ICT Systems policies, procedures and risk

Return to index **[1]**

IT Systems Policies and Risk

1. Introduction

The IT systems policies are designed to achieve best value and to **reduce risk**. They need to be considered in the context of the Awarding Organisation functional context rather than as separate isolated provision. There are two key sites relevant to the Awarding Organisation function, the certification site and the community learning site. The certification site is the most significant as this is where awards are made and the assessment data related to those awards, stored. The community learning site is used as an optional facility for managing evidence and tracking progress adding value through support for assessment for learning. It can be used to input data to the certification site but it is not mandatory. Dependency on it would be a problem in some environments eg the prison service.

The following two strategies underpin these aims

1. Use of Linux based and open source systems to reduce costs and **risk** associated with dependencies on single points of supply
2. Use of the cloud and out-source of data hosting to **reduce risk associated with physical threats** to buildings and benefit from the economies of scale of using the web.

2. Operational Strategy

2.1. Security

All critical systems are patched regularly by the hosting company, United Hosting [2]. There is a dedicated server hosting the systems and these are backed up 4 times per day. Internal systems are patched as soon as security updates are notified as being available. United Hosting host over 70,000 sites and has a good reputation for reliability and security. TLM's dedicated server with United Hosting is the location of theingots.org domain containing the main data associated with the awarding function. Transactions with the server are done through encrypted HTTPS requests.

This leaves the main potential **risk** from a security vulnerability as the password. Password strength is metered and only secure passwords are allowed. These require the use of letters, numerals, characters, upper and lower case and reasonable length. Users that have insufficiently strong passwords will not be able to set up accounts. The most significant **risk** is in user error either leaving themselves logged in and leaving the system unattended or allowing others to find their password. The **risk** assessment shows that this is almost certain to happen at some time and is by far the greatest security vulnerability. The following actions have been taken to reduce possible damage.

- Timed automatic log out so that the system will auto log out if in active for longer than a set period.
- Permissions that limit most users to editing a single account.
- Facilities for data recovery should an account be compromised.
- Education through training and aspects inherent to TLM qualifications.

Example scenarios/use cases

- If an intruder gets into the system and deletes records in the certification site they are not

actually deleted, rather they are simply rendered invisible. The system manager can restore such damage very quickly.
- An intruder awarding grades to their own or someone else's account is likely to be noticed by the assessor. Data stamping of records enables us to determine when such an intervention took place.
- No awards can be made without authorisation by the Account Manager so while additional marks could be inserted it would not be possible to make an award without communication between the Account Manager and the legitimate assessor owning the account.
- On the community site, a learner or assessor leaving themselves logged is could have their pages deleted or altered. However, there is a versioning systems so all new pages are date stamped and the system can be reverted to earlier versions of pages. Should this be ineffective backups are available from which to retrieve work. This is certainly a better situation than a candidate losing a paper based file which would have no back up and no possible way of being restored.

Security testing

- Periodically we will test the security of the hosted systems with typical attacks such as dictionary for passwords.

Service outage

- United Hosting servers have an average of 99.99+% uptime, based on an independent review service (HyperSpin)
- Outages have occurred but none has caused serious disruption
- If an outage does cause a significant disruption we will ensure that any assessment affected is reviewed to ensure fairness to candidates

We are currently considering setting up a local backup facility so that in the event of a significant outage at UH we could temporarily host the sites from TLM. In any case, short outages tend to be inconvenient rather than catastrophic and the worst case scenario of losing the UH service entirely and permanently is to be back on line within 24 hour. Currently, none of TLM's qualifications is tied to a specific time point therefore there are no key deadlines that if missed by 24 hours would lead a candidate to miss the opportunity to get the qualification. In terms of **risk** assessment, the fundamental **risk** to delivering a qualification is having a specific critical time where the candidate has to participate.

In 2015 TLM will implement on-line testing as part of a level 2 qualification that is eligible for headline performance points. This has been field tested with a non-acredited football qualification based in Singapore. The security in delivering the test is designed to have minimum points of failure. (More details on this below) There is a trade off in **risk** between allowing centres flexibility over the times that different groups sit the on-line exams and the consequent possibility of content leaks and the chance that even a small outage disrupts a timed test for all. If all candidates do the test at a specific time all at the same time, the **risk** of a serious failure is unacceptably high. There will be maximum pressure on the system and concurrent use means insufficient personnel available to support many simultaneous requests for help should they occur. Since all Centres must sign agreements to uphold professional standards before using the systems it is less likley that there will be malicious intent but it would be possible for those attending an earlier exam to give information about the content to a candidate taking a later paper. Having more than one version of the exam, such that candidates taking it at the same site at different times get at least a proportion of different questions mitigates the **risk**. By staggering the exam times we also make it easier for centres to manage their IT facilities since a smaller number of terminals is needed and it is less disruptive to time tabling. In considering risk, all of these factors need to be taken into account so that the cost-benefit is sensible in the actions taken. This is both on the supply side, and the centre side in terms of the administrative overhead locally, beyond any qualifications fees paid.

