Qualifi Level 5 Diploma in Cyber Security

Specification (For Centres)

August 2018

About QUALIFI

QUALIFI provides academic and vocational qualifications that are globally recognised. QUALIFI's commitment to the creation and awarding of respected qualifications has a rigorous focus on high standards and consistency, beginning with recognition as an Awarding Organisation (AO) in the UK. QUALIFI is approved and regulated by Ofqual (in full). Our Ofqual reference number is RN5160.

Ofqual is responsible for maintaining standards and confidence in a wide range of vocational qualifications. QUALIFI is also a signatory to BIS international commitments of quality.

As an Ofqual recognised Awarding Organisation, QUALIFI has a duty of care to implement quality assurance processes. This is to ensure that centres approved for the delivery and assessment of QUALIFI's qualifications and awards meet the required standards. This also safeguards the outcome of assessments and meets national regulatory requirements.

QUALIFI's qualifications are developed to be accessible to all learners in that they are available to anyone who is capable of attaining the required standard. QUALIFI promotes equality and diversity across aspects of the qualification process and centres are required to implement the same standards of equal opportunities and ensure learners are free from any barriers that may restrict access and progression.

QUALIFI's policy document for learners with specific requirements or who need special consideration is available for centre reference. Centres are responsible for reviewing the applicant's ability to complete the training programme successfully and ultimately achieve a qualification. The initial assessment by the centre, will need to take into account the support that is readily available or can be made available to meet individual needs as appropriate. The centre must also consider prior learning and qualifications and they must be in a position to make a judgement on the learner's entry requirements.

Supporting Diversity

QUALIFI and its partners recognise and value individual difference and have a public duty to promote equality and remove discrimination in relation to race, gender, disability, religion or belief, sexual orientation and age.

Learner Voice

Learners can play an important part in improving the quality of this course through the feedback they give. In addition to the ongoing discussion with the course team throughout the year, there are a range of mechanisms for learners to feed back about their experience of teaching and learning. This can include questionnaires and surveys to allow both centres and QUALIFI to understand how we can improve the learner experience.

Contents

1 Introduction

1.1 Why Choose QUALIFI Qualifications?

QUALIFI qualifications look to provide a realistic and broad opportunity for learners seeking career and professional development. They will support learners in realising their potential and provide clear objectives.

These objectives are to:

- provide career path support to learners who wish to develop their management skills, enterprise capabilities and opportunities in their chosen sector
- improve learner understanding of any given business environments and organisations and how they are managed and developed
- develop skills and abilities in learners to support their professional development.

Our qualifications provide a rich mix of disciplines and skills development opportunities. Learners will gain insight into the functioning, objectives and processes of organisations, appreciating their diversity and the influences and impact of external forces on them. The fast-changing and complex business environment and different organisational ability to stay resilient and respond positively to change and opportunities will be explored.

Our qualifications will develop learner ability to:

- apply analytical and evaluative techniques and to enhance those skills
- investigate issues and opportunities
- develop their awareness and appreciation of managerial, organisational and environmental issues
- use management techniques and practices in imaginative ways
- make use of relevant information from different sources
- develop and encourage problem solving and creativity to tackle problems and challenges
- exercise judgement and take responsibility for decisions and actions
- develop the ability to recognise and reflect on personal learning and improve their personal, social and other transferable skills.

1.2 Employer Support for the Qualification Development

The development of these qualifications has been initiated and guided by discussions and idea sharing with a range of employers, providers and existing centres demonstrating the rigor, validity and demand for the qualification.

Discussions and feedback have been taken throughout the development of the qualifications on content, the potential learner audience for the qualification and assessment methods, ensuring a valuable experience and a recognised set of skills, knowledge and understanding is realised.

1.3 Qualification Titles and Codes

These qualifications have been accredited to the Regulated Qualification Framework (RQF) and have their own unique Qualification Accreditation Numbers (QAN). This number will appear on the learner's final certification document. Each unit with the qualifications has its own RQF code. The QANs for these qualifications are as follows:

QUALIFI Level 5 Diploma in Cyber Security: 603/4139/7

1.4 Awarding Organisation

QUALIFI LTD

2 Programme Purpose

2.1 Reasons for the Qualification

The qualification has been created to develop and reward those learners who are looking to or already have chosen a career in a business-related sector.

We hope that centres and learners take the opportunity to learn a great deal from this programme that will provide relevant new skills and qualities.

It is envisaged that this programme will encourage both academic and professional development so that your learners move forward to realise not just their own potential but also that of organisations across a broad range of sectors.

The Diploma is accredited at Level 5 with a total equivalence of 120 credits. It is envisaged that learners completing this Level 5 programme will progress to a university Level 6 Top-Up programme in the risk management field.

2.2 Rationale for the Diploma

The rationale of the programme is to provide a career path for learners who wish to develop their core capabilities within the cyber security and risk management sector. The outcome of the Diploma, which is a recognised UK Qualification, is for learners to develop the cyber security skills required by organisations globally. It is also to provide a pathway via learner credits and potential direct entry into related Level 6 Cyber Security and/or Risk Management Degree programmes.

