Developing a Competency Framework for Building Cybersecurity Professionals

Ruhama Mohammed Zain[1], Zahri Yunos[2] , Mustaffa Ahmad[3], Lee Hwee Hsiung[4], and Jeffrey Bannister[5]
[1,2,3,4] CyberSecurity Malaysia
[5]Orbitage Sdn Bhd, Malaysia
ruhama@cybersecurity.my, zahri@cybersecurity.my, mus@cybersecurity.my, hh.lee@cybersecurity.my, jbannister@orbitage.com

Abstract **- The provision of secure networks and services is becoming more critical with the continuing growth of online services and prevalent hacks against systems. In particular, at the national level, countries must protect their critical infrastructure from malicious attacks. Central to this is the requirement to have an adequate pool of industry professionals who are well-versed in cybersecurity. These skillsets must be built and maintained in a structured manner and have a roadmap of lifelong learning for sustainability. A wide range of cybersecurity certification schemes are available; however, many are either prohibitively expensive to build large pools of professionals or have assessment mechanisms that do not measure individual abilities practically. This paper presents an approach to define a structured framework for building core critical skills in cybersecurity that is in line with industry requirements, provides a lifelong learning roadmap, incorporates professionalism and has a practical, competency-based assessment mechanism.**

KEYWORDS - Competency Framework, Cybersecurity Professional, Cybersecurity Education, Knowledge, Skill, Attitude, KSA

I. INTRODUCTION

According to a recent article in Forbes magazine [1] that cites figures from the Information Systems Audit and Control Association (ISACA), an information security advocacy group, a global shortage of two million cybersecurity professionals is predicted by 2019. In the U.S., employers are currently struggling to fill cybersecurity positions, with many job ads going unanswered. Cisco's 2017 security survey found that certification and talents are the third and fourth barriers respectively, to effective security implementation.

In addition to vendor specific certifications, there is a growing number of vendor-neutral certifications. In the cybersecurity domain, several well-respected certifications are in existence. Whilst some of these are specific to particular equipment or processes, many are not and the coverage is extensive. For instance, Law Enforcement Agencies are seeking forensics to capture criminals, "C" level addresses risk, governance and business continuity, and Government Armed Services are looking for ways to defend a country.

Numerous "generic" national, regional and international standards, recommendations and guidelines have been developed and can be referenced by program developers in creating learning programs [2][3]. However, an assessment mechanism, particularly at the entry level, focuses on online assessments. In addition, many dominant assessment mechanisms are exorbitantly expensive for organisations to build large numbers of certified personnel.

II. METHODOLOGY

The Global Accredited Cybersecurity Education Scheme (Global ACE Scheme) introduced by CyberSecurity Malaysia, an agency under the Ministry of Communication and Multimedia, Malaysia, is a holistic cybersecurity professional certification framework. It outlines the overall approach, independent assessment requirements, examination impartiality, trainer competences, cybersecurity domain identification and classification, professional membership requirements and professional development action plans. This scheme, similar to cybersecurity itself, is applicable and relevant across all Critical National Information Infrastructure (CNII) sectors, including national defence and security, banking & finance, information & communications,

energy, transportation, water, health services, government, emergency services and food & agriculture, as they all rely on secure IT systems. The Global ACE Scheme was developed in line with international standards ISO/IEC 9000 series [4] on processes, ISO/IEC 17024 [5] on people certification and ISO/IEC 27001 [6] on security management.

Contributions of this paper are in describing the key features of the Global ACE Scheme framework and highlighting the principal benefits of the scheme, which centres on competency-based assessment and affordability. This article also explains the structure and elements of the Knowledge, Skills and Attitudes (KSA) descriptors and how KSA links to training and assessment.

III. DISCUSSION

A. The Need For Competence-Based Assessment

It is essential today to have controls, policies and processes in place to ensure business continuity. Every day major issues arise with online systems, such as large amounts of personal details, medical records, credit card and other sensitive information being stolen or locked and encrypted by ransomware, or systems/mechanisms being compromised to steal data. This is not only happening to industry organisations but also to governments [7].