Design of on-line tests and associated security

Delivering a test through a computer can be done in three principle ways

1. Download test software to each individual computer and run each instance of the application separately.
2. Download a test to a local network server and deliver the test software from it.
3. Deliver the test directly from the internet.

In most cases to this point, delivery of on-line tests has required installation of some proprietary software application(s) locally, either on the server or deployed to work stations. The advantage of this is that it enables control to be exercised over local machines with specific ways of, for example, using the technology to block access to local resources or internet access. The disadvantage of these methods is that they incur two type of cost. The first is a license cost for any proprietary software not owned by the company delivering the test and the second is in the administrative overhead associated with installing the software. This can be more involved than it first appears since there are many possible systems configurations that could conflict with the software settings. A further disadvantage is that it tends to confine delivery to a single platform, MS Windows at a time when it is actually now a minority computing platform taking into account mobile technologies. There is also the issue of data transfer from the Centre to the Awarding Organisation and the more complex the system the greater **the risk** of data losses. **Risk** is again complicated with associated costs.

We have based TLM's solution to these issues on 3 basic principles

1. All on-line exams will be supervised in the same way as paper based exams making the **risks** comparable.
2. All exams should be deliverable on any platform that has a reasonably up to date standards compliant web browser.
3. There should be no need to download and install software.
4. All centres can opt to take the exam on paper but it will be more expensive reflecting the higher costs of delivery.

What are the **risks** associated with delivering an examination through a standard web browser?

The most obvious is internet access and searches. It is very difficult to use a software solution to this because if it was easy to install software directly from a browser on a local machine there would be nothing to stop malware being deployed in exactly the same way. There is a more elegant solution. Restrict the user to a specific area of the screen while taking the test and disable keyboard shortcuts that enable the user interface to be bypassed. The user only needs the alphanumeric keys in a test and we can detect any movement of the mouse. By restricting the operating area on the screen it makes it impossible for users to access other resources and with supervision it reduces the **risk** to the same level as in a conventional paper based exam. The system is designed to control the release of the test questions to specific times and only to enable access to particular tests authorised for the particular candidate at a particular time. Results are transferred directly to the server so the **risk** of data loss through a local machine crash is minimised. Some types of question can be marked automatically eg multiple choice and that reduces the risk of transcription errors as well as costs associated with stationery and mark readers employed in more conventional settings. Extended and open ended answers are linked to mark schemes and systems management to make marking tests more efficient, again lowering costs and mitigating human error.

Evidence managment and submission

The evidence managment system on the community learning site is optional. It supports self-assessment, peer assessment, independent local assessment and verification and external verification and moderation. Centres can use as much or as little of this system as they want. The most significant **risks** with these systems are more relatated to human factors than the technology. If a learner submits work as evidence the assessor must be confident that it is the student's own work and that it supports the assessment criteria appropriately. All assesors sign an agreement to uphold these standards and this is part of the initial training as well as handbook documentation.

Copying chunks of text from the internet is on the face of it a high risk. However, it is just as easy to check this as to do it. Try copying and pasting the following "Ofqual's Chief Executive is Glenys Stacey, who was previously the Chief Executive of Standards for England" into a search engine. It will find that string immediately as an entry in Wikipedia. If assessors do this periodically and show candidates how easy it is to detect plagiarism, they are much less likely to try it. The likelihood of getting caught reduces **the risk** of this type of malpractice. The evidence management system also provides a record and audit trail of coursework and since it is always available on-line, any of it can be externally checked at any time by moderators and at low cost. This again reduces **risk** by making it less expensive and easier to make checks.

3. Choice of platforms

It is clear that the IT platform most vulnerable to virus and malware attacks is MS Windows. This is partly because it has the biggest user base but also due to a past history of lax security in the design specification. For these reasons the company adopted the Ubuntu GNU/Linux platform for all desktop use at the time it started its awarding function. One machine runs MS Windows for testing the web sites with Internet Explorer. The legacy Windows server is still used for the company accounts but all other critical data is stored on hosted servers with web access. The accounts are backed up to a removeable drive that is taken off site and a separate cloud based repository which is itself synced back to a local drive on a laptop that is normally taken off site. The longer term intention is to move entirely to web hosted services. With web based archives backed up across at least two independent service providers.

