Information Security Qualifications

FACT SHEET

January2015

Protect • Comply • Thrive

Information Security Qualifications

Introduction

There is a perception in society and the working world that, with the exception of degrees like the MBA, formal education ceases after leaving university. This has become something of a self-fulfilling belief, as those who hold it rarely go on to further study or to hold professional qualifications.

In rapidly shifting and evolving environments such as IT, however, this belief must be expunged, lest it put the enterprise at risk.

It is important to hold the pace of advance in mind when considering ongoing educational needs for IT. As technologies change, becoming more mobile and posing new challenges to the business environment, key staff should be encouraged to seek educational opportunities and develop the skills to respond.

Encouraging ongoing education and qualifications is all well and good, of course, but the focus must be on opportunities that provide the right information for your enterprise. While university qualifications are broad and encourage the development of critical skills, more focused syllabi must be sought out for professionals already embedded in the industry.

The obvious solution is to look for courses and qualifications developed to meet the specific needs of the industry. Because IT fulfils similar roles across a multitude of industries (management of information, security of information, business continuity concerns, etc.), it is possible to find options that provide the required expertise without restricting their applicability to a specific industry.

It is clear that requirements laid down by industry standards offer the best guidance for professional qualifications.

The business case

There are many reasons for a business to invest in courses and qualifications for key IT professionals. Some business models – consultancies in particular – will see significant benefits from this investment, while other business models favour a more cautious approach.

Aside from the immediate benefits generated by improved knowledge and expertise, the primary reasons to seek out professional qualifications are:

- Demonstrating a commitment to a level of expertise within the enterprise.
- Demonstrating a commitment to employee development.
- Developing crucial skills to be held in-house.
- Enabling the dissemination of expertise and knowledge within the enterprise.
- Getting ahead of emerging risks.

These benefits fall into three broad categories: external marketing, internal marketing and leveraging expertise.

With a demonstrable commitment to specific expertise, the organisation improves customer perceptions. This is especially true for businesses that offer directly related services (such as auditing or consultancy).

Internal marketing can be an equally significant gain where having a highly skilled workforce is crucial to the business. By demonstrating a commitment to the development of key professionals, the organisation improves loyalty and employee retention.

Developing expertise within the enterprise need not be limited to those who achieve the qualification. While the certification is limited to those who do achieve it, knowledge can be expanded throughout the enterprise to offer ongoing returns. Further, as many qualifications require ongoing education and experience, this expertise is maintained against the growth and development in IT, enabling the enterprise to better prepare for and mitigate emerging risks.

The professional case

Individuals holding professional qualifications are highly sought-after in IT. Certification in many cases leads to improved salaries[1], discretionary bonuses and enhanced career progression[2], and the prospects for this to continue in the future are good.

The 2013 (ISC)[2] Global Information Security Workforce Study[3] reported that 56% of organisations believe there is a lack of suitably qualified information security professionals. Furthermore, 46% of all responding companies require that their information security staff have a professional qualification.

The demand for qualified professionals naturally opens up opportunities for further development and provides powerful bargaining leverage in contract negotiations.

Qualifications

There is a wide range of qualifications available to IT professionals, with a particular focus around areas subject to regulatory pressures (whether legally mandated or entered into voluntarily). The complexities of these areas enable suitably qualified individuals the ability to streamline a compliance project for their organisation, potentially saving considerable time and investment.

CISA

The Certified Information Systems Auditor (CISA) qualification, awarded by ISACA®, is a globally accepted standard among information systems audit, control and security professionals. The qualification is based on the understanding of five key areas of information systems audit:

- The process of auditing information systems
- Governance and management of IT
- Acquiring, developing and implementing information systems
- Information systems operations, maintenance and support
- Protecting information assets.

Developing the skills to audit information systems are of special importance to internal and external auditors, finance/CPA professionals, information security professionals and any other IT professionals with an interest in ensuring the correct management of information systems.

The CISA qualification requires applicants to prove at least five years' relevant work experience before sitting the notoriously difficult exam.

Exams are held in June, September and December each year. Residential and in-house training courses for the CISA qualification run regularly.