All QUALIFI programmes create learning that advances the thought leadership of organisations, offering conceptual and practical insights that are applicable in the companies of today and tomorrow.

Furthermore, we look to develop the cyber security team leaders, managers and leaders of the future through the creation and delivery of learning appropriate for that industry.

The qualification will:

- advanced levels of higher education learning
- prepare learners for employment; and
- support a range of senior IT and Digital, Data and Security roles in the workplace.

By 2019, it is predicted that cyber security breaches will cost the global economy $2 Trillion per annum (Forbes). Back in 2015, insurance firm Lloyd's of London assessed cyber breaches to have cost international commerce some $400bn. This multiplication of the economic value of threat and risk (500% over four years) is likely to continue following a wave of mega data breaches, state- sponsored attacks, bespoke malware refinement, and the mainstreaming of IoT (50 billion web- enabled devices: Cisco) and cryptocurrencies. The cyber security market sector has now reached at least $100bn in value (GlobalCyberAcademy.com: 2018). As an exemplar, the median annual wage for Information Security professionals was some $87,000 in the USA by 2012. This is expected to rise by 37% by 2022 (*Bureau of Labor Occupational Handbook 2014-15*).

This Level 5 qualification is potentially unique because it is about 'cyber security' as a workplace management discipline. It is therefore a semi-technical qualification that examines technical cyber security measures as well as the management, project management and leadership skills required to organise internal and external business responses to major incidents (or the threat of such).
Due to the huge economic risks to businesses, sectors, as well as global regions, from specific and dynamic forms of threat vectors, this course programme will provide solid business management and leadership education (including disaster management, project management and business continuity management) within the context of the digital tech and cyber security threat environment. The course programme is designed and delivered by a mix of academics from Business Schools and Security Management teaching roles.

This Level 5 course is especially designed for existing or aspiring organisational executives and leaders who are tasked with responsibility for business resilience, information security, safe

technological innovation, safe and secure change management, HR planning and physical risk management, professionals.

The course is flexible and online. It is easily able to be blended. The programme utilises many case studies from business and public-sector organisations and embeds isomorphic learning into its technical and management education. The programme is particularly suited for those who are already in work. Or those who are seeking to develop a structured management competency in information security, risk management and organizational resilience.

This course particularly suits students who work for large multinational firms, international organisations or widely distributed governmental bodies and agencies. Often our learners might be employees who are responsible for colleagues' and customer data located across several time-zones via diverse, international business IT and telecoms networks and environments. This qualification will therefore also incorporate converged security considerations critical for those leading and managing the protection of people, assets and information, as well as those responsible for the confidentiality, integrity and availability of company data processes. Cyber security considerations have now very much converged with physical security requirements. Due to the course's more advanced technical settings, it is recommended that applicants without any technical experience or understanding of computer networking, network security, programming or security risk management principles, should first complete the Qualifi Level 3 Diploma in Cyber Security Management and Operations, then scale up to the Level 4 Diploma in Cyber Security, before enrolling onto this course programme. Learners seeking to enter a university degree top-up programme will be required to have successfully completed our Cyber Security Diplomas at Levels 4 and 5, and attain the respective 240 learning credits, before their application for a Level 6 Top-Up application with a university can be considered.

The qualification will identify and evaluate practical ways to safely and securely protect people and organisations from cyber-attacks, data breaches and the consequential impacts. This will be done by accessing and researching a wide range of open-source information: websites, specialist books, journals, manuals, news articles, guidance, International Standards, court documents and other materials. Videos, audio, course content, informal exercises and formal assignments will all be provided by the course tutor team.

2.3 Aims of the Diploma

This Level 5 programme provides the opportunity for individuals to develop a more advanced career in a specific area of business or public organisations by developing analytical knowledge and deeper understandings of several core cyber security operational domains. The course will also provide core information security technical and generic management and leadership teaching. Much of this teaching will be directly relevant to learners moving forward into Information Security Management technical qualifications at the higher-end of the industry market, including the CompTIA Security + accreditation and the cyber security industry gold standard: The Certified Information Systems Security Professional (CISSP).

At key points, in each unit, learners will be asked to use their own equipment to practise using, and conduct live exercises on, technical IT hardware and software platforms and apps, including Virtual Machines, Linux OS, as well as working beyond the GUI (Graphical User Interface) and into their own Command Lines.

Learners studying this course via the Global Cyber Academy (globalcyberacademy.com), our Approved Learning Centre, will have free access to its many cyber security industry events, videos, audio and e-library.

This course's core aims are:

1. To equip individuals with the knowledge, understanding and skills required for success in information-security-related employment
2. To enable progression into a university approved Level 6 Degree award
3. To provide specialist study relevant to individual vocations and environments in which learners are currently working, or to which learners are aiming to work within business and public service sectors
4. To develop learners' ability to contribute positively to good and ethical practice in technology and risk management environments, through effectively utilising the practical and theoretical knowledge and skills gained
5. To develop skills and techniques, personal qualities and attributes essential for successful performance in working life and thereby enabling learners to make a positive contribution to their employment and therefore enhance their prospects for promotion and remunerative advancement.

