Power of ISMS: Driving Value & Growth for SMEs in Malaysia

As Malaysia progresses swiftly towards becoming a Digital Economy, businesses large or small need to review their operations and processes to embrace digitalisation. Over the past two years, the Covid-19 pandemic has also necessitated Malaysia's SMEs (small and medium enterprises) to digitalise in order to survive due to changing market requirements.

Why should one care about information security?

The core of a business organisation's assets is its information. Information security protects customers and trade secrets. A strong security ecosystem guards against any information risks – be it externally through cyber breaches or worse still, internally through leaks by employees or associates due to disgruntlement or lure of monetary payoff. Protection of personal records and commercially sensitive information is critical within any organisation.

Data breaches are becoming more rampant and severe, yet many organizations still assume they will never suffer one. Most SMEs underestimate their risk level for cyber-attacks. A report by Chubb found that 67% of Malaysian SMEs believed that they are **less likely** to become victims compared to larger corporations, yet the same report found that 84% of SMEs were victims of cyberattacks in 2018. According to Cybersecurity Malaysia, 8,669 cases of cybersecurity incidents were reported to Cyber999 help centre from January to November 2021, the top three categories being fraud, intrusion and malicious code.

It has therefore become mission critical for information to be secured to ensure its **Confidentiality** – meaning data can only be accessed by authorized people; **Integrity** – by keeping data accurate and complete; and **Availability** – data to be accessed as and when it is required. In short, **"CIA"** of information management.

Information Security Management System (ISMS) is a system of processes, documents, technology and people that helps manage, monitor, audit and improve an organisation's information security. One of the most accepted international information security standards is **ISO/IEC 27001**. ISO/IEC 27001 is the international standard for companies that needs a robust approach to managing information security and building resilience. It is a framework that enables organisations to manage security incidents holistically and systematically.

Implementing ISO 27001 will improve internal working relationships and help retain existing customers, as well as provide a proven marketing edge against competitors. More importantly, an ISO 27001-certified ISMS also helps protect an organisation against cyber-attacks and the financial and reputational damage as a result.

With ISMS certification, organisational information is secured in all its forms. Rules will be put in place governing how an organization identify risks, to whom risk ownership is assigned, how such risks will impact the confidentiality, integrity and availability of the information, and the method of estimating the impact and likelihood of the risk. Such methodical approach increases the organisation's resilience to cyber-attacks and provides a centrally managed framework that keeps an organisation's information safe and managing it all in one place.

Robust cyber security requires an ISMS built on three key pillars: **People**, **Processes** and **Technology**. By implementing ISMS, one can secure information, increase resilience to cyber-attacks, and reduce costs associated with information security.

ISMS' holistic approach covers the entire organisation, not just IT. This enables employees to readily understand risks and embrace security controls as part of their everyday working practices. Most importantly, ISMS offers organisation-wide protection from technology-based risks and other more common threats such as poorly informed staff or ineffective procedures.

The main challenge of ISMS implementation lies in the organization itself – whether its top management has the commitment and determination as implementation requires the resources from all levels. Strong commitment from management helps the staff better appreciate the ISMS implementation; and not just for the sake of getting the certification. A lack of clear understanding of the ISO/IEC 27001 standard and information security will be a stumbling block. Therefore, ISMS implementation must be embraced by all. Achieving such certification increases transparency and efficiency in an organization. It also enables an organisation's capability to become **Measurable**, **Verifiable** and **Improvable** for future growth.

ISMS scope and boundaries determine the extent to which the ISMS is applied. Identifying the right ISMS scope is crucial because it will assist organisations in meeting their security requirements and planning for ISMS implementation such as determining resources, timeline and budget required.

"This is best determined by the organization itself as they will know what are the critical services or information that need protection in terms of 'CIA'. Many organizations without the "right" scope end up getting little or no commitment from the top management, or being questioned the benefits of ISMS implementation," said Wan Shafiuddin Zainudin, Head of Information Security Certification Body (ISCB). Therefore, it is important to have good knowledge of the ISO/IEC 27001 standard and other 27000 standards group.

The ISMS scope should be derived from an organisation's known risks. For example, in a financial institution, the risks of unauthorised access of online transactions may give critical impact to its business operations. Thus, the ISMS scope for this financial institution can be defined as online transaction services. For clarity, organisations should seek the advice of a Certification Body (CB) on the proposed ISMS scope and boundaries, as and when the need arises.

The **Information Security Certification Body** (ISCB) is a department within the national cybersecurity specialist agency, **CyberSecurity Malaysia**. ISCB manages and provides certification services based upon three main international standards and guidelines, namely Common Criteria (ISO/IEC 15408), ISMS (ISO/IEC 27001) and the World Trustmark Alliance (WTA) Code of Conduct. ISCB's **CSM27001 scheme** provides a model for certifying organisations against the internationally recognised MS ISO/IEC 27001 ISMS standard.

The process of ISMS certification can be divided into 6 main stages:

Engagement with Certification Body (CB)

The organisation can engage with a CB to discuss the organisation's ISMS scope for ISMS certification. A CB will verify and ensure that the scope and boundaries of an organisation's

ISMS are clearly defined in terms of characteristics of business, its location, assets, and technology.

Enquiry and Quotation

Organisations should complete an enquiry form and forward it to the CB for application review. If there is a need to obtain more information about the organisation's ISMS, or if there is a need to clarify some of the details contained in the application, then CB will contact the organisation to obtain the required additional information.

Once the CB is satisfied with the organisation's application, a quotation will be generated for the certification work to be done. If the organisation accepts the quoted price, provision for legal agreements will be made.

Stage 1 Audit

Part of Stage 1 audit is carried out at the organisation's premises to audit the organisation's ISMS documentation and evaluate the organisation's location and site-specific conditions. The CB will collect necessary information regarding the scope of the management system, processes and location(s) of the organisation; and related statutory and regulatory aspects and compliance. Stage 1 audit findings will be documented and communicated to the organisation, including identification of any areas of concern that could be classified as non-conformity.

Stage 2 Audit

Stage 2 audit evaluates the implementation, including effectiveness of the organisation's ISMS. Where non-conformities are observed, the CB will formally document it in a Non Conformity Report (NCR)/Opportunities For Improvement (OFI) template. The organisation should define all non-conformities and provide an appropriate set of corrective actions to resolve the identified non-conformities.

Certification Approval

All information and audit evidence gathered during Stage 1 and Stage 2 audits will be analysed in order to review the audit findings and agree on the audit conclusions. The CB will make the final decision after all non-conformities have been resolved

Issuance of Certificate

Once approved for certification, the organisation will be entitled to receive a copy of the ISMS certificate. To renew for a further term of 3 years, an organisation needs to notify their CB and provide updates on their ISMS implementation. A recertification audit will then be conducted before expiry of the certificate. If the certification is successfully renewed, similar process of surveillance audits will be carried out by Certification Body.

Information security is only as strong as the weakest link. Through ISMS certification, an organisation can develop a culture of security by integrating security into its corporate structure and daily operations. Utilizing a reputable certification body also enables one to gain customers' trust in certification. Therefore, maximize the return in investment by leveraging on the reputation of a recognised certification authority such as ISCB.

-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.***