practicable:

(a) Name of the E-learning Activity Provider;

(b) Title of the E-learning Activity;

(c) Reference number assigned by the Hong Kong Council for Accreditation of Academic and Vocational Qualifications ("HKCAAVQ") for Type 1 Qualified CPD Activities (or by the IA for E-learning Activities which are Type 7 Qualified CPD Activities);

(d) Date on which the user completed the E-learning Activity;

(e) A statement to the effect that the CPD activity was completed by e-learning;

(f) Type of Qualified CPD Activity (i.e. Type 1/Type 7);

(g) Full name of the user who has completed the E-learning Activity (as shown on the identification document);

(h) CPD hours (or Compulsory CPD hours on "Ethics or Regulations" as the case may be) awarded to the user;

(i) Name of a responsible person (e.g. the head of organization or person-in-charge), together with his/her printed signature and the printed stamp of the E-learning Activity Provider; and

(j) Certificate issue date and a unique certificate number.

3.1.5.4. As an alternative to a certificate/record of completion, E-learning Activity Providers could issue to the users an electronic periodic completion record or "usage report" (i.e. quarterly, half-yearly or annually) which contains all the information set out in para 3.1.5.3.

3.1.5.5. E-learning Activity Providers should re-issue the attendance certificate/ attendance record upon the request of users within 4 years of the date of CPD activity held with or without charges. The charge, if any, should be of a reasonable amount. To this end, they should maintain the electronic completion records and usage records of the users to enable them to accede to the request of users for a reissued certificate/record of completion.

3.1.6. Requirements applicable to E-learning Activity Providers

E-learning Activity Providers must:

(a) be qualified and experienced in the design, delivery and administration of E-learning Activities;

(b) has adequate infrastructure and technical knowledge for electronic delivery of E-learning Activities;

(c) maintain back-up and recovery systems for E-learning Activities in case of system failures or other technical problems;

(d) ensure that all personal data are kept strictly confidential and protected, and not to be released to any other parties for any other usage. They should be responsible for complying with relevant data privacy legislations and maintaining all kinds of security needed to ensure privacy for the data transmission is preserved; and

(e) keep relevant audit trail records of the users for at least 4 years and such records should be available in a legible format for inspection by the IA upon request.

3.1.7. Activity Design

3.1.7.1. E-learning Activities should illustrate **a degree of interactivity** between the users and the learning materials to enhance and reinforce the learning process. For instance, users can be asked to answer small quizzes throughout the E-learning Activity so as to enhance their attention and interest. It is helpful to provide users with the correct answers to the quizzes with full explanation to facilitate learning.

3.1.7.2. **Effective online support** should be available including prompt and thorough response to enquiries, provision of guidance to individual learners upon request, etc. E-learning Activity Providers should provide timely online help to users when the users have any questions or difficulties in using the E-learning Activity or the learning management system. Such online support should handle users' enquiries about technical issues (e.g. users might have problems logging in the learning management system), and contents of the activity (e.g. users might have questions concerning the contents of an E-learning Activity). It is expected that E-learning Activity Providers should have sufficient human and financial resources with regard to subject expertise and technical know-how to ensure that online support is provided as soon as reasonably practicable or within the next working day, at the latest.

3.1.8. Warning against impersonation

3.1.8.1. E-learning Activity Providers should explicitly warn all users before the start of each E-learning Activity that impersonation, or any other incidents of allowing an impostor to take E-learning Activity on the users' behalf for the purpose of claiming CPD hours under the CPD Guideline, will be reported to the IA and/or other law enforcement agencies. Such incidents may adversely affect the fitness and properness of the persons involved and may result in a disciplinary action to be taken by the IA against these persons.

3.1.8.2. E-learning Activity Providers should report to the IA all incidents of impersonation or abuse involving individual licensees as soon as reasonably practicable.

3.1.9. Off-the-shelf E-learning Activities

3.1.9.1. Where a Principal (i.e. an authorized insurer, a licensed insurance agency or a licensed insurance broker) or an organizing body acquires off-the-shelf online learning courses from e-learning course developers, instead of developing its own E-learning Activities, the requirements applicable to E-learning Activities as set out in sections 3.1.1 - 3.1.8 apply equally to off-the-shelf E-Learning Activities.

3.1.9.2. The Principal or the organizing body concerned should monitor the quality of such off-the-shelf E-Learning Activities.

3.1.9.3. If a secured login and continual identity-checking system in compliance with sections 3.1.1.4 – 3.1.1.6 is not embedded in an off-the-shelf online learning course, the Principal/organizing body should adopt the measures set out in sections 3.1.1.7 - 3.1.1.8.

Insurance Authority
September 2019