Level 3 - Unit 4 - IT Security for Users (3 credits)

Platinum - Unit 4 - IT Security for Users

Relevant LINKS

BACK TO ITQ UNITS **[1]**

Handbook home page **[2]**

Overview (Under Development)

The candidate can understand and use the correct procedures when working online and will be able to monitor and adjust those procedures to make sure they are fit for purpose. They should also be able to understand what causes systems performance issues and work towards fixing these. They should be capable of carrying out a basic threat analysis and deploy various tools and techniques to minimise these threats.

A work activity will typically be 'non-routine or unfamiliar' because the task or context is likely to require some preparation, clarification or research to separate the components and to identify what factors need to be considered. For example, time available, audience needs, accessibility of source, types of content, message and meaning, before an approach can be planned; and the techniques required will involve a number of steps and at times be non-routine or unfamiliar.

Example of context – an example might be to carry out a systems threat analysis project for a local business, draft a recommendation and oversee the implementation of some possible fixes.

Activities supporting the assessment of this unit **[3]**

Example of work at this level **[4] (coming soon)**

Assessor's guide to interpreting the criteria

General Information

QCF general description for Level 3 qualifications

- Achievement at QCF level 3 (EQF Level 4) reflects the ability to identify and use relevant understanding, methods and skills to complete tasks and address problems that, while well defined, have a measure of complexity. It includes taking responsibility for initiating and completing tasks and procedures as well as exercising autonomy and judgment within limited parameters. It also reflects awareness of different perspectives or approaches within an area of study or work.

- Use factual, procedural and theoretical understanding to complete tasks and address problems that, while well defined, may be complex and non-routine.

- Address problems that, while well defined, may be complex and non-routine. Identify, select

and use appropriate skills, methods and procedures. Use appropriate investigation to inform actions. Review how effective methods and actions have been.

- Take responsibility for initiating and completing tasks and procedures, including, where relevant, responsibility for supervising or guiding others. Exercise autonomy and judgement within limited parameters information and ideas

Requirements

- Standards must be confirmed by a trained Platinum Level Assessor or higher
- Assessors must at a minimum record assessment judgements as entries in the on-line mark book on the INGOTs.org certification site.
- Routine evidence of work used for judging assessment outcomes in the candidates' records of their day to day work will be available from their e-portfolios and on-line work. Assessors should ensure that relevant web pages and files are available to their Account Manager on request by supply of the URL.
- When the candidate provides evidence of matching all the criteria to the specification subject to the guidance below, the assessor can request the award using the link on the certification site. The Account Manager will request a random sample of evidence from candidates' work that verifies the assessor's judgement.
- When the Account Manager is satisfied that the evidence is sufficient to safely make an award, the candidate's success will be confirmed and the unit certificate will be printable from the web site.
- This unit should take an average level 3 learner 50 hours of work to complete.

Assessment Method

Assessors can score each of the criteria N, L, S or H. N indicates no evidence. L indicates some capability but some help still required. S indicates that the candidate can match the criterion to its required specification. H indicates performance that goes beyond the expected in at least some aspects. Candidates are required to achieve at least a S on all the criteria to achieve the full award.

Expansion of the assessment criteria

1. Candidates will select, use and develop appropriate procedures to monitor and minimise security risk to IT systems and data

1.1 I can evaluate the security issues that may threaten system performance
Candidates should be able to evaluate any IT system and list and describe the main threats.

Evidence: will be provided by guidelines and portfolios.

Additional information and guidance

Most IT systems are threatened by the same types of security issues, but perhaps in different amounts. The main types of threat are physical: people breaking in, physical damage to hardware, or existential, which are external threats such as hacking, malware, viruses and other Internet born problems. Some of the threats might not be that obvious. It is estimated that millions of home computers are infected with Botnets and the users are unaware of their presence. In 2004, a number of these machines were controlled remotely to launch an attack on US government sites such as the White House website. All of these additional pieces of unwanted software cause performance issues on machines and the servers that are linked to them. If a devices is compromised and sending out spam, this volume will slow down servers up the line as they try to process the extra communication volume. Other elements need to be explored and described and some idea of their overall impact shown with examples.

1.2 I can select, use and evaluate a range of security precautions to protect IT systems and monitor security
Candidates should be able to explain, with examples, some tools that will minimise problems.

Evidence: will be assessor observations and student portfolios.