In today's environment, security awareness, knowledge and skills need to be central rather than peripheral. This requires an adequate pool of industry professionals who are well-versed in cybersecurity. The skillsets must be built and maintained in a structured manner and have a roadmap of lifelong learning for sustainability.

Many recent cases of massive security breaches have made headlines, indicating that despite technical advances, systems are still vulnerable, while lack of skills and awareness in the cybersecurity area is a key contributing factor [8]. As an example, the recent 'WannaCry' ransomware attacks affected systems that were not patched and updated – a crucial area that should be addressed by a proper security policy implemented in an organisation [9].

Countries are now adding cybersecurity skills as part of the national agenda, right through the learning life cycle from promoting cybersecurity as a career choice all the way through to reskilling and continual professional development. For instance, a UK government "National Cyber Security Strategy 2016-2021" report [10] stated the following in its opening lines, and committed £1.9b to the strategy over the next 5 years:

"The challenge of our generation is to build a flourishing digital society that is both resilient to cyber threats, and equipped with the knowledge and capabilities required to maximise opportunities and manage risks" [10]

In the 1990s the Internet took hold and began growing at a tremendous rate. This meant huge volumes of equipment to be sold and maintained. As such, a "quick" method of certifying personnel who could perform "configuration" correctly needed to be rolled out globally. This gauntlet was taken up by Information Technology (IT) vendors who quickly realised that the more people were certified, the more equipment they could sell. Many of these programs were very well-designed in terms of content; however, to scale up and reach the masses, a simple assessment method was required, consisting of sets of online multiple choice questions offered through "prometric" testing centres [11]. It should be noted that some vendors had structured pathways to advanced levels that incorporate "practical, hands-on" assessment. Although this met "quick-fix" needs in the 1990s, in today's world it is viewed as sorely lacking [12]. Two main concerns arising from these types of assessment that significantly reduce their effectiveness for employers are:

i. They mainly measure knowledge and memory capacity and have limited effectiveness in measuring critical thinking skills;
ii. A question bank is often available and training programs on passing exams are offered.

Technical personnel are now not only expected to configure but also to have an end-to-end view of a complete system, understand "why" a configuration is done in a particular way, and be able to configure various equipment from different vendors securely by having a transferrable skill set. All of this needs to be captured in the assessment mechanism, so that employers can be confident in somebody's ability rather than

their skills in memorising multiple choice questions [13].

It should be noted that DoD Directive 8570.01-M [14] requires personnel with privileged access to DoD systems to have recognised certification. CompTIA Advanced Security Practitioner (CASP) [15] currently meets this requirement via only 80 multiple choice questions. Clearly, there is a requirement for a better means of assessing whether the certified person can actually perform the tasks required of a given job role.

The Global ACE Scheme is designed to enhance both the knowledge and skill sets of cybersecurity professionals with current and state-of-the-art techniques for strategizing, mitigating, developing and providing cybersecurity services. This ensures optimal application of cybersecurity knowledge and skills in the wider community.

B. The Challenge For Human Resource Departments

In most organisations, it falls on Human Resources (HR) to manage staff development and up-skilling. It has been observed, particularly in large technical organisations, that there is often a disconnection between HR and technical managers in terms of training development. Since technical managers do not generally see development as their job, they may provide HR with limited feedback. Consequently, because HR personnel are not generally technical, they source the same programs and certifications used previously, as they might not be aware of alternatives or able to interpret the technical requirements adequately.

At this time, organisations need to be more agile to meet market requirements. Hence, HR is expected to provide more such as consider strategic plans for organisational competency development, whereby skills are developed in a structured manner [16]. In many cases, HR does not have in-house capabilities to identify critical security competences and thus needs to work with external consulting organisations that have the necessary track record and expertise in the area. In the context of cybersecurity, such framework provides HR with a ready-made solution for developing skills. The framework thus has already identified the skills required by the industry, has a roadmap from foundation through to specialization, and offers a practical, hands-on certification process that validates individual ability to apply their skills.

The Global ACE Scheme is designed to measure an individual's ability to "do" a given task and understand "why" it is done by taking context into consideration rather than relying solely on knowledge-based assessments. It consists of 3 levels: foundation, practitioner and specialist, as highlighted in Figure 1.