2.4 Learning Outcomes of the Diploma

Learners studying for the Level 5 Diploma in Cyber Security will be expected to develop the following skills during the programme of study:

1. The ability to read and utilise relevant technical and security literature (including threat intelligence feeds), hardware and software, with a proficient or developed competence
2. Understanding: the ability to think independently and solve potential overarching cyber security issues within a business or organisation
3. Apply subject knowledge and understanding to address familiar and unfamiliar problems in the cyber security and digital risk management domains within their workplace and/or sector
4. Recognise the moral and ethical issues of business practice and research; appreciating the need for ethical standards and professional codes of conduct, including in relation to conducting investigations, audits and incident responses
5. An appreciation of the interdisciplinary and interdependent nature of cyber security within wider business and service provision, and broader operating environments and supply chains
6. Capacity to give a clear and accurate account of a subject, in a mature way; engage in credible debate and dialogue both with specialists and non-specialists in relation to cyber security- related issues and challenges

7. To develop transferable skills and knowledge – including in project management, business continuity management crisis management, disaster recovery and management and incident response - which will enable individuals to meet the requirements of, and successfully manage/lead, major business incidents
8. To motivate individuals to progress to further professional development and advancement through future study or as part of their chosen career
9. To instill and embed a sense of understanding and respect of the global nature of the cyber threat environment; as well as the criticality of respecting, anticipating and learning from diverse, international business practices and the global operating context.
10. To engender positive digital citizenship, inculcating an ethos of understanding responsibilities and exercising personal and organisational 'rights' in an ethical, responsible and sustainable manner

These are the overall learning outcomes in line with a Level 5 qualification. The learning outcomes for each of the units are identified in Appendix 1 within the descriptors.

3. Delivering the Qualification

3.1 Quality Assurance Arrangements

All centres go through an approval process to be recognised as an approved centre. Centres must have in place qualified and experienced tutors. The experience of tutors and their ability to support learners will be important. Centres must commit to working with QUALIFI and its team of Quality Reviewers/External Verifiers. Continuing professional development (CPD) for tutors is also required.

Approved centres will be monitored by QUALIFI External Quality Reviewers (EQAs) to ensure that learners are provided with appropriate learning opportunities and guidance. EQAs will ask to see and discuss a centre's formative assessment plans. The suitability of these plans will be agreed with the centre.

QUALIFI's guidance on invigilation, preventing plagiarism and collusion will apply to centres. QUALIFI Quality Reviewers/External Verifiers will monitor centre compliance. For assessment purposes, unless otherwise agreed, QUALIFI:

- appoints assignment setters, markers and moderators
- sets and agrees assignments
- marks and moderates assignments
- agrees the final mark and issues certificates.

QUALIFI's 'Handbook on Guidance and Requirements for Assessment and Marking' will apply to its assignment setters, markers and moderators.

3.2 Access to Study

All learners should be invited to an induction event to be introduced to the programme in detail through presentations and discussions with tutors and the centre support team.

All learners should be issued with the Diploma handbook, a timetable and meet with their personal tutor and fellow learners. Centres should assess learners carefully to ensure that they take the right qualification and the right pathways or optional units, to allow them to progress to the next stage.

Centres should check the qualification structures and unit combinations carefully when advising learners. Centres will need to ensure that learners have access to a full range of information, advice and guidance in order to support them in making the necessary qualification and unit choices. When learners are recruited, centres need to give them accurate information on the title and focus of the qualification for which they are studying.

All learners must be registered with QUALIFI within 30 days of centre registration.

3.3 Entry Criteria

QUALIFI Level 5 Diploma in Cyber Security:

This qualification has been designed to be accessible without artificial barriers that restrict access and progression. Entry to the qualification will be through a centre application form or interview and the candidates will be expected to hold the following:

- learners who possess qualifications at Level 4 and/or;
- learners who have some technical and risk management work experience in a computing or security business environment and demonstrate ambition with clear career goals;
- learners who possess a Level 5 qualification in another discipline and want to develop their careers in cyber security and/or risk management.

In certain circumstances, learners with considerable experience but no formal qualifications may be considered, subject to interview and being able to demonstrate their ability to cope with the demands of the programme.

In the case of applicants whose first language is not English, then IELTS 5 (or equivalent) is required. International Qualifications will be checked for appropriate matriculation to UK higher education post-graduate programmes. The applicants are normally required to produce two supporting references, at least one of which should preferably be academic.

4 Structure of the Qualification

4.1 Units, Credits and Total Qualification Time (TQT)

The QUALIFI Diploma in Cyber Security is a Level 5 qualification made up of **four units** equating to 120 credits.

