International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:10, No:8, 2016

CyberSecurity Malaysia: Towards Becoming a National Certification Body for Information Security Management Systems Internal Auditors

M. S. Razana, Z. W. Shafiuddin

***Abstract*—**Internal auditing is one of the most important activities for organizations that implement information security management systems (ISMS). The purpose of internal audits is to ensure the ISMS implementation is in accordance to the ISO/IEC 27001 standard and the organization's own requirements for its ISMS. Competent internal auditors are the main element that contributes to the effectiveness of internal auditing activities. To realize this need, CyberSecurity Malaysia is now in the process of becoming a certification body that certifies ISMS internal auditors. The certification scheme will assess the competence of internal auditors in generic knowledge and skills in management systems, and also in ISMS-specific knowledge and skills. The certification assessment is based on the ISO/IEC 19011 Guidelines for auditing management systems, ISO/IEC 27007 Guidelines for information security management systems auditing and ISO/IEC 27001 Information security management systems requirements. The certification scheme complies with the ISO/IEC 17024 General requirements for bodies operating certification systems of persons. Candidates who pass the exam will be certified as an ISMS Internal Auditor, whose competency will be evaluated every three years.

***Keywords*—**ISMS internal audit, ISMS internal auditor, ISO/IEC 17024, Competence, Certification

I. Introduction

INTERNAL audit is to be understood as an independent and objective evaluation within an organization. According to [1], internal audits are "conducted by the organization itself, or on its behalf, for management review and other internal purposes (e.g. to confirm the effectiveness of the management system or to obtain information for the improvement of the management system)." For organizations that comply with the ISO/IEC 27001 standard, internal audit activity is one of the mandatory requirements to ensure compliance with the standard. It is also a compulsory for organizations to ensure that persons assigned to establish, implement, maintain and improve the information security management system (ISMS) within an organization are competent. To achieve the objectives of an internal audit, it is critical for organizations to select internal auditors who have certain competencies to perform auditing in a given knowledge area.

According to [2], [3], one of the most common nonconformities found during ISMS audits is in internal audit. According to BSI America, "10.5% of companies fail to comply with the Internal ISMS audit (Clause 6) where they are unsuccessful in conforming, effectively implementing and performing in what an audit expects of them". CyberSecurity Malaysia (CSM) is very concerned with the quality of internal audits. As the certification body for the CSM27001 scheme which is based on the ISO/IEC 27001 standard, 40% of organizations that were audited failed to comply with the requirements of the internal audit clause of the standard. Objective evidence found during the audits that resulted in noncompliance, were failure in following the internal audit procedure set by organizations, and failure in defining the audit criteria, scope and competency of the auditors.

In realizing the need to develop more competent internal auditors specialized in ISMS, CyberSecurity Malaysia is now in the process to becoming a certification body that certifies ISMS internal auditors. The ISMS Internal Auditors (ISMS-IA) certification scheme will assess the competence of internal auditors and is developed based on the ISO 19011 Guidelines for auditing management systems, ISO/IEC 27007 Guidelines for information security management systems auditing and ISO/IEC 27001 Information security management systems requirements. These standards provide generic, as well as specific knowledge and skills in auditing ISMS. The ISMS-IA certification scheme also fulfills the requirements of the ISO/IEC 17024 General Requirements for Bodies Operating Certification Systems of Persons. In order to be certified as ISMS Internal Auditors, candidates must sit for the ISMS-IA examination. Once they passed the examination, they will be certified as ISMS Internal Auditors and their competence in auditing will be evaluated every three years.

II. ISMS Internal Audit

Internal auditing is a process that comprises many elements such as planning, organizing and involves field work activities such as observing, verifying, analyzing, reporting and follow-up. It also requires interpersonal skills in interviewing, communicating, negotiating and presenting an audit report. An effective internal audit process contributes to the quality of an audit and as such, the competence of internal auditors is an important element that affects the quality of audit conducted [4]. In a study by [5], low proficiency of auditors is ranked as the second most important factor that affects the audit effectiveness in an organization. The study also found that long-term professional development schemes, such as a professional scheme with the objective of attaining an internal audit certification, are important to achieve a higher level of auditing proficiency and the improvement of skills.

Razana Md Salleh and Wan Shafiuddin Zainudin are both with CyberSecurity Malaysia, Malaysia (e-mail: razana@cybersecurity.my).

As a certification body that conducts external audits for organizations that seek ISO/IEC 27001 certification for their ISMS, based on the sample data collected through audit activities, an average of four out of 10 organizations audited failed to fulfill the internal audit requirement of the standard. Some of the objective evidence found during the audits that resulted in nonconformity in the internal audit, were due to the failure to follow the procedure set by organizations in conducting internal audit activities and the failure to fulfill the requirement of the ISO/IEC 27001 standard to define the audit criteria, scope and the competence of the auditors.