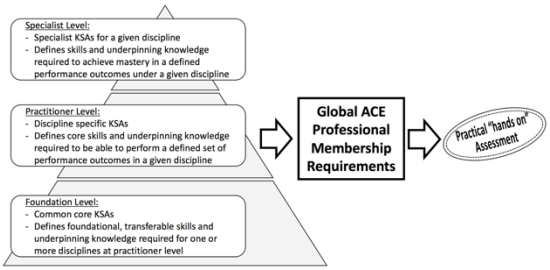

Figure 1: Competency framework

Each level consists of a number of competency modules referred to as KSA Descriptors (Knowledge, Skills, Attitudes) that prescribe a particular set of skills. For the purposes of this scheme, competency is defined as a skill plus the underpinning knowledge associated with that skill. At lower framework levels, these KSA Descriptors are written so as to enable the "transferability of skills" between job functions. Thus, a flexible, lifelong learning roadmap is possible with multiple career changes in the cybersecurity field. The framework is extendable in terms of the number of Descriptors based on industry requirements as identified via industry focus group workshops. Bloom's taxonomy [17] serves to ensure that the levelling complies with international norms and that there is consistency at a given level across descriptors. Further details on alignment with other reputable systems and how assessment reliability, validity and verification are ensured are given below.

C. Building A Structure For Identifying Competencies: The Ksa Descriptor (Knowledge, Skills, Attitudes)

Before it is possible to identify, develop, measure and maintain the "competencies" that the industry requires, a structured template is needed first, which can frame the requirements. This template provides a model to maintain consistency across each distinct area defined. For the purpose of this professional cybersecurity certification scheme, the template is referred to as a KSA Descriptor, the structure of which is the work product of a set of workshops conducted with a broad representation of industry players, cybersecurity experts, government

representatives and cybersecurity professionals. The KSA Descriptor's key purpose is to act as a reference guide, identifying the skills, underpinning knowledge and attitudes that professionals in the cybersecurity area require. The core functions of the KSA Descriptor are to act as:

i. A reference for training providers to facilitate the development of suitable training courses relevant to the identified roles and functions;
ii. A reference for developing examination questions to effectively assess the identified job roles and functions;
iii. A reference for developing professional trainers able to effectively deliver training in line with the requirements of the identified job roles and functions.

One of the first questions to be addressed when developing the template is whether it should be framed from the perspective of a set of job functions or a set of learning outcomes. Since the main goal of the scheme is to develop cybersecurity professionals, we decided that it should lean towards training/development while keeping in mind that it should closely follow the performance requirements for a job. Therefore, a central part of the KSA Descriptor is to identify a set of performance outcomes for each given area; in other schemes, these are often referred to as 'tasks' [3].

The KSA Descriptor defines a benchmark of Knowledge, Skills and Attitudes onto which both training and assessment are mapped. Critical to success is for the certification to maintain quality throughout all processes to ensure that credibility is maintained. Therefore, in addition to the details of the KSA elements, a set of processes is also necessary to ensure quality and consistency are maintained throughout, as discussed in this paper under the heading "An ecosystem for skill development and assessment".

Another question arising during the definition phase is regarding the "A" in KSA. A survey of existing KSA type structures indicates that "A" referring to Ability or Attitude tends to occur in equal measures. However, it does become apparent that when referring to ability, it is challenging to discern the differences between a "skill" and an "ability" and there seems to be no consensus regarding this [18]. Using "attitude" fits in well with the overall philosophy of professional certification in cybersecurity, since attitude is an important attribute of a professional, particularly when related to security matters. We found, for example, that "ethics" features extensively in matters related to security and should be blended into the fabric of skill development in this area.

The proposed framework shall address the three research areas and will not only focus on specific problems in isolation, for example, it assesses security in a SCADA network or makes a threat assessment of the latest zero-day vulnerability affecting a SCADA vendor [19]. The idea is to look at an overall research framework with the aim of increasing the dependability, resiliency and robustness of the SCADA network to support its critical processes.

The KSA Descriptor structure is split into five main sections, which are described in Table 1.