The CISA qualification must be maintained with continuing professional education (CPE) to ensure that qualified professionals maintain a standard of knowledge and proficiency in the world of audit, control and security. ISACA provides information about maintaining your CISA qualification.

CISM

The Certified Information Security Manager (CISM) qualification is awarded by ISACA and is a globally accepted standard of achievement among information security, information systems audit and IT governance professionals. The CISM qualification develops expertise in four critical areas:

- Governance of information security
- Information risk management and compliance
- Developing and managing information security programmes

- Information security incident management.

The CISM is an important and useful qualification for risk managers, security auditors, information security professionals, compliance personnel, CSOs, CISOs and CIOs.

CISM certification is awarded to candidates who have at least five years of relevant work experience and who pass a rigorous written examination, held in June and December each year.

There are training courses available, which have been designed to provide a complete preparation to pass the ISACA CISM examination at the first attempt.

Like the CISA, a CISM qualification must be maintained with continuing professional education to ensure that you maintain a standard of knowledge and proficiency in the world of information security, audit and governance. ISACA provides information about maintaining your CISM qualification.

CISSP

The Certified Information Systems Security Professional (CISSP) qualification has become a pre-requisite for anyone looking to make a career in information security. The CISSP certification provides information security professionals with an objective measure of competence and a globally recognised standard of achievement.

CISSP is based on ten key areas, collectively known as the Common Body of Knowledge (CBK). These comprise:

- Access control
- Telecommunications & network security
- Information security governance & risk management
- Software development security
- Cryptography
- Security architecture & design
- Operations security
- Business continuity & disaster recovery planning
- Legal, regulations, investigations & compliance
- Physical (environmental) security

CISSP is considered an essential qualification for information security professionals seeking or holding senior positions, such as senior security managers, CISO and CSO.

To apply to sit the CISSP examination, you must have at least five years direct, full-time security professional work experience in two or more of the ten domains of the (ISC)² CISSP CBK. You will also have to have your qualifications endorsed by another (ISC)² credential holder.

CISSP certification is achieved by passing the official CISSP exam, which is managed by (ISC)², who maintain a database of examination dates and locations.

Training in preparation of the examination is recommended, and CISSP training programmes are available throughout the year ahead of the exam.

All CISSPs are required to maintain their expertise, which can be done in a number of ways, including official CISSP online review courses and information security training courses.

CIS LA

The ISO27001 Certified ISMS Lead Auditor (CIS LA) qualification, awarded by the International Board for IT Governance Qualifications (IBITGQ), is designed to prepare you to plan and execute audits of information security management systems in line with the International Standard, ISO/IEC 27001.

There are no formal prerequisites to become a qualified CIS LA but, as a lead auditor qualification, it expects a level of experience in auditing information systems. As such, it is an excellent qualification for auditors working in or assisting in the implementation of an ISO27001 Information Security Management System (ISMS).

The exam to qualify as a CIS LA is designed by IBITGQ and managed on their behalf by the Global Association for Software Quality (gasq). All IBITGQ exams are ISO/IEC 17024 audited. Approved CIS LA training

courses usually incorporate the examination (and associated fees) into the schedule.

While the CIS LA qualification has no mandated upkeep requirement, the process of training for and achieving the qualification can be put towards the maintenance of other professional qualifications.

CIS LI

The ISO27001 Certified ISMS Lead Implementer (CIS LI) qualification, from IBITGQ, delivers a comprehensive education in ISO27001 implementation and a recognised industry standard certification.

Like the CIS LA qualification, there are no prerequisites for CIS LI, but it does expect a certain level of existing expertise in the implementation of information security systems.

Due to the scope of implementation in an ISO27001 ISMS, this qualification is extremely useful for a wide variety of professionals. Essentially, any manager involved in the implementation of the ISMS will benefit, as will key staff such as auditors, information security professionals, HR, legal and business users.

The exam to qualify as a CIS LI is designed by IBITGQ and managed on their behalf by gasq. Approved CIS LI training courses usually incorporate the examination and fees into the schedule.

While the CIS LI qualification has no mandated upkeep requirement, the process of training for and achieving the qualification can be put towards the maintenance of other professional qualifications.