All units are 30 credits in value. These units have been designed from a learning time perspective and are expressed in terms of **Total Qualification Time (TQT)**. TQT is an estimate of the total amount of time that could reasonably be expected to be required for a student to achieve and demonstrate the achievement of the level of attainment necessary for the award of a Qualification. TQT includes undertaking each of the activities of Guided Learning, Directed Learning and Invigilated Assessment. Each 30-credit unit approximates to a TQT of 300 hours incorporating 180 hours of GLH.

Examples of activities which can contribute to Total Qualification Time include:

- guided learning
- independent and unsupervised research/learning
- unsupervised compilation of a portfolio of work experience
- unsupervised e-learning
- unsupervised e-assessment
- unsupervised coursework
- watching a pre-recorded podcast or webinar
- unsupervised work-based learning.

Guided Learning Hours (GLH) are defined as the time when a tutor is present to give specific guidance towards the learning aim being studied on a programme. This definition includes lectures, tutorials and supervised study in, for example, open learning centres and learning workshops. Guided Learning includes any supervised assessment activity; this includes invigilated examination and observed assessment and observed work-based practice.

Some examples of activities which can contribute to Guided Learning include:

- classroom-based learning supervised by a tutor
- work-based learning supervised by a tutor
- live webinar or telephone tutorial with a tutor in real time
- e-learning supervised by a tutor in real time
- all forms of assessment which take place under the immediate guidance or supervision of a tutor or other appropriate provider of education or training, including where the assessment is competence-based and may be turned into a learning opportunity.

4.2 Qualification Structure

There are four mandatory units for this qualification. All units cover a number of topics relating to learning outcomes. Each unit has the equivalency of 30 credits.

Learners are required to complete four units to achieve the 120 credits required to gain the Level 5 Diploma in Cyber Security. Learners will be expected to attend lectures and workshops that will introduce the subject matter. Formative assessments (weighted at 0%) may be used in lectures or tutorials to check knowledge and understanding of specific topics and subject areas. Units require reflective exam sets and/or summative assessments for marking.

The QUALIFI Level 5 Diploma in Cyber Security comprises four units in total:

The Diploma requires 4 Mandatory Units

Unit Reference	Mandatory Units	Level	Credits	TQT	GLH
DCS01	Cryptography	5	30	300	150
DCS02	Digital Investigations and Forensics	5	30	300	150
DCS03	Communications and Incident Management	5	30	300	150
DCS04	Strategic Leadership	5	30	300	150

4.3 Progression and Links to other QUALIFI Programmes

Learners completing the QUALIFI Level 5 Diploma will progress to:

- (Pending a successful application to our Partner institution) a Level 6 University Degree (Top-Up) course
- directly into employment in an associated profession.

4.4 University Exemptions

QUALIFI has exemptions for learners to progress to a number of universities to complete a master's degree. This generally requires completion of a dissertation only.

The pathways are an indication of a learner's progress towards a university degree and are based on the university's review of QUALIFI's learning programmes and outcomes. Further information is available here http://www.QUALIFI.net/learning-pathways/

4.5 Recognition of Prior Learning

Recognition of Prior Learning (RPL) is a method of assessment (leading to the award of credit) that considers whether learners can demonstrate that they can meet the assessment requirements for a unit through knowledge, understanding or skills they already possess, and so do not need to develop through a course of learning.

QUALIFI encourages centres to recognise learners' previous achievements and experiences whether at work, home or at leisure, as well as in the classroom. RPL provides a route for the recognition of the achievements resulting from continuous learning. RPL enables recognition of achievement from a range of activities using any valid assessment methodology. Provided that the assessment requirements of a given unit or qualification have been met, the use of RPL is acceptable for accrediting a unit, units or a whole qualification.

Evidence of learning must be valid and reliable. For full guidance on RPL please refer to QUALIFI's policy document on RPL.

5 Guidance to Teaching and Learning

To ensure consistency and quality of delivery amongst centres, QUALIFI has outlined a number of policies and procedures required to ensure the very best standards are available to learners. These include:

- expertise of staff
- learning and teaching methods
- study skills
- learning resources
- personal development planning
- career opportunities.

The policies and procedures are available on request to all accredited centres or to those wishing to apply for accreditation to deliver QUALIFI qualifications.

6 Learner Support

Centres should continue to support learners and encourage appropriate behaviour. To ensure consistency and quality of delivery amongst centres QUALIFI, has outlined a number of policies and procedures to ensure the very best standards are available to learners. These include:

- learners with disabilities
- health and safety
- conduct
- progression
- weekly timetable/attendance requirements.

The policies and procedures are available on request to all accredited centres or to those wishing to apply for accreditation to deliver QUALIFI qualifications.