Table 1: Explanation of the Main KSA Descriptor Sections

Section	Explanation
Summary	Provides an overall summary of the scope and performance outcomes of the KSA descriptor, including pathway, document ID, version & date and an overview of the recommended training & assessment delivery mechanisms.
Knowledge (K)	Provides a set of Knowledge elements for the competency area. This is what one should "know."
Skills (S)	Provides a set of Skills elements for the competency area. This is what one should be "able to do."
Assessment Methods	Provides a legend to explain the different possible assessment methods for the K & S elements
Attitudes (A)	Provides a set of Attitudes elements for the competency area. This is what traits one should exhibit. Unlike the K & S elements, it is not expected that an assessment method should explicitly measure these, but rather that a training program should blend them into the learning fabric. This must be evaluated when the training program is submitted for evaluation.

The major information elements of the summary section are explained in Table 2.

Table 2: KSA Descriptor - Summary Section

Section	Explanation
Synopsis	Provides an overview of the KSA descriptor scope. This is useful for HR personnel to get a summary of the KSAs and assist with mapping the competency area to the relevant job roles in an

	organisation.
Performance Outcomes	Provides a set of outcomes that a successful individual should be able to demonstrate if they possess all KSA elements – these could also be termed "tasks".
Learning Pathway	Identifies where this fits in the overall development roadmap.
Recommended learning time	Provides a minimum time benchmark for the duration of a course of building these KSAs in numbers of hours.
Training Strategy	Provides a summary of the type of learning environment to which a training program is expected to align.
Required Experience/Qualifications	Identifies pre-requisites expected before one would approach this set of KSAs. This is described in general terms and, if available, a KSA that identifies the pre-requisites.

The Knowledge elements are explained below in Table 3.

Table 3: KSA Descriptor - Knowledge Section

Section	Explanation
Knowledge Element	Each knowledge element breaks the competency area down into the required knowledge at sufficient granularity at which it can be assessed. Training providers use this to ensure the knowledge element is covered sufficiently in training; exam question authors use this to ensure the element is assessed effectively. Both will utilize the Indicator for further scope clarification.
Indicator	The indicator provides further clarification on the knowledge element scope. It provides the information to allow both training organisations and examiners to build content & assessments to ensure the topic is addressed.
Weightage	Provides an indication of the amount of coverage there should be in the overall course/examination, e.g. 5% would indicate that in a 40-hour course, 2 hours should be spent on this Knowledge element.
Assessment Method	For element assessment, the method provides an indicator of the recommended way in which it should be assessed. A letter code is given to identify the method (e.g. PA – practical assessment, etc.) as shown in the legend below the elements (see Table 5). Appropriate learning & assessment techniques and educational best practices should be used in assessment development.

The skills elements are explained as follows in Table 4.

Table 4: KSA Descriptor - Skills Section

Section	Explanation
Skills Element	Each skills element breaks down the competency area into the required skills at sufficient granularity for assessment. Training providers use this to ensure the skills element is covered sufficiently in training; exam question authors use this to ensure the element is assessed effectively. Both utilize the indicator for further scope clarification.
Indicator	The indicator provides further clarification on the skills element scope. It provides the information to allow both training organisations and examiners to build content & assessments to ensure the topic is addressed.
Weightage	This provides an indication of the amount of coverage there should be in the overall course/examination, e.g. 10% would indicate that in a 40-hour course, 4 hours should be spent on this skills element, i.e. practical activities
Assessment Method	For the assessment of this element, the method provides an indicator of the recommended way in which it should be assessed. A letter code is given to identify the method (e.g. PA – practical assessment, etc.) as shown in the legend below the elements (see Table 5). Appropriate learning & assessment techniques and educational best practices should be used in the development of assessments.

Finally, each attitudes element breaks down the behaviours that should be developed and exhibited after training. Training providers use this to ensure the attitudes element is covered sufficiently in training; exam question authors do not need to use this, as the attitudes are not assessed separately but rather should be blended into the fabric of knowledge and skills development.