Additional information and guidance

Depending on whether the candidates are protecting one machine or a network, will determine what systems and tools they evaluate and use. Most modern operating systems have some type of software defense. A home or school network will also have some type of hardware defense, such as firewalls or filters. They might also look at stronger measures such as root kit detectors on servers such as Fail2ban [5] which looks for rogue code installs and isolates and removes them. Monitoring tools are also available and many open source ones monitor thousands of servers such as Nagios [6]. They should address the basic security issues above such as physical and external and give examples of how these can be addressed effectively.

1.3 I can evaluate the threats to system and information security and integrity
Candidates should be able to evaluate the different kinds of threat and rate the need to stop them which will therefore inform further action.

Evidence: will be provided by candidate feedback and assessor observations

Additional information and guidance

Evaluating some of these threats might sometimes mean prioritising them in terms of their likelihood and potential damage. It is likely that the data help on a local school system may not be as tempting and valuable to criminals as the bank in the town centre. None the less, candidates need to show that they can make these judgements based on their knowledge and gathered evidence. It may be useful to carry out a security audit and note down the threats, how they are currently dealt with, if there are room for improvements and any other relevant suggestions.

1.4 I can manage access to information sources securely to maintain confidentiality, integrity and availability of information
Candidates should show an understanding of roles, responsibilities and access rights on networks to aide security.

Evidence: will be portfolio evidence.

Additional information and guidance

Related to 1.3 above, an audit of the type of data and the way it is accessed will give more detail to a security exercise. The school's central database, for example, might be the most important aspect of the school system so will need the most detailed protection or range of systems. Related to other units, such as Unit 3, they should show that they know what access rights, roles and permissions are required by people in a complex network to maintain integrity and confidentiality. They should also have some understanding of availability, for example should data be accessible outside of the local

(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');

network. If so, how can it be carefully protected.

1.5 I can explain why and how to minimise security risks to hardware, software and data for different users
Candidates should be able to explain roles and responsibilities and threats to software and hardware.

Evidence: will be candidate portfolios and assessor feedback.

Additional information and guidance

Each part of a network will have different threats and therefore different needs. The main threats to hardware will be physical. Most servers in a school, or local computers, for example, will be locked uop in some way. In small school, they often deploy secure steel cabinets to lock up their gadgets. The software risks need to be protected from hacking and bad software installations. many organisations have specific policies about software patches and updates as some code can be badly made or compromised and lead to problems. Access to data also needs to be controlled. many schools desktop computers only allow access to controlled areas of the network and some may not allow external USB drives to be used as these can be used to load dangerous software. The software itself is usually controlled by only allowing certain roles to be able to execute code.

1.6 I can apply, maintain and develop guidelines and procedures for the secure use of IT
Candidates should be create guidelines and follow them, as well as instruct others how to

Evidence: will be assessor observations and feedback from network managers.

Additional information and guidance

It might be useful if candidates can assist a local primary school or local business in order to assist them in their security policies and procedures. The candidates can carry out an audit as part of other criteria and develop documents and procedures based on their findings. These can then be implemented and tracked for effectiveness.

1.7 I can select and use effective backup and archiving procedures for systems and data
Candidates should be able to backup and archive systems.

Evidence: will be assessor or network manager feedback.

Additional information and guidance

Various backup and archive procedures need to be investigated and explored and the most effective ones implemented and commented on. The procedures should be carefully explained in terms of their effectiveness and any additional concerns highlighted. One aspect of backups is that they can be very time consuming. If a large system goes down and it was many GB in size, even a fast server and network will take hours to re-build from this data back-up.

Moderation/verification

The assessor should keep a record of assessment judgements made for each candidate and make notes of any significant issues for any candidate. They must be prepared to enter into dialog with their Account Manager and provide their assessment records to the Account Manager through the on-line mark book. They should be prepared to provide evidence as a basis for their judgements through reference to candidate e-portfolios and through signed witness statements associated with the criteria matching marks in the on-line markbook. Before authorizing certification, the Account Manager must be satisfied that the assessors judgements are sound.

Source URL: https://theingots.org/community/sil3u4x

Links
[1] http://theingots.org/community/ITQ_unit_development
[2] http://theingots.org/community/handbook2
[3] http://www.theingots.org/community/ITQcourse1
[4] https://theingots.org/community/sites/default/files/uploads/user4/PupilFNC7.pdf
[5] http://www.fail2ban.org/wiki/index.php/Main_Page
[6] https://www.nagios.com/products/nagios-network-analyzer/