6.1 Data Protection

All personal information obtained from learners and other sources in connection with studies will be held securely and will be used during the course and after they leave the course for a variety of purposes. These should be all explained during the enrolment process at the commencement of learner studies. If learners or centres would like a more detailed explanation of the partner and QUALIFI policies on the use and disclosure of personal information, please contact QUALIFI via email support@QUALIFI-international.com

7. Assessment

These qualifications are vocational as they can support a learner's career progression. To meet QUALIFI's aim to provide an appropriate assessment method each unit will be assessed through tasks that will be written in a way to make them realistic 'work-related' tasks wherever possible. Learners will need to demonstrate knowledge, understanding and. Original thought, problem solving and recommendations on actions will also be asked for from learners where appropriate for the unit. Intellectual rigour will be expected appropriate to the level of the qualification.

Assignments will contain a question strand for each of the given unit's learning outcomes. The assignment tasks will address the LO (learning outcome) and AC (assessment criteria) requirements. Within assignments there will always be requirements for learners to engage with important and relevant theory that underpins the subject area.

The assignment questions will require learners to draw on real organisations to illustrate their answers. To support this activity during the programme of learning, centres are required to make sure that they include case studies of relevant organisations and, wherever possible, facilitate in-company opportunities for learners to undertake research and investigation projects and/or support the organisation with various tasks. Mature and part-time learners will ideally be able to draw on their personal work experience too.

Sample assessments and marking scheme are available on request as part of the Qualification Specification supplied to centres.

QUALIFI has an assessment policy and procedure documents that are available to all centres delivering this qualification. QUALIFI's 'Handbook on Guidance and Requirements for Assessment and Marking' covers the following:

- assessment strategy
- assessment arrangements for learners with a disability
- verification
- marking scheme/pass mark
- deferral after valid mitigating circumstances
- referral after failure

- dealing with difficulties in meeting assessment deadlines
- late submissions
- assessment boards
- appeals
- cheating and plagiarism
- referencing
- confidential material
- submission.

8. Course Regulations

8.1 Course Requirements

Learners must complete all units and pass the appropriate mark to receive the full Diploma Award. QUALIFI will issue certificates to all successful students through the registered centres.

8.2 Classification of Awards

Where a candidate has achieved an overall average mark of at least 70% from all the units, QUALIFI may award a Distinction, although offering such a grade to individual candidates is at the discretion of QUALIFI and is not normally given after any successful referral attempts.

Decisions about the overall classification of awards are made by QUALIFI through the application of the academic and relevant course regulations. It is based on the Average Percentage Mark (APM) or, at the discretion of QUALIFI, on the basis of your overall profile and performance subject to the minimum requirements.

8.3. Learner Voice

Learners can play an important part in improving the quality of this course through the feedback they give. In addition to the ongoing discussion with the course team throughout the year, there is a range of mechanisms for learners to feed back about their experience of teaching and learning.

8.4 Complaints

QUALIFI recognises that there may be occasions when learners and centres have cause for complaint about the service received. When this happens, the complaints procedure is intended to provide an accessible, fair and straightforward system that ensures as an effective, prompt and appropriate response as possible.

For more information on our formal complaints procedure please contact in the first instance or email: support@QUALIFI-international.com

9 Equality and Diversity

QUALIFI recognises that discrimination and victimisation are unacceptable and that it is in the interests of QUALIFI employees to utilise the skills of the total workforce. It is our aim to ensure that no employee or other representative of QUALIFI receives less favourable facilities or treatment (either directly or indirectly) in recruitment or employment on grounds of age, disability, gender/gender reassignment, marriage/civil partnership, pregnancy/maternity, race, religion or belief, sex, or sexual orientation (protected characteristics).

Our aim is that our workforce will be truly representative of all sections of society and each employee feels respected and able to give their best. We oppose all forms of unlawful and unfair discrimination or victimisation. To that end the purpose of this policy is to provide equality and fairness for all.

Our staff will not discriminate directly or indirectly, or harass customers or clients because of age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, and sexual orientation in the provision of QUALIFI's goods or services.

This policy and the associated arrangements shall operate in accordance with statutory requirements, particularly the Equality Act 2010 https://www.gov.uk/equality-act-2010-guidance. In addition, full account will be taken of any guidance or codes of practice issued by the Equality and Human Rights Commission, any government departments, and any other statutory bodies.

The policy document will be monitored and reviewed annually and can be downloaded from our website or by making contact with QUALIFI.

10. Further Professional Development and Training

QUALIFI supports UK and international customers with training related to our qualifications. This support is available through a choice of training options offered through publications or through customised training at your centre.

The support we offer focuses on a range of issues including:

- planning for the delivery of a new programme
- planning for assessment and grading
- developing effective assignments
- building your team and teamwork skills
- developing student-centred learning and teaching approaches
- building in effective and efficient quality assurance systems.

You can request customised training through your registered centre in the first instance. If you need to contact QUALIFI directly:

Our customer service number: +44 (0) 115 8882323

Or email: support@QUALIFI-international.com

Website: www.QUALIFI.net www.QUALIFI-international.com

Appendix 1: Unit Descriptors

QUALIFI Level 5 Diploma in Cyber Security

Unit DSC01: Cryptography

Unit code: J/617/4634
RQF level: 5

Aim

The process of encrypting and decrypting information forms the basis of much computer, device and network security. Cryptography is designed and used to protect the confidentiality, integrity and authenticity of information. From the very beginnings of computing, and throughout the industry's evolution, the establishment of policies, guidelines and laws has shaped the disciplines of information security and organisational resilience in profound and, often, unintended, ways.