D. Identifying And Defining Key Industry Skill Requirements In The Cybersecurity Space

The approach adopted to identify and define industry requirements is to assemble a cross section of industry players for whom cybersecurity is critical, as well as academic representatives. This is done for two main reasons:

i. Placing the two groups to work together means that skill requirements can be identified to meet industry requirements while also being structured in a way suitable for developing learning programs and assessment mechanisms.
ii. Industry and academia are able to share their individual perspectives and appreciate each other's roles and viewpoints.

A number of workshops took place to identify the areas with wide appeal across industries as the core, in-demand skillsets, and subsequently build the KSA Descriptors for each.

One of the key outcomes is that to build skills in cybersecurity, technical practitioners need a solid foundation that addresses two fundamental areas: computer networks and operating systems. It was found that before an individual may consider security, they need to understand how services are offered and how traffic flows to and from these services. Thus, descriptors were built to identify these core skills and to act as pre-requisites for security-specific disciplines.

The descriptors were consolidated and circulated to produce a finalised set. The KSA Descriptors developed in this first phase are as follows:

i. Cybersecurity Core/Foundations:
   a. Computer Networking (security)
   b. Operating Systems (security)

ii. Cybersecurity-specific:
   a. Business Continuity
   b. Intrusion Detection, Monitoring & Prevention
   c. Penetration Testing
   d. Secure Application Development
   e. Digital Forensics
   f. Internet of Things (IoT) – security

E. An Ecosystem For Skill Development And Assessment

The KSA Descriptor forms a common benchmark for each defined area that specifies what the training and assessment outcomes should be. Figure 2 below shows the relationship between training, assessment and the KSA Descriptor.

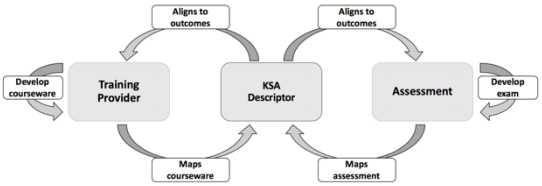

Figure 2: Relationship between training, assessment and the KSA Descriptor

To succeed, mechanisms and processes need to be in place to evaluate and validate training and assessment to ensure the following outcomes:

i. Training and assessments align with the KSA descriptor
ii. There is adequate and balanced coverage of each descriptor element based on the defined weightage
iii. The training and assessment delivery mechanisms are consistent and meet the quality requirements set by Global ACE

For example, in training course development, the course developer must ensure that in developing the training materials:

i. Each Knowledge element is covered in the training materials, e.g. slides and notes
ii. Each Skills element is covered in the practical exercises
iii. For each, the indicators are used to clarify the scope of coverage
iv. The correct weightage is achieved for each element
v. There is a strategy to develop and reinforce the Attitude elements throughout the training

Upon submitting course materials to an evaluation panel, the training organisation must adhere to the evaluation requirements. This includes marking all training materials to validate that all KSA elements are covered, for example:

i. Provide highlighted slides, workbooks, notes, etc. to identify that each Knowledge & Skills element is addressed;
ii. Provide a schedule to indicate the coverage of each element with the correct weightage
iii. Provide a description of the training philosophy & mechanisms used to

build the Attitude elements through the Knowledge & Skills elements

For assessment delivery, the exam system must ensure that the appropriate assessment technique is used to assess each Knowledge & Skills element, e.g. if the descriptor indicates that "PA" practical assessment should be used, then the exam system must assess this in a practical context. It should be noted that does not preclude the use of a computer-based examination system; however, it must demonstrate how the system can emulate a live environment/scenario. The assessment must also ensure there is sufficient coverage of each Knowledge & Skills element in accordance with the weightage guidelines provided in the descriptor, e.g. if the Knowledge element indicates "MC" is the assessment method and 5% is the weightage and if the exam has 40 multiple choice questions, at least two should cover the element. The overall weightage in the exam must be maintained, e.g. if there is a set of short answer/written questions in addition to multiple choice questions, this should not dilute the weightage of the topic.

F. Assessment: The Importance Of Measuring Skills Practically

As mentioned earlier, effective assessment is a central requirement for structured skill development. The closer the assessment methods and criteria are to a real-world situation, the more successfully an organization can identify that an individual is competent [1][11].

