More and more emphasis is being placed worldwide upon certification. Suzana Lopes explains the need for rigorous exam security, and looks at how it is done today.

Increasing numbers of companies and organisations insist on their staff holding the correct, up-to-date, industry-recognised qualifications for many reasons. Candidates that are certified to a higher level have proven that they have the competencies and skills to deliver higher-value services for their company. A better, higher qualified workforce gives a company a competitive advantage: training and certification add value to companies and give reward and motivation to employees.

The IT sector is a perfect example of this, and it has been leading the way in terms of training and testing of skills. Because of the rapid pace at which technology is evolving, it is vital that people’s knowledge and skills keep up.

Often, whole careers hinge upon the passing or failing of a high-stakes test. If a test or exam is to be truly meaningful, it is of course imperative that the most rigorous security is applied at every stage, to ensure that candidates are who they say they are, and that their performance in the test is based solely on their own efforts rather than by cheating. The number one threat to test security is test content theft, whereby the test taker memorises as much of the test content as they can and then makes it available, for example, by publishing it on the internet, frequently for commercial gain. Secondly, and also a significant threat is proxy testing, also known as test fraud through impersonation; where the test taker gains an unfair advantage by hiring someone else to take their test for them.

This is an important matter to training providers too. If the certification standard is compromised then so too is the value in training for that certification. If it were possible to pass a test via some illicit short cut, then of course fewer people would pay for training.

Thankfully, much technology exists to ensure security for the whole life cycle of a test. From the creation of the items (questions or tasks) and their use in exams, through the delivery at the test centre, to forensic analysis of exam results, there are proven procedures to make sure content does not fall into the wrong hands or risk being misused.

Secure test development
Firstly, owing to the complexity of the modern test, many people are involved in creating it. It is not simply a case of one chief examiner deciding what the questions should be: the creation process involves input from many people – from psychometricians to analyse the reliability and validity of the items and exams, to subject matter experts to keep a check on the accuracy of content – plus it needs to be cross-checked for use across geographical, cultural and language boundaries. Many tests also involve the cooperation of employers and organisations to ensure that certifications are aligned with the job roles they are testing for.

Thanks to the size of this panel of experts therefore, test items need to be created within a secure environment, using
appropriate workflow management controls, tracking items through the development process, with all those on the panel requiring role-based access rights. The item creation workflow can be designed allowing as few individuals as possible to have access to the final, live item bank. By these methods, awarding bodies can be confident that their sensitive exam content will remain known only to those authorised individuals on a need-to-know basis. But it is once the exam is published that the larger threats become a danger.

Just as a chain is only as strong as its weakest link, so too is a network of test centres. The first concern when publishing a test is that the distribution is sufficiently safe. Systems including operational procedures in every test centre must be standardised, regardless of where they are in the world, because should just one of them leak, a test that has cost much time and money to create could be rendered invalid.

Global identity management
Because much IT testing takes place on a global scale, it’s critical for IT organisations to identify candidates in a way that deters cheating, yet can be managed efficiently across multiple countries and multiple test centres. Testing organisations should not allow a candidate to test unless they can be identified by at least a recognised government-issued ID bearing a photo and signature, such as a driver’s licence, national ID card or passport. Ideally, test centres should also capture a digital photograph and signature as part of the permanent record of the candidate’s testing session, for subsequent review in the event that test fraud is suspected. Further, publishing the candidate’s photo on a score report or to a secure website allows employers and other interested parties to verify that the person who actually took the test is the person pictured with the test results. These measures allow test centres to provide a superior level of security without compromising candidate convenience.

Palm vein recognition
For the highest of high-stakes IT exams, such as those related to a top-level certification, some organisations are choosing to test in centres featuring the most state-of-the-art test centre technology available for candidate identification-palm vein recognition. With fewer negative cultural connotations than fingerprinting, and greater accuracy, palm vein recognition involves an infrared scanner that examines the unique patterns in the veins of the palm of a candidate’s hand. This streamlines the check-in process and gives each candidate a single record that is virtually impossible to forge or tamper with, thereby eliminating the possibility that multiple people could test under a single identity.

The palm is scanned, and the information about the individual’s unique vein patterns is stored as an encrypted digital template. After the test is complete, this template is sent along with the test-taker’s results via encrypted transmission to the testing company. Because of its accuracy, ease of use and built-in privacy controls, palm vein technology is increasingly being recognised as the most secure, protected method of verifying candidate identity in high-stakes testing environments.

Item banking
Having verified that each test-taker is the genuine candidate, there is then the consideration of making sure that test content cannot be taken from the test room and passed on to future candidates for cheating purposes, or posted on an online ‘brain dump’ site. This is where the computer-based testing (CBT) concept of item banking comes into its own. A paper-based test form can only be delivered once before the content is considered public knowledge – cheating in subsequent sittings would be easy if that paper were to be re-used. With CBT item banking however, the testing body can select items from a suitably sized computerised item bank and create a new test form each time. Firstly, this means that a number of different tests can be compiled from the same item bank, and that each item can be used more often because the software controls how much exposure each item gets. As long as items do not become stale or over-exposed then candidates will not become able to pass them too easily.

Secondly, it means that on any given day, every candidate could be sitting a different test, containing a unique mix of items that add up to a test of the same difficulty level as the one being sat by the next candidate. With this model, the test could be available for candidates to sit at their convenience on any day of the year, without every test requiring all-new items to be created, and because every test is different, no candidate can take the short cut of completing a test from memory of a ‘past paper’. On top of this, any unscrupulous individual would not stand to gain anything from leaking or selling exam content after their test, as it is highly unlikely that the same content will occur in the same combination in other people’s sittings of the same test.

Even with security measures such as the above in place, testing providers must always still monitor all tests to look for any aberrant trends or to detect if the test has been compromised in any way. There are many tools that can do this, both while the test is live and also after the fact. For example, forensic analysis software can detect any unusual patterns in scores, pass rates or other aspects of the test (such as how fast the candidate answers different types of questions, or how well they perform on easy questions compared to difficult ones). This analysis can be performed immediately following each test so that aberrant trends can be quickly identified and action taken to minimise further risk while further investigation or other action takes place.

It is thanks to security like this that modern computer-based testing, as used in almost all IT certification, can be trusted as a reliable proof of an individual’s skills and competencies, and those individuals can be confident that their qualifications gained in this way really mean something.

Suzana Lopes is EMEA VP Sales and Marketing at Pearson VUE (www.pearsonvue.co.uk), a global leader in computer-based testing for information technology, academic, government and professional testing programmes around the world.

Pearson VUE provides a full suite of services from test development to data management, and delivers exams through the world’s most comprehensive and secure network of test centres in 165 countries. Pearson VUE is a business of Pearson (NYSE: PSO; LSE: PSON), the international media company, whose businesses include the Financial Times Group, Pearson Education and the Penguin Group.

www.pearsonvue.co.uk