In this unit learners will be introduced to the concept and history of cryptography, and its subdisciplines (including cryptology), and how cyber-enabled networks and devices have their communications security underpinned by cryptographic methods and sector standards. Learners will explore methods of attack, including side-channel, additional encryption methods and escrow principles and key.

Learners will look at how businesses can deploy encryption to enhance their information security approaches.

Learners will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand key cryptographic principles and modes	1.1 Define the concept and application of cryptography 1.2 Explain symmetric and asymmetric modes and approaches 1.3 Assess how cryptographic methods and standards underpin the communications security of cyber-enabled networks and devices
2 Understand the standards, regulations and laws that apply to business and government organisations in relation to encryption	2.1 Explain the key principles of the related standards, regulations and laws and why they are in place 2.2 Assess the consequences for organisations and individuals of non-compliance with these standards, regulations and laws

3 Design an encryption plan and courses of action for a given organisation	3.1 Explain the methods of attack used to target encrypted data 3.2 Assess the additional encryption methods available 3.3 Explain the key principles of escrow and recovery 3.4 Explain the importance of having robust encryption arrangements within IT systems 3.5 Evaluate the existing encryption arrangements 3.6 Design an encryption plan to meet the needs of a given organisation, with recommended courses of actions

Indicative Content

-The science of crypto

-Cipher types

-Symmetric and asymmetric

-Methods of attack

-Standards, regulations, legal domains

-Key escrow and recovery

Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by Qualifi to all centres. This learner-support information will be presented within clearly separated tabs, including:

Unit Content: Actual learning content broken down into weekly stages with a reflective learning end-section.

Video-shelf: Unit content and additional information provided by the course leader via video.

E-library: Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list.

Assignment Instructions: Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing as well as making presentations.

Discussion Board: Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

Assessment Guidance

Each unit will be worth **30 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each module assessment point.

During each of the four 30-credit units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will by way of completing a formative exercise/s throughout the unit.

Summative Assignment: CONSULTANCY REPORT - Write a company or business report reviewing a) existing encryption arrangements within the IT system, and b) offering a Courses of Action group of recommendations for the company's CISO (3000 words).

Suggested Resources

Gordon Corera (2015) Intercept: The Secret History of Computers and Spies (London: W&N), available at: **https://www.amazon.co.uk/Intercept-Secret-History-Computers-Spies/dp/0297871730**

Krebs on Security (Online) accessed at: https://krebsonsecurity.com/

Lawrence Miller and Peter Gregory (2018) CISSP For Dummies (USA: John Wiley & Sons), available at: **https://www.amazon.co.uk/CISSP-Dummies-Computers-Lawrence-Miller/dp/0470537914**

Twitter - @GlobalCAcademy
-@bruceschneier

Unit DCS02: Digital Investigations and Forensics

Unit code: L/617/4635
RQF level: 5

Aim

This unit describes and explains how to conduct investigations with cyber-enabled equipment, including on public-internet-facing networks, or other network environments. Much evidence is lost or ruled inadmissible within courts and tribunal environments because it has been mishandled and corrupted (or could have been) by investigators, or those with a perceived chain of custody over the data. Moreover, in a planet of several billion cyber-enabled devices, but few qualified cyber investigators, it is now the case that many organisations have to manage part or all of a cyber incident investigation, because the national CERT or police/security agencies are otherwise prioritised.

In this unit learners will examine the requirements for digital investigations including team formations and tools, understanding the prospects of recovering information, gathering evidential data (including from mobile and IoT devices), safeguarding evidential integrity, as well as the complexity and challenges of storing and presenting evidence within legal environments.

Learners will develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the cyber security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand the core principles of digital investigations	1.1 Explain the investigation lifecycle from initiation to conclusion 1.2 Explain how a 'digital' domain investigation is organised and managed
2 Apply the types of tool that support professional digital investigations at a strategic level	2.1 Analyse the range of tools that assist digital investigations in different situations 2.2 Select the appropriate tools to carry out a digital investigation for a given situation, justifying the selection

3. Plan for an investigations and forensics teams	3.1 Explain the types of skills required to undertake a variety of investigations and forensic-related work 3.2 Explain dynamics of forming and integrating digital investigation teams and geographically distributed and dispersed investigations and teams 3.3 Develop a plan for the formation of an investigation and forensics teams
4. Understand the importance of safeguarding evidential integrity in digital investigations	4.1 Explain how evidence can be retrieved from mobile devices and IoT devices 4.2 Analyse how evidential integrity is safeguarded during digital investigations 4.3 Assess how evidence is stored and presented within legal environments

Indicative Content

-Requirement for digital investigations

-Understanding evidential data and prospects of recovery

-Mobile, portable and apps in DI

-Evidential integrity and chain of custody

-Processes and timelines

-Legal domains and cross examination

-Management and budgeting

Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by Qualify to all centres to deliver. This learner-support information will be presented within clearly separated tabs, including:

Unit Content: Actual learning content broken down into weekly stages with a reflective learning end-section.