For this reason, central to the KSA framework is that the assessment should cover both the Knowledge and Skills elements determined based on what the industry requires individuals to do as part of their jobs. The assessment methods are defined in the KSA Descriptor as follows:

Table 5: Assessment methods

KSA	Associated Assessment Methods	When Assessed
Knowledge	Continual assessment (CA)	During training
	Multiple Choice (MC)	Post training
	Theory/underpinning knowledge assessment (UK)	Post training During/post training
	Assignments (AS)	During/post training
	Case Studies (CS)	
Skills	Continual assessment (CA)	During training
	Practical assessment (PA)	Post training
	Assignments (AS)	During/post training
	Case Studies (CS)	During/post training

G. Managing & Tracking Professional Development

Managing and tracking certified professionals are two key activities to attract and retain scheme members. One vital mechanism to achieve this is to require that certified professionals maintain Continuing Professional Development (CPD) points in order to renew their membership status. It is a requirement under the scheme that certified members are constantly up-to-date with state-of-the-art developments in the field and technological changes. This will prevent the certifications from becoming outdated too quickly due to the fast-changing nature of cybersecurity. The Global ACE Scheme facilitates and enables opportunities for certified professionals to earn CPD points by organizing educational and professional events and publishing a list of recognized external events and activities. This fully supports the Malaysia Board of Technologists (MBOT) [20] function to promote education and training such that registered professionals may further enhance their knowledge related to their professions. Members will also benefit by having access to other experts in the course of attending the programs while at the same time enhancing their knowledge and skills.

H. Alignment With National Higher Education Ministries And Government Training Agencies

In Malaysia, the Ministry of Higher Education (MoHE), Malaysian Qualifications Agency (MQA) & Ministry of Human Resources/Department of Skills Development (JPK) are well-established and are the key organizations covering the spectrum of post school qualifications. MoHE and MQA govern both public and private universities and colleges, with JPK in charge of skills development with all three using the Malaysian Qualifications Framework (MQF) [21]. These organizations have a wealth of knowledge and processes in place to ensure quality mechanisms throughout the whole

value chain to ensure credibility, review of processes and sustainability [22][23].

The Global ACE scheme does not intend to reinvent the wheel in terms of certification, but recognizes that there are many Cybersecurity Professional Certifications on the market. Mechanisms will be put in place to determine how persons with such certifications can have a route to specialist certification if they so desire. The relevant committees will evaluate reputable certifications on the market and look at how to map them to the KSA Framework levels and standards [24].

I. Validation By Experts

The Global ACE Scheme framework has been validated by experts from industry, academia and the Malaysian government. The validation mechanism was a series of meetings and workshops during which all aspects of the framework were proposed, deliberated, revised based on feedback received and presented again for final acceptance by the relevant committees. Table 6 summarizes some of the meetings and workshops conducted to validate the scheme. The nature of engagement with experts from academia, government and industry is described along with the number of workshops held and the total number of attendees.

Table 6: Meetings and workshops conducted

Sector	Nature of engagement	Number of workshops	Number of attendees
Academia	• Scheme framework development • KSA descriptor development • Assessment questions development • Board of governance	16	63
Government	• Scheme framework development • KSA descriptor development • Scheme risk management • Board of governance	16	157
Industry	• Scheme framework development • KSA descriptor development • Assessment questions development • Board of governance • Training content mapping & alignment	15	95

IV. LIMITATION

It is acknowledged that this is a preliminary study that seeks to identify and build the necessary components for a competency-based framework for developing cybersecurity professionals. In order to improve this framework further, an in-depth study of existing training and certification frameworks will have to be undertaken for the purpose of comparison and ensuring its continued relevance and currency. This is reserved as a future work.

V. CONCLUSION

The Global ACE scheme takes a competency-based approach that focuses on building and assessing both knowledge and skills in a practical context across key domains within the cybersecurity landscape. This approach was chosen to address the critically growing global shortage of talent in the cybersecurity field. The emphasis is on assessments that measure practical competence rather than purely theoretical and/or multiple- choice question assessments alone. In short, the scheme aims to produce cyber-security professionals with the necessary critical thinking skills, confidence and true ability to complete tasks. The scheme also outlines a structured roadmap to build and maintain professionals across the cybersecurity domain.