III. Competence of ISMS Internal Auditors

Reference [6] defines competence as the ability to apply knowledge and skills to achieve intended results. According to [1], ability implies the appropriate application of personal behavior during the audit process. Therefore, the quality of internal audits is highly influenced by the competence of the internal auditors in fulfilling the audit objectives. Since internal auditing works requires knowledge and skills in a wide range of systems and operations, it is imperative to select auditors with extensive skills and knowledge in the area to be audited.

Reference [1] provides generic knowledge and skills of management system auditors. The four areas in which internal auditors should be equipped are highlighted below:

1) Audit principles, procedures and methods;
2) Management system and reference documents;
3) Organizational context;
4) Applicable legal and contractual requirements and other requirements that apply to the organization.

The generic knowledge and skills in the auditing management system should be complemented with the competence in the auditing information security area.

According to [7], ISMS internal auditors should also be equipped with ISMS specific knowledge and skills. There are three areas highlighted in which internal auditors should be competent with, which are as follows:

1) Information security management method, which includes the information security terminology, management principles and risk management methods and their application;
2) General knowledge in information technology and information security techniques applicable or access thereto. For example, if an organization implements physical and logical access controls, the auditors should have access to the knowledge on access controls technology and techniques;
3) Current information security threats, vulnerabilities and controls for the ISMS in the organizations.

The ISMS-IA certification will assess the competence of the ISMS internal auditors based on generic and ISMS specific knowledge and skills.

IV. CyberSecurity Malaysia's Role in Information Security

The National CyberSecurity Policy (NCSP) of Malaysia emphasizes the importance to protect the Critical National Information Infrastructure (CNII) in the country. The objective of the NCSP is to accumulate national effort in securing CNII by addressing the risks to the networked information systems of 10 critical sectors in Malaysia. CyberSecurity Malaysia, under the purview of the Ministry of Science, Technology and Innovation (MOSTI), is established to coordinate the effort and strengthen the country's cyber security area. One of CSM's key functions is to promote compliance to information security standards across the CNII and grow the competency of information security professionals in the country. In 2010, in achieving the NCSP's objective, the government has given a directive to all CNIIs to be ISO/IEC 27001 certified by the end of 2012. Pursuant to the directive, as of 2015, 230 organizations in Malaysia are now certified against the ISO/IEC 27001 [8].

The ISO/IEC 27001 standard is used throughout the world by organizations as a basis for the management of the organization's policy and implementation of information security. It is being used by small, medium and large organizations across a diverse range of business sectors. In fact, the standard has become the de facto for information security management. As a body that promotes compliance to information security standards, CSM itself is an ISO/IEC 27001 certified organization. It is also the certification body for the CSM27001 scheme that certifies organizations based on the ISO/IEC 27001 standard. CSM is entrusted by the government to safeguard the security of Malaysia's cyberspace by strengthening the national cybersecurity capability. To achieve this, CSM has taken the initiative to establish the ISMS-IA certification scheme, which is an internationally recognized certification scheme that certifies internal auditors who audit the ISMS in organizations.

Through the ISMS-IA certification scheme, CSM can contribute in promoting the competence of ISMS internal auditors. Through the certification scheme, the knowledge and skills for internal auditors can be developed, assessed and monitored. As effectiveness of an internal audit largely depends on the competence of the auditors, ISMS-IA certification can provide assurance that certified auditors are capable of conducting audits, thus achieving the ISMS internal audit objectives.

V. Towards ISO/IEC 17024 Accreditation

The ISO/IEC 17024 is an international standard used to accredit certification bodies that certify personnel. This standard ensures that a certification body has a structured method and process to verify the competency of personnel. As a certification body, CSM is currently taking the initiative to develop the ISMS-IA certification scheme and later obtain the ISO/IEC 17024 accreditation. The ISMS-IA accredited scheme can be used to recognize, approve and promote the competence of national ISMS internal auditors. By complying

with the ISO/IEC 17024 requirements, the knowledge and skills of the ISMS internal auditors can be standardized, consistent and can be trusted.

The ISMS-IA certification scheme is developed based on three main standards. Firstly, ISO 19011 describes the principles of auditing and guidance on the general knowledge and skills for management systems internal auditors. Secondly, ISO/IEC 27007 provides additional guidance to the ISO 19011 but is more specific for ISMS auditors. Lastly, the ISO/IEC 27001 elaborates on the requirements to establish, implement, maintain and continually improve the ISMS in an organization. Based on these standards, the ISMS-IA assessment criteria and examination questions are established.

VI. The ISMS-IA Certification Scheme

A. Certification Process

In the effort to obtain the ISO/IEC 17024 accreditation, appropriate procedures and methods to assess the competence of ISMS internal auditors must be developed. Procedures and methods developed will be accredited by the Department of Standards Malaysia. Fig. 1 shows the process of ISMS-IA certification.