In summary the formal policy is to move entirely to open systems delivered from hosted servers using the web. The economies of scale mean that out-sourcing the infrastructural provision has significant cost-benefit. Control of the development is, however, maintained in-house with specific elements contracted out to **low risk** suppliers with whom we have long term established relationships. We are confident that the current systems can scale to any requirements without too much difficulty. The main issue is in having the volume of business to justify the increased costs.

4. Maintenance

There are two aspects to maintenance. The fundamental infrastructure maintenance; provision of servers, server side software and its maintenance and the maintenance of TLM specific systems such as the on-line mark book and the community site.

The on-line mark book is maintained and developed using a LAMP stack approach and the code is managed using DARCs. The community site is maintained through a combination of administrators and users since the whole point of the community is to encourage user generated learning resources. This site currently has over 33,000 pages many of them user generated. The maintenance is out-sourced to a consultant in Mongolia who spent two years workiing with TLM after his MSc at Birmingham University. **Risk** is lowered by having a second technical expert on-site and TLM has out-source contacts eg in Bulgaria that have the appropriate skills set to take over.

5. Monitoring

The Open Source principle "Many eyes make bugs shallow" is employed with user feedback encouraged to enable improvements, fault finding and bug fixes. All TLM members monitor the use of systems and discussions related to improvements are discussed regularly both informally and in formal evaluation reports. Monitoring of mailing lists and forums will alert technical support staff to any need to review the malware policy. Local systems are patched routinely from monitoring alerts for security updates. At present this together with training in sound user practice reduces any need for for anti-virus and anti-spyware software. This results in further savings. In recent times we have been approached by other awarding organisations about the technological approach and this has provided an opportunity to show othrs and get feedback on the systems. This again helps reduce **risk** of "group think" within the organisation.

6. The certification site

The certification site is managed using software applications provided by United Hosting. The code developed by TLM is managed through the DARCs distributed revision control system. Any changes resulting in code development that will affect end users must be agreed with the Chief Assessor or Senior Account Manager before implementation. Test and development sites are used for protyping that are completely separate from the active site. The password systems built into the certification site mean that weak user passwords are not allowed. The Technical Support Manager is responsible for the configuration and general technical management of the Certification Site including issues of security and ensuring software is appropriately up dated.

7. The community site

The community site is an optional resource made freely available to the community. It is not as critical as the certification site but it does contain learner work. (They are advised to keep their own back ups of important files) The software environment of the community site is Drupal. When a significant upgrade is to be performed, it will take place during the summer vacation period when there is lowest usage. The procedure is to check that current modules needed for current operation are available. If they are, a test site is created to test migrating current data to the new version. Testing of the data migrated to the new environment is then undertaken over a two week period with TLM staff performing typical user operations. Any problems are rectified. Once the test period is ended a meeting is held of all staff to confirm that the migration should be continued. If there are any objections these must be resolved before implementing the change.

Minor changes to the configuration of the community site eg to the Primary Links menu, must be notified to the Chief Assessor before implementation. Changes to news items and general information can be made by the Office Administration team as appropriate. The Director of Administration and Finance vets all account applications for the community learning site to prevent spammers and advertising pests setting up accounts. This is in addition to the normal captcha facilities.

8. Workstations and mobile technologies

The configuration of individual workstations and mobile technologies is left to the individual but must as a minimum include the default firewall settings. Windows systems must be protected by up to date anti-malware software.

9. General information strategy

Some information needs to be secure, other information is intended to be spread widely. The strategy is to provide systems that treat information appropriately for its intended use and is not bound into proprietary and closed technologies. This is an inherent part of the TLM qualifications development. There are a collection of policies related to these issues from the Creative Common Share Alike licensing of much of the information on the community site to secure private web pages for management meeting minutes to the complete separation of the certification site from general use. TLM is registered with the Data Protection registrar and provides information to educate users about safe and secure use of digital information. There is an inevitable balance to be struck between making information available to promote learning and sharing and restricting information for privacy and safety. Achieving this balance is a significant feature in the overall information strategy. In the world of global digital communications we are trying to move away from business practices based on file attachments and technologies that were designed for a world where digital information systems relied on replicating and moving information rather than holding information centrally and making it available to relevant parties on demand. This does depend on the business processes of other people since communicating information is bi-directional. It is in the interest of all who want to reduce the costs associated with the awarding process to maximise the use of internet based technologies and move away from proprietary desktop applications. In the World of HTML 5 and beyond, the standards compliant web browser can replace most expensive and cumbersome

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

desktop office applications.