Video-shelf: Unit content and additional information provided by the course leader via video.

E-library: Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list.

Assignment Instructions: Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing as well as making presentations.

Discussion Board: Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

Assessment Guidance

Each unit will be worth **30 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each unit assessment point.

During each of the four 30-credit units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will by way of completing a formative exercise/s throughout the unit.

Summative Assignment: (REPORT) Conduct an investigation into a suspected mega breach of an Internet Services Provider that has lost the login credentials for 150,000 business clients.
Questions:

1. Explain to their CEO the investigative stages that you have passed through and why each stage was necessary. (1000 words)
2. Imagine that your suspicions are now focused on an internal leak, perhaps a group or couple of employees located offsite in your 'hot' disaster recovery centre. Identify and explain what tools you might need to acquire to prove your case further, and estimate the costs (1000 words)
3. Explain and evaluate how you will securely store the evidence until it is handed over to the local police. (1000 words)

Suggested Resources

Bilton, N. (2017) American Kingpin: The Epic Hunt for The Criminal Mastermind Behind the Silk Road (Portfolio)

Sachowski, j. (2018) *Digital Forensics and Investigations: People, Processes and Technologies* (CRC Press)

Sikorski, M and Honig, A., (2012) *Practical Malware Analysis* (No Starch Press)

Unit DSC03: Communications and Incident Management

Unit code: R/617/4636
RQF level: 5

Aim

The professional and lawful response to managing an incident can be the difference between company survival or otherwise. Poor responses to major incidents, including mega data breaches, have significantly damaged organisational reputations and financial performance. Significantly mismanaging a cyber incident can result in catastrophic personal and organisational consequences. Such business 'impacts' are covered in-depth within our Threat and Risk units at Levels 2, 3 and 4. and will be explored during this Level 5 unit as part of the contextual case-study learning, and isomorphic reflections, that are central to this unit.

In this unit learners will explore the types of site, personnel and equipment required in relation to planning for Incident Management and forming an organisational CERT team (Computer Emergency Response Team). They will then explore the core sub-disciplines and side-disciplines of Cyber Incident Management: Disaster Recovery, Business Continuity Management and Crisis Management. Learners will discuss the importance of the business organisational requirement for skilled and planned communications to operate in combination with advanced and developed management responses and strategy.

Learners will develop an understanding of the security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP).

Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand the physical and human resources required to manage a major suspected cyber security incident	1.1 Explain site-set-up, staffing and organisational arrangements for major suspected cyber-related incidents
2 Apply Business Continuity Management to major incident planning and response	2.1 Assess how Business Continuity Management can be aligned and integrated into a suspected cyber-enabled incident 2.2 Explain the people, assets and processes required within a Business Continuity Plan

3 Understand how Disaster Recovery and Crisis Management are integrated into a suspected major cyber-enabled incident	3.1 Assess how DR and CM strategies and tactics in relation to a suspected major cyber-enabled incident 3.2 Explain the components of good practice in DR and CM plans
4 Evaluate the potential impact of NOT planning crisis communications and incident response	4.1 Evaluate the isomorphic lessons from major cyber breaches and company shutdowns 4.2 Analyse communications approaches and perceived failures in cases of catastrophic business loss related to IT systems failure or attack 4.3 Justify recommendations that would support a cyber-resilient approach

Indicative Content

-Equipment and location requisites

-Disaster Recovery and Management

-Business Continuity Management

-Crisis Management

-Cyber Resilience: including considerations of future-proofing and disruptive technology

Delivery Guidance

This unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by Qualifi to all centres. This learner-support information will be presented within clearly separated tabs, including:

Unit Content: Actual learning content broken down into weekly stages with a reflective learning end-section.

Video-shelf: Unit content and additional information provided by the Course Leader via video.

E-library: Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list.

Assignment Instructions: Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing as well as making presentations.

Discussion Board: Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and

answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

Assessment Guidance

Each unit will be worth **30 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each module assessment point.

During each of the four 30-credit units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will by way of completing a formative exercise/s throughout the unit.

Summative Assignment: ESSSAY – Identify and explain a case study that could be translated as a weak organisational response to a major cyber-security incident. Evaluate how the organisation responded and provide recommendations that would support a more cyber-resilient approach over the next five years. (3000 words)

Suggested Resources

Austin, L and Jin, Y (2017) *Social Media and Crisis Communication* (Routledge)

Richard Bingley (2015) *The Security Consultant's Handbook* (Ely: IT Governance Press), available at: **https://www.itgovernance.co.uk/shop/product/the-security-consultants-handbook**

Heng, G.M (2017) A Manager's Guide to Business Continuity Incidents for Cyber Security Incidents, The Business Continuity Management Institute, available at: **https://www.bcm-institute.org/product/a-managers-guide-to-business-continuity-management-for-cybersecurity-incident-response/**

Unit DSC04: Strategic Leadership

Unit code: Y/617/4637
RQF level: 5

Aim

In order for an organisation to be more cyber secure, leadership across employee and stakeholder networks is required to be delivered by the C-Suite. However, what happens if the C-Suite either doesn't listen or doesn't understand the Tier One threat posed by information security vulnerabilities.