CIS RM

The ISO 27005 Certified ISMS Risk Management (CIS RM) qualification, issued by IBITGQ, provides the knowledge and skills required to undertake information security risk management based on the best practice guidance as outlined in ISO/IEC 27005 and fully meeting the requirements of the ISO 27001 Standard.

There are no prerequisites to qualify as a CIS RM, but a level of experience in risk management and ISO/IEC 27001 is expected.

As risk management is a significant component of a certified ISO/IEC 27001 ISMS, the CIS RM qualification is of distinct value to information security managers, CIS LI holders who need to further develop effective and practical risk management processes, risk managers, and ISO 27001 consultants.

The exam to qualify as a CIS RM is designed by IBITGQ and managed on their behalf by gasq. Approved CIS RM training courses usually incorporate the examination and fees into the schedule.

The CIS RM qualification does not require upkeep through ongoing education, but the process of training for and achieving the qualification can be put towards the CPE requirements of some other professional qualifications.

CRISC

Awarded by ISACA, the Certified in Risk and Information Systems Control (CRISC) qualification is awarded to IT professionals who identify and manage risks through the development, implementation and maintenance of information systems controls.

The CRISC qualification develops expertise in five key domains:

- Risk identification, assessment and evaluation
- Risk response
- Risk monitoring
- Information systems control design and implementation
- IS control monitoring and maintenance.

In providing crucial knowledge and expertise in risk management, the CRISC qualification is ideal for IT professionals, risk professionals, business analysts, project managers and compliance professionals.

CRISC certification requires at least three years relevant work experience as well as a written examination. Exams are held in June and December each year.

CRISC training courses are available, and provide a complete preparation to ensure that you pass the CRISC examination at the first attempt.

Like many other professional qualifications, certified CRISC professionals must maintain expertise in risk management and information system controls. ISACA provides information about maintaining your CRISC qualification.

[1] http://www.networkworld.com/newsletters/2008/060908ed1.html
[2] http://www.isaca.org/Certification/Pages/CISA-CISM-CGEIT-Certification-Recognition.aspx
[3] https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/2013%20Global%20Information%20Security%20Workforce%20Study%20Feb%202013.pdf

Useful Resources

IT Governance offers a unique range of products and services, including books, standards, pocket guides, training courses, staff awareness solutions and professional consultancy services.

Training Courses

- **CompTIA Security+ Training Course**

The CompTIA Security+ training course is a 5-day classroom session designed to provide an intensive and complete preparation for delegates who wish to save time and pass the CompTIA Security+ examination at the very first attempt.

- **CompTIA Advanced Security Practitioner (CASP) Training Course**

This CISM training course is a 4-day intensive preparation course to become a Certified Information Security Manager (CISM). Updated annually to reflect the latest official guidance and content for the global CISM qualification.

- **CISA - Certified Information Systems Auditor Training Course**

This 4-day CISA course is the perfect intensive preparation course for the CISA exam and is run by the official UK reseller of ISACA's CISA materials. The CISA exam changes every year, and our course is updated to reflect the latest official guidance on content and exam questions.

- **CISM - Certified Information Security Manager Training Course**

This CISM training course is a 4-day intensive preparation course to become a Certified Information Security Manager (CISM). Updated annually to reflect the latest official guidance and content for the global CISM qualification.

- **CISSP Accelerated Training Programme**

The CISSP training – ”CISSP Fast Track” course is an intensive, in-depth training program that has consistently achieved over 95% pass rates in the final CISSP examination. If you don’t pass first time you are welcome to resit the course for free.

- **ISO27001 Certified ISMS Lead Auditor Training Course**

A 4.5 day intensive course to become a certified ISMS Lead Auditor, based on ISO27001 - the international standard for best practice in information security management systems.

- **ISO27001 Certified ISMS Lead Implementer Masterclass**

This three-day ISO27001 Certified ISMS Lead Implementer Masterclass provides comprehensive and practical coverage of all aspects of implementing and maintaining an ISO 27001 project, leading to the coveted Certified ISMS Lead Implementer (CIS LI) qualification.