For future work, a detailed study to compare this scheme framework to other training and certification scheme frameworks is proposed. It would also be fruitful to research the outcome of implementing this scheme in terms of the number and quality of cybersecurity professionals produced.

VI. REFERENCES

[1] J. Kauflin, "The Fast-Growing Job with a Huge Skills Gap: Cyber Security," Forbes, Mar-2017.

[2] SFIA framework — SFIA," SFIA Foundation, 2015. [Online]. Available: https://www.sfia-online.org/en/sfia-6. [Accessed: 03-Jan-2018].

[3] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," NIST Spec. Publ., pp. 800–181.

[4] "ISO 9001:2015 Quality Management Systems." International Organization for Standardization, Geneva, Switzerland, 2015.

[5] "ISO/IEC 17024:2012 Conformity assessment -- General requirements for bodies operating certification of persons." International Organization for Standardization, Geneva, Switzerland, 2012.

[6] "ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements." International Organization for Standardization, Geneva, Switzerland, 2013.

[7] "Cisco 2017 Annual Cybersecurity Report," San Jose, California, 2017.

[8] "Mitigating the Cybersecurity Skills Shortage Top Insights and Actions from Cisco Security Advisory Services," 2015.

[9] S. Gibbs, "WannaCry: hackers withdraw £108,000 of bitcoin ransom | Technology | The Guardian," The Guardian, 2017. [Online]. Available: https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom. [Accessed: 03-Jan-2018].

[10] UK Government, "National Cyber Security Strategy 2016-2021," 2016.

[11] Prometric, "Overview," 2017. [Online]. Available: https://www.prometric.com/en-us/about-prometric/pages/prometric-advantage-overview.aspx. [Accessed: 03-Jan-2018].

[12] J. Richard, "Forensication Education: Towards a Digital Forensics Instructional Framework Forensication Education: Towards a Digital Forensics Instructional Framework GIAC (GCFE) Gold Certification Forensication Education 2," SANS Institute, InfoSec Read. Room, 2017.

[13] H. Bound, A. Chia, and S. Yang, "Assessment for the changing nature of work," Inst. Adult Learn., 2016.

[14] "Information Assurance Workforce Improvement Program," DoD 8570.01-M, 2015.

[15] "(CASP) Advanced Security Practitioner Certification | CompTIA IT Certifications," certification.comptia.org, 2017. [Online]. Available: https://certification.comptia.org/certifications/comptia-advanced-security-practitioner. [Accessed: 03-Jan-2018].

[16] J. Gothelf, "How HR Can Become Agile (and Why It Needs To)," Harvard Business Review, 2017. [Online]. Available: https://hbr.org/2017/06/how-hr-can-become-agile-and-why-it-needs-to. [Accessed: 03-Jan-2018].

[17] D. R. Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain. New York: David McKay Company. Inc., 1956.

[18] D. H. P. R. G. & Collier, Motor Learning and Development. Human Kinetics, 2011.

[19] E. Byres, D. Leversage, and N. Kube, Security incidents and trends in SCADA and process industries. The industrial ethernet book, 2007.

[20] "Malaysia Board of Technologists," 2017. [Online]. Available: http://www.mbot.org.my. [Accessed: 08-Dec-2017].

[21] Malaysia Qualifications Agency, "Malaysian Qualifications Framework Point of Reference and Joint Understanding of Higher Education Qualifications in Malaysia." 2016.

[22] Jabatan Pembangunan Kemahiran, "Jabatan Pembangunan Kemahiran - Home," 2017. [Online]. Available: http://www.dsd.gov.my/index.php/en/. [Accessed: 08-Dec-2017].

[23] Kementerian Pendidikan Tinggi, "KPT - Utama," 2017. [Online]. Available: http://mohe.gov.my/. [Accessed: 04-Jan-2018].

[24] "Cyber Security Certifications | Explore Your Options," Cyber Degrees, 2017. [Online]. Available: http://www.cyberdegrees.org/resources/certifications/. [Accessed: 03-Jan-2018]