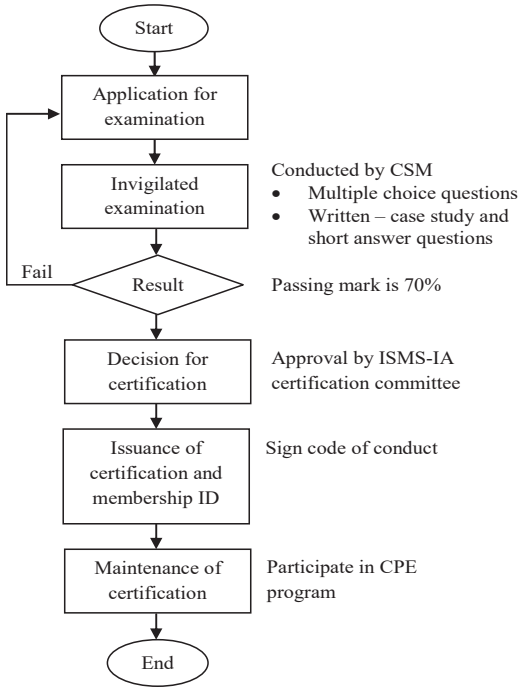

Fig. 1 ISMS-IA Certification Process

B. Knowledge and Skills

The knowledge and skills area for the ISMS Internal Auditor (ISMS-IA) assessment is based on these standards:

1) ISO 19011:2011 Guidelines for auditing management systems;
2) ISO/IEC 27007:2011 Guidelines for information security management systems auditing; and,
3) ISO/IEC 27001:2013 Information security management systems requirements.

Based on these standards, nine topics were identified to develop the assessment for ISMS-IA certification. The ISMS-IA knowledge and skills area is shown in Table I.

TABLE I
ISMS-IA Assessment

Knowledge and Skills	Assessment Method
Topic 1: Overview of information security management • Processes, science and technology underlying information security management • Current information security threats, vulnerabilities and controls • Overview on other relevant standards and guidelines such as ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005	Multiple choice questions
Topic 2: Laws and regulations dealing with information security • PDPA, copyright act, computer crime act and other relevant acts	Multiple choice questions
Topic 3: Requirements of ISMS • Identification and evaluation of customer and interested parties' requirements • Risk assessment and trends in technology, threats and vulnerabilities • Information security risk management • Methods and practices for information security controls • Methods and practices for information integrity and sensitivity • Methods and practices for measuring and evaluating effectiveness of the ISMS and associated controls • Methods and practices for measuring, monitoring and recording performance	Multiple choice questions
Topic 4: Principles of auditing • Six principles of auditing • PDCA of audit programme	Multiple choice questions
Topic 5: Initiating the audit • Audit planning • Initiating and preparing on-site audit • Developing audit plan, scope and audit criteria	Written
Topic 6: Preparing audit activities • Performing document review in preparation for the audit • Preparing audit plan • Preparing work documents	Written
Topic 7: Conducting audit activities • Opening meeting • Performing document review while conducting audit • Communicating during audit • Collecting and verifying information • Generating audit findings • Preparing audit conclusions • Closing meeting	Written
Topic 8: Preparing audit report • Preparing audit report • Completing audit	Multiple choice questions
Topic 9: Conducting audit follow-up • Audit follow up	Written

C. Maintenance of Certification

ISMS-IA certification is valid for a period of three years. Certified auditors are required to participate in the Continuing Professional Education (CPE) program to maintain their certification status. The CPE program requires auditors to accrue points through regular participation in audits and continual professional development. Every three years, ISMS-IA auditors must submit the following declaration of activities to the Certification Body:

- Evidence of audit activities (sampled audit reports);

- Evidence of formal continuing education trainings;
- Evidence of attendance of meetings, seminars and conferences;
- Evidence of authoring articles, presentation; and,
- Evidence of examination on knowledge and skills.

The declaration of activities will be audited by the certification body once every three years. Submission of the declaration is mandatory to maintain ISMS-IA certification. Failure to comply with this requirement will result in suspension of the certification.

VII. Conclusion

CyberSecurity Malaysia's initiative to be recognized as a certification body for ISMS internal auditors is one of its commitments in ensuring organizations' compliance with the ISO/IEC 27001 standard. Through this certification, the competence of ISMS internal auditors in Malaysia can be assessed and assured, thus contributing to the audit effectiveness in organizations.

References

[1] ISO E. 19011. Guidelines for auditing management systems. 2011.
[2] Common Nonconformities. Available: https://www.batalas.co.uk/how-to-guides/auditing-iso-basics/common-nonconformities/.
[3] Top 3 Major Non-Conformities in ISO27001. http://www.itgovernance.co.uk/blog/top-3-major-non-conformities-in-iso27001/.
[4] M. Schelker, "Auditor expertise: Evidence from the public sector." Economics Letters, 116(3), 2012, pp. 432-435.
[5] D. Getie Mihret, D. and A. Wondim Yismaw, "Internal audit effectiveness: an Ethiopian public sector case study." Managerial Auditing Journal, 22(5), 2007, pp. 470-484.
[6] ISO/IEC E. 27000. Information security management systems-Overview and vocabulary. 2014.
[7] ISO/IEC 27007. Guidelines for information security management systems auditing. 2011.
[8] Department of Standards Malaysia Accreditation Statistics. Available: http://www.jsm.gov.my/statistics#.