Building Cybersecurity Competency through Global ACE Certification

Against a backdrop of escalating cyber threats and mass digitalisation, the global cybersecurity job market is growing exponentially with a surge in demand for cybersecurity professionals. As companies of all sizes across the globe migrate to digital platforms spurred more recently by the pandemic, they require cybersecurity experts to design, engineer, and maintain cybersecurity systems and infrastructure.

According to independent market research firm Providence Strategic Partners, the total cybersecurity industry in Malaysia is forecasted to grow by 18.7% CAGR from an estimated RM3.9 billion in 2021 to RM5.5 billion in 2023. Despite the rapid industry growth, Malaysia still lags behind in cyber security talent pool development. Malaysia recorded a shortage of almost 8,000 cyber security professionals in 2020. Meanwhile, Malaysia Digital Economic Blueprint (MyDigital) has set a goal for the nation to produce 20,000 cyber security experts by 2025.

With the escalating threat of cyber-attacks, cyber security spend has also increased dramatically. Based on a report by GlobalData Market Opportunities Forecasts, IT expenditure in Malaysia will reach RM103.75 billion by 2023. As such, there will be a surge in demand for cyber security experts from security analysts and security architects, cyber threat intelligence analysts, consultants and cyber incident analysts.

To protect an organisation against cyber threats, there are three important elements: **people, process** and **technology**. In Malaysia, companies tend to focus on purchasing hardware and technology, but still lack in people element.

What is Global ACE

The Global Accredited Cybersecurity Education (ACE) scheme is a holistic framework of cybersecurity professional certification that outlines the overall approach, independent assessments, impartiality of examinations, competencies of trainers, identification and classification of cyber security domains and the requirements of professional memberships.

The scheme is a systematic plan of actions that certify and recognise competency of cybersecurity workforce. It is industry driven and vendor-neutral, developed in collaboration with government agencies, industry partners and academia. The establishment of the scheme is in tandem with international standards such as ISO 9001 on processes, ISO/IEC 17024 on certification of persons and ISO/IEC 27001 on security management, which is vital to assure workforce capability and experience, secure and validate core skills, knowledge, attitude and experience.

Participants who pass the certification examination are eligible to apply as **Professional Technologies or Certified Technicians** from the Malaysia Board of Technologists (MBOT) under the Technologist and Technicians Act 2015 (Act 768), subject to MBOT terms and conditions.

Global ACE received an award from World Summit on the Information Society (WSIS) in 2020, in recognition of its "Global ACE Certification Centre of Excellence for Building and Lifelong Learning" project.

Why Global ACE Certification

Global ACE Certification encourages advancement in all cyber security professional programmes. Most importantly, organisations will be assured that cyber security professionals have been thoroughly evaluated. Global ACE also enhances the skill-sets of the cybersecurity workforce congruent with local and international requirements. In fact, Global ACE Scheme Recognition Arrangement permits mutual recognition of certified cybersecurity workforce across countries.

Through the Global ACE Certification's Mutual Recognition Arrangement, TPP partners have the potential to access to wider market within the OIC member countries. TPP partners are permitted to access training resources such as scheme certified pool of trainers, training facilities and examination centres

Enhance KSA through Global ACE

KSA stands for **Knowledge**, **Skills** and **Attitude**, three main tenets upon which Global Ace certification and training is structured. KSA forms a reference point for training providers to design cyber security training courses. It also serves as reference for the development of examination questions to effectively assess the identified job roles and functions, thus facilitates delivery of training courses in line with the requirements of the identified job roles and functions.

Global ACE Certification defines competency as a skill equipped with relevant knowledge associated with KSA. It serves as an indicator that an individual meets a minimum standard of knowledge and skill, which can be used to demonstrate competency for current or potential employers.

Ensuring High Competency through Global ACE

The Global ACE framework encompasses two broad categories, namely **"Cyber Security Technical Competencies"** and **"Cyber Security Generic Competencies".** Technical competency refers to technical skills and knowledge required by a professional to conduct its task as a certified professional from Digital Forensics, Incident Handling and Response, Security Assurance, Cryptography, Governance, Risk and Compliance.

Global ACE certification also covers **Generic Competencies** in delivering cyber security services and consultation. Such competency covers three domains in soft skill sets from People, Process to Business Acumen skills. Under the people skills domain, members will learn about people management from leadership, coaching to communications and strategic thinking. In addition to dealing with people, they must also apply process management skills that include change management, organisational and even financial management. Last but not least, a competent cyber security professional should possess good business acumen that nurtures entrepreneurship, customer relations and innovativeness among others.

Global ACE Membership

Global ACE Certification offers membership to individuals who have passed the certification examination under the programme. As a qualified member of the programme, an individual gains industry recognition, networking opportunities, priority access to professional development events, and access to members-only knowledge banks and whitepapers.

The membership allows participants to continuously increase their respective cyber security capacity and critical cognitive skills through lifelong learning programs and gain new skills at their own pace. It is also a platform for members to share knowledge, expertise, and skills, identify latest cyber threats as well as appropriate mitigation methods.

Global ACE credentials are maintained by either taking the current certification exam or maintaining Continuing Professional Development (CPD) points.

For cyber security practitioners, there are two broad categories for membership.

Associate Member is a certified individual with less than 5 years working experience in cyber security. To qualify, a candidate must pass any one of the certifications provided by the Global ACE Certification or has obtained other professional certifications that is recognized by the Global ACE Certification and he/she must possess minimum education qualification of a Degree from recognized universities.

To be accepted as **Professional Member** under Global ACE scheme, the criteria required is similar to associate member category but one must have garnered more than 5 years working experience and demonstrated relevant competency and knowledge in cyber security area.

Benefits of Global ACE Certification

Through Global ACE certification, cyber security professionals can increase their value to the organization. More importantly, the scheme provides a competitive advantage for individuals seeking job advancement.

For organisations, the scheme gives them confidence that Global ACE certified individuals who are securing the systems and networks are competent. Through periodic re-certification, Global ACE certification ensures that all certified personnel maintain their knowledge and skills, thus uplifting productivity and competence of Malaysia’s cyber security community.

-END-

About Us

Information Security Certification Body (ISCB) is a department established under CyberSecurity Malaysia since 2008. Based on Malaysian Government Cabinet decision, Malaysian Common Criteria Certification Body (MyCB) is established as the sole Certification Body for the Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme.

After 2010, MyCB had evolve it certification services to CyberSecurity Malaysia Information Security Management System Audit and Certification (CSM27001) Scheme and Malaysia Trustmark for Private Sector (MTPS) Scheme. Therefore, MyCB name is changed to ISCB Department as the department role also grown to other areas of certification which is categories under management system, product and personnel certification.

For more information contact us ***certification[at]cybersecurity.my*** *or visit* ***https://iscb.cybersecurity.my.***