Risk assessment for award of certificates

Return to index **[1]**

QCF 5.14 - 5.16

QCA 6.1

Purpose of qualifications

1. The key issue is the authentication of the qualification. A qualification provides information about the capability of an individual in a particular field. When an individual claims to have a qualification how can its authenticity be verified? There have been well-publicised cases of people teaching and even performing major surgery with no qualifications. The first issue is how easy it is to verify someone's claim to be qualified?

Authenticating the certificate

2. The traditional method is for the candidate to declare that they possess the certificate (eg in a job application form) and then the interested parties can choose to verify whether or not this is the case. The first point of failure is when the individual claims to have the certificate and no-one checks the veracity of the claim. There is no means of dealing with this situation and it is the same for any qualification. The next potential point of failure is when the candidate produces a certificate that is not valid, a forgery that is accepted on face value and not checked. This is far more likely to succeed if the verification process is not free and immediate because verification then takes some effort. If a paper certificate is convincing it is very unlikely to be checked and with current inexpensive computer graphics tools forging a paper certificate is very easy to do. In the age of computers the record of the certificate in a database defines the certification, the paper copy of the certificate is simply a convenient means of representing the verifiable computer record without having to go to the computer to verify the contents of its database. The Internet changes this because of the ubiquitous access to computer terminals that can make secure access to databases anywhere in the world. Whether a paper or electronic certificate, if the certificate is checked back to the Awarding Body it is almost certain that the Awarding Body will check the name of the candidate and the certificate number against entries in its database. In effect the paper certificate is simply a representation of the information in the database. With modern communications technology it is straightforward to authenticate any certificate directly in the Awarding Body's database over the Internet. If any certificate is not verifiable in this way there is a much greater chance that forgeries will be accepted and this is probably the most significant potential point of failure.

Obtaining certificates by deception and identity theft

3. The next stage of vulnerability is a significantly lower risk. If a certificate is authenticated against a database entry, how can we be certain that the holder of the certificate is the same person that was awarded the certificate? Whether it is an entirely paper based system or an electronic system the candidate would first of all have to have the same name as the true holder of the certificate and would have to know the certificate number. This alone makes the risk much lower but identity theft is still an issue. The only real means of verification is to cross-reference against other personal details that would be specific to the candidate, such as who made the assessment and where and when it was made. Date of birth or Unique Learner number could be other points of reference. Photographic evidence or other personal records at the centre where the assessment took place might also be used. An audit trail with such information is only likely to be followed up in any system in cases where there is real suspicion about the candidate. It would be possible to attach a digital photograph of the candidate to the certificate but the benefits of doing this have to be weighed against the additional time, expense and inconvenience to all assessors and candidates for relatively few cases that would ever get used. On balance being able to directly authenticate the certificate

from any web browser against entries in the Awarding Body database, with scope to follow through an audit trail to who awarded the certificate, appears to be a good compromise and at least as robust as most systems to date.

Errors in assessment or security of data entry

4. A fundamental source of risk is in the ability of the assessor to make an accurate judgement that truly reflects the capability of the candidate. This is tackled by moderation and training and is inherent to any system of assessment. Assuming that the assessors have sound judgement they then pass on those judgements in the form of marks or grades and these are processed and then converted to the awards which are then entered into a database. Whenever this type of information is recorded and passed on there is scope for error. It therefore makes sense to reduce the number of transactions to the minimum possible. Direct transfer of the assessment judgement by the assessor into the Awards database minimises risk in transcription errors but raises the risk of security breaches through incompetent use of passwords. The trade off is then which is the biggest source of risk? If we assume that at some point someone will have a password compromised and some other individual will gain access to an Assessor's account, what is the scope for damage? First of all if the security of the system is sound access will only be gained to the students of that particular assessor. If the system does not allow deletion, there is no way that the person breaking into the account could delete anything. They could register new students but presumably the assessor would know which students were not their own and could then E-mail the awarding body who would then delete the bogus names. The intruder could add new awards to existing students but as long as the assessor realised that the system had been compromised, the system manager could revert it back to the state it was in before the security breach. Finally, the intruder could try to create themselves an award but this would fail because all Awards require independent authorisation by the Awarding Body. It would be far simpler to get a paper certificate from a friend, scan it into a computer and add their own name in place of the legitimate owner. On balance the convenience and reduced risk of transcription and transfer errors outweighs the small risk of compromised passwords leading to bogus awards, especially if the users are professional people trained in the importance of using secure passwords. We can also only allow reasonably secure passwords to be used by programming the system to reject weak passwords automatically. It is still important to impress upon the assessors the importance of password security but this is no different from when they deal with on-line banking or similar on-line transactions where there is valuable information at stake.

Further evidence

5. In practical ICT qualifications where students are required to document their work through Web-logs and similar on-line methods, the evidence can be used to make sure that the work actually took place. In the previous scenario, if an intruder created themselves a certificate which was dependent on the evidence of a Web-log or recorded discussion via E-mail, the lack of any record of these would determine that the entry must be bogus. This is again easily verifiable using the Internet. Since the criteria for awarding certificates can be made easily available to any web browser, it is also very easy to check a candidates familiarity with the criteria against which they are supposed to have been assessed.

Return to index **[1]**

Links
[1] https://theingots.org/community/ofqual_policies

-->