- **ISO 27005 Certified ISMS Risk Management**

This course is designed to provide delegates with the knowledge and skills required to undertake information security risk management based on the best practice guidance as outlined in ISO 27005 and fully meeting the requirements of the ISO27001 standard.

- **Certified in Risk & Information Systems Control (CRISC) Training**

Three-day certified CRISC training course in London. Prepare for the CRISC exam and be best placed to pass it the first time around with this comprehensive CRISC qualification.

Books and Toolkits

- **CISA Review Manual 2015**

The CISA Review Manual 2013 is a comprehensive reference that will assist you in preparing for the CISA exam. It is also for individuals who wish to understand the roles and responsibilities of an information systems auditor.

- **CISM Review Manual 2013**

The CISM Review Manual 2013 is a comprehensive reference guide that will assist individuals in preparing for the CISM 2013 exam. It is also an ideal source of information for those who wish to understand the roles and responsibilities of an information security manager.

- **Official (ISC)^2 Guide to the CISSP CBK, Third Edition**

The Official (ISC)^2 Guide to the CISSP CBK, Third Edition is an essential resource for information security professionals, especially those studying for the CISSP examination.

- **CISSP Certification All-In-One Exam Guide, Sixth Edition**

Up to date with the latest version of this CISSP exam, this bestselling exam guide continues to be the essential resource for CISSP exam candidates. Written by Shon Harris, a leading trainer on the subject, this exam guide is critical to CISSP exam success.

- **CRISC Review Manual 2013**

This official ISACA manual will help you to prepare for and pass the CRISC exam in either June or December 2013. The manual will help you to understand IT-related business risk management roles and responsibilities.

- **Lead Auditor Toolkit**

This toolkit contains all the core documents that will enable you to plan and manage an internal audit of any management system. This toolkit meets the requirements of management standards such as ISO 9001, ISO 14001, ISO 27001, ISO 20000, etc.

- **ISO27005 (ISO 27005) ISRM**

ISO/IEC 27005:2011 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001. ISO/IEC 27005:2011 is designed to assist the satisfactory implementation of information security based on a risk management approach.

IT Governance Solutions

IT Governance source, create and deliver products and services to meet the evolving IT governance needs of today's organisations, directors, managers and practitioners.

IT Governance is your one-stop-shop for corporate and IT governance information, books, tools, training and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can benefit from them individually and also use different elements to build something bigger and better.

Books

Through our website, www.itgovernance.co.uk, we sell the most sought after publications covering all areas of corporate and IT governance. We also offer all appropriate standards documents.

In addition, our publishing team develops a growing collection of titles written to provide practical advice for staff taking part in IT Governance projects, suitable for all levels of staff knowledge, responsibility and experience.

Toolkits

Our unique documentation toolkits are designed to help small and medium organisations adapt quickly and adopt best management practice using pre-written policies, forms and documents.

Visit www.itgovernance.co.uk/free_trial.aspx to view and trial all of our available toolkits.

Training

We offer training courses from staff awareness and foundation courses, through to advanced programmes for IT Practitioners and Certified Lead Implementers and Auditors.

Our training team organises and runs in-house and public training courses all year round, covering a growing number of IT governance topics.

Visit www.itgovernance.co.uk/training.aspx for more information.

Through our website, you can also browse and book training courses throughout the UK that are run by a number of different suppliers.

Consultancy

Our company is an acknowledged world leader in our field. We can use our experienced consultants, with multi-sector and multi-standard knowledge and experience to help you accelerate your IT GRC (governance, risk, compliance) projects.

Visit www.itgovernance.co.uk/consulting.aspx for more information.

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organisations worldwide to be ISO27001-compliant.

Visit www.itgovernance.co.uk/software.aspx for more information.

Contact us: + 44 (0) 845 070 1750

www.itgovernance.co.uk servicecentre@itgovernance.co.uk

[1] http://www.networkworld.com/newsletters/2008/060908ed1.html
[2] http://www.isaca.org/Certification/Pages/CISA-CISM-CGEIT-Certification-Recognition.aspx
[3] https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/2013%20Global%20Information%20Security%20Workforce%20Study%20Feb%202013.pdf