10. Procedures for dealing with technical issues

Technical issues fall into 2 categories

1. Urgent
2. Important

Any issue that affects users ability to log in and use the system should be treated as Urgent and important and reported in the first instance to the Director of Administration. The DoA will assess the situation and take such action as is necessary to resolve the issue as soon as possible. Progress should be made public by posting a message on the front page of the web site explaining the situation and estimated time of resolution.

If notified by the DoA the Technical Manager will make resolution of the problem the first priority and will draw up on such support from other members of the team or externally as deemed appropriate.

Issues that are important but do not have an immediate effect on users will be triaged by notifying the DoA. She will decide on the urgency of the issue and allocate time and expertise to it determining the priority against other issues and the general business of the organisation.

11. Procedure for dealing with physical issues related to the building

Any defects or problems with the fabric of the building should be notified to the DoA as soon as they become apparent. The building should be maintained securely with external doors shut and requiring a key for entry. Any local data that is critical to the business will be backed up with copies taken off site and held in a secure place by a designated member of staff. This policy is to ensure security of company assets. The DoA will decide on the urgency and importance of the issue and allocate the appropriate time and resources to them. In a case where the building becomes uninhabitable we will set up a temporary base in at 36 Ashby Road. Should damage to the internet connection be terminal, use of cellphone 3G internet access from netbooks and laptops will keep workflow and telphone numbers will be diverted to cell 'phones.

In any such case, where there is likely to be any prolonged degradation of the service provided, the DoA will inform Ofqual, LRS, Bathdata and post a notice on the web site front page for customers.

12. Disaster recovery policy

A disaster is a specific case of technical, human or physical failures that if unaddressed will halt or seriously impair the function of the business. The key risks are:

People

Incapacity of key personnel. No single person is so critical that the general business could not operate. However, if all personnel were to be incapacitated at the same time there would be a significant problem. Since there are no times when all are in the same place at the same time this is not very likely but it is the most serious risk to cessation of the business. The only way to recover from such an extreme disaster would be to co-operate with another Awarding Organisation to maintain continuity. There is sufficient documentation to enable a professional to take over and manage the TLM business and we have appropriate relationships with collegues in other awarding organisations.

Destruction of the buildings

Destruction of the place of work would be traumatic and the greatest impact would most likely be the emotional effect on the people. In physical terms the business could be run almost immediately in the short term from any location as all the critical information is on-line. The disaster recovery policy is to target all possible resources to maintaining continuity of service while alternative premises are acquired.

Loss of IT systems

Should there be a total loss of all IT systems and data, (unlikely given the hosting and backup strategies) the policy is to contact all customers and explain the situation. The regulators would be informed and proposals to accept data collected by the centres as a normal part of their business used to minimise the impact on learners and their certification. The data recording structures can be restored from backups and repopulated should the customers have their own data backups. It is impossible to gauge the extent to which evidence of attainment against the assessment criteria would be available but the first priority is to protect learners from losing credit.

13. Disposal of assets and data security

Any computer hardware which has hosted sensitive or confidential data will be treated appropriately to make the data inaccessible to third parties. As a minimum, drives will be low level formatted and filled with new random data before disposal. In cases where the hardware is to be scrapped, or in cases where the data is judged to be critically confidential the hard drives will be physically destroyed to make data retrieval impossible. To dispose of sensitive data assets held on-line, a file of the same size and name as the original, filled with random data will be uploaded to replace the file containing the sensitive data thus destroying the sensitive data. Backups are recycled every 2 weeks and therefore back up data will be destroyed on a 2 week cycle. In general, sensitive data should not be stored or transferred on USB keys, CDs, discs and other removable media. Using a secure network connection and strong passwords is generally a more appropriate approach than copying data as the policy is to keep copies of sensitive media to a minimum.

Audit and review

Systems will be under constant scrutiny and review with evidence gathered from customers and the community as well as staff. The great majority of staff are IT literate at graduate level or above. Nevertheless systems and methods are discussed with independent external colleagues to ensure that good and affordable practice is in place. A formal independent audit will be invoked if there is evidence of need.

14. Cookie Policy

The cookie policy [3]is designed to meet the new PECR act [4]derived from EU e-privacy directive 2009. [5] up dated on 26 May 2011.

Return to index **[1]**

-->

Links
[1] https://theingots.org/community/ofqual_policies
[2] http://www.unitedhosting.co.uk/testimonials-and-awards.php
[3] https://theingots.org/community/cookie-policy
[4] http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications.aspx
[5] http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/09/13&format=HTML&aged=1&language=EN&guiLanguage=en

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');