In this unit learners will develop an understanding of the key features of tech leadership and performance management. Learners will evaluate strategic leadership and management approaches, within a tech sector setting, and what it means to be a 'senior level influencer'.

Learners will also develop an understanding of security technical and generic management and leadership teaching. Much of this teaching will be particularly relevant to learners wishing to move into more advanced Information Security Management technical qualifications, including the CompTIA Security + accreditation and the Cyber Security industry gold standard: The Certified Information Systems Security Professional (CISSP). The unit is also highly applicable to learners who are considering taking an MBA, or MBA in Cyber Security, at a later date or who looking to advance into senior management roles within their organisation or sector.

Learning Outcomes and Assessment Criteria

Learning Outcomes. To achieve this unit a learner must be able to:	Assessment Criteria: Assessment of these outcomes demonstrates a learner can:
1 Understand the role senior leaders and strategic leadership	1.1 Explain the key roles and responsibilities of senior leaders in a tech sector setting 1.2 Assess how strategic leadership and core goal-setting can enable stronger security cultures
2 Evaluate the management streams and performance monitoring mechanisms that relate to information security	2.1 Explain the importance of integrating management and operational programmes in relation to optimum levels of performance and cyber resilience 2.2 Anlayse the performance monitoring mechanisms in place to protect information security 2.3 Assess how cultural and diversity-related complexities impact on management and performance monitoring
3 Understand how threat and risk identification and	3.1 Evaluate risk management and threat identification within the context of wider corporate strategy,

management is integrated into C-Suite considerations and governance	responsibilities and governance 3.2 Explain the impact of poor or ineffective C-Suite understanding and direction 3.3 Assess the importance of business ethics and leadership in business values, including within end-user environments of ICT systems
4 Understand how data protection legislation impacts considerations of strategy-setting and strategic leadership	4.1 Evaluate how major data protection laws, impact on C-Suite strategic level decision making and strategy setting 4.2 Assess the consequences for individuals and organisations of non-compliance with this legislation

Indicative Content

-Strategic leadership

-Strategic management, project management and configuration management

-Threat and risk management: global business environments

-Cultural complexity

-Ethics, compliance and governance

Delivery Guidance

This 30-credit unit lends itself to a model of blended delivery. Learners will be able to access a course shell with various information sources provided by Qualifi to all centres. This learner-support information will be presented within clearly separated tabs, including:

Unit Content: Actual learning content broken down into weekly stages with a reflective learning end-section.

Video-shelf: Unit content and additional information provided by the Course Leader via video.

E-library: Access to electronic books, books produced by the course team, journals, data sources and news articles, as well as a recommended book and journals list.

Assignment Instructions: Clear and precise instructions and contact details for compiling and submitting assignments. Support materials such as guides to report, portfolio and essay writing as well as making presentations.

Discussion Board: Interactive zone for learners to network, share ideas and co-explore information sources.

Case studies and reflective case-study learning will underpin all theory. The support will provide blended delivery formats: written, videoconferencing and interactive learner-tutor question and

answer sessions that can either be visual (via VOIP) or written (via feedback on the two-way Student Journal).

Assessment Guidance

Each unit will be worth **30 credits** and the qualification is designed to be flexible for learners who are already working and in demanding jobs. Every unit must be passed in order to achieve the Diploma.

Learners will be able to progress sequentially through each unit, accumulating credits as they pass each module assessment point.

During each of the four 30-credit units, every learner will have the opportunity to 'practise' and hone their ability to undertake the final (formal) assessment. Such non-mandatory practice will by way of completing a formative exercise/s throughout the unit.

Summative Assessment: REPORT: Identify an organisation that recently experienced a mega data breach.

1. Prior to the event, what was the style of leadership, the corporate strategy, the goals of that organisation? (800 words)
2. Prior to the event, analyse how well the company/organisation was perceived by the market and its shareholders to be performing. (800 words)
3. Following the data breach, in your assessment, what laws in relation to the major incident (or related activities) is the company guilty of breaching? (800 words)
4. Following the data breach, in your assessment, how well is the company performing? (800 words)
5. Following the data breach, to what extent has the company/organisational strategic leadership been successful? (800 words)
   (Total: 4000 words)

Suggested Resources

Henderson, G. (1994) Cultural Diversity in the Workplace, Praeger

'Krebs on Security' cyber security and news blog accessed at: https://krebsonsecurity.com/

Rumelt, R (2017) *Good Strategy: Bad Strategy: The difference and why it matters* (Profile Books)