Information Security Qualifications

FACT SHEET

March 2015

Protect • Comply • Thrive

Information Security Qualifications

Introduction

There is a general perception that, with the exception of degrees like the MBA, formal education ceases after leaving university, especially as those who hold degrees rarely go on to further study or to hold professional qualifications.

In such rapidly evolving environments as IT, however, this belief must be challenged so that it doesn't put enterprises at risk.

It is important to hold the pace of advancement 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, but the focus must be on opportunities that provide the right levels of expertise for your enterprise. While university qualifications are broad and encourage the development of critical skills, more focused syllabuses must be sought for professionals already embedded in the industry.

The obvious solution is to look for courses and qualifications that have been developed to meet the specific industry needs. Because IT fulfils similar functions across a multitude of industries (information management, information security, business continuity, and so forth), it is possible to find options that provide the required expertise without being restricted to a specific industry.

Guidance offered by industry standards offers the best pathway 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 favor a more cautious approach.

Aside from the immediate benefits generated by improved knowledge and expertise, the primary reasons to seek 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.

By demonstrating its commitment to specific expertise, the organization improves customer perceptions. This is especially true for businesses that offer directly related services, such as auditing or consultancy.

Internal marketing can also benefit from having a highly skilled workforce: by demonstrating a commitment to the development of key professionals, the organization improves loyalty and employee retention.

Developing expertise within an enterprise need not be limited to those who achieve qualifications. While certification is limited to those who achieve it, their knowledge

can be transferred throughout the enterprise to offer ongoing returns. Furthermore, as many qualifications require ongoing education and experience, this expertise is maintained by 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.

An ESG presentation at RSA Conference 2014 showed that 83% of organizations found it somewhat or extremely difficult to recruit information security professionals[3]. At the same conference, Ponemon Institute presented results from a survey showing that professional qualifications such as a CISSP were second only to extensive experience in determining an ideal candidate for an information security role. These significantly overshadowed the value of a university degree in IT security[4].

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 on areas subject to regulatory pressures (whether legally mandated or entered into voluntarily). The complexities of these areas provide suitably qualified individuals the ability to streamline a compliance project for their organization, 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 is 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 a 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 more 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 programs.
- Information security incident management.

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' relevant work experience and who pass a rigorous written examination, held in June and December each year.

Like 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 prerequisite for anyone looking to develop a career in information security. The CISSP certification provides information security professionals with an objective measure of competence and a globally recognized standard of achievement.

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

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

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

To sit the CISSP examination, you must have at least five years' direct, full-time, professional security 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, which maintains a database of examination dates and locations.

CIS LA

The ISO 27001 Certified ISMS Lead Auditor (CIS LA) qualification, awarded by the International Board for IT Governance Qualifications (IBITGQ), has been designed to prepare candidates 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 ISO 27001 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 mandatory upkeep requirement, the process of training for and achieving the qualification can be put towards the maintenance of other professional qualifications.

CIS LI

The ISO 27001 Certified ISMS Lead Implementer (CIS LI) qualification, from IBITGQ, delivers a comprehensive education in ISO 27001 implementation and a recognized 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.

Because of the scope of implementation in an ISO 27001 ISMS, this qualification is extremely useful for a wide variety of professionals. Essentially, any manager involved in the implementation of an ISMS will benefit, as will key staff such as auditors, information security professionals, and HR, legal, and business users.

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

While the CIS LI qualification has no mandatory 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 their 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.

Certified CRISC professionals must maintain expertise in risk management and information system controls. ISACA provides information about maintaining your CRISC qualification.

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

- **ISO 27001 Certified ISMS Foundation Online**

Take the first steps towards developing a best-practice information security management system (ISMS) using the ISO 27001:2013 standard.

- **ISO 27001 Certified ISMS Lead Auditor Online Masterclass**

A four-and-a-half-day intensive course to become a certified ISMS Lead Auditor, based on ISO 27001 – the international standard for best practice in information security management systems.

- **ISO 27001 Certified ISMS Lead Implementer Masterclass**

This three-day ISO 27001 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 ISO 27001 standard.

Books, toolkits and standards

- **CISA Review Manual 2013**

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. The manual will help you to understand IT-related business risk management roles and responsibilities.

- **Lead Auditor Toolkit**

This toolkit contains all of 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.

- **ISO 27005 information security risk management standard**

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 sources, creates, and delivers products and services to meet the evolving IT governance needs of today's organizations, 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.itgovernanceusa.com, 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-sized organizations adapt quickly and adopt best management practice using pre-written policies, forms, and documents.

Visit www.itgovernanceusa.com/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 programs for IT practitioners, and Certified Lead Implementers and Auditors.

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

Visit www.itgovernanceusa.com/training.aspx for more information.

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

Consultancy

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

Visit www.itgovernanceusa.com/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 organizations worldwide to be ISO 27001-compliant.

Visit www.itgovernanceusa.com/software.aspx for more information.

Contact us: **1-877-317-3454**

www.itgovernanceusa.com servicecenter@itgovernanceusa.com

[1] http://resources.infosecinstitute.com/average-cissp-salary-2013/
[2] http://www.isaca.org/Certification/Additional-Resources/Pages/CISA-CISM-CGEIT-Certification-Recognition.aspx
[3] http://www.rsaconference.com/writable/presentations/file_upload/prof-m03a-the-security-staff-and-skills-shortage-is-worse-than-you-think.pdf
[4] http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_IT_Security_Jobs_Report.pdf