Ensuring Business Continuity in the Digital Age

With an unpredictable global weather due to climate change and fresh geopolitical crisis threatening world peace, uncertainty has never been more certain today. Coupled with the current pandemic and escalating cyber-attack threats, businesses the world over are facing volatile situations every day.

The recent flood that had devastated the Klang Valley in Malaysia during December 2021 caused an estimated RM6.1 billion in overall losses. The manufacturing sector accounted for RM900 million. There were also widespread damages to vehicles, business premises and homes. Any major incident that escalates to disaster could have a significant business impact on an organisation.

What is BCMS?

Business Continuity Management or BCMS is defined as the advanced planning and preparation of an organization to maintain business functions or quickly resume after a disaster has occurred. At its highest level, BCM is implemented to keep business operating at its maximum capability. It is also about making proactive and reactive plans to help organizations avoid crisis and disasters and quickly return to a state of normalcy or 'business as usual'.

BCMS emphasizes the importance of understanding an organization's needs and the necessity for establishing business continuity policies and objectives. The system will help establish operating processes, as well as capabilities and response structures for ensuring that the organization survive any disruption. BCMS mandates that its performance and effectiveness are constantly monitored and reviewed so that continuous improvements can be made both qualitatively and quantitatively.

The implementation of BCMS protects the following critical aspects against disasters and major disruptive events:

- **People** – Ensuring safety of employees
- **Key interested parties** – Encompasses shareholders, investors, customers, business partners, suppliers and even visitors
- **Key information and physical assets**
- **Critical business functions**

What is ISO 22301

ISO 22301:2019 *Security and resilience – Business continuity management systems – Requirements*, is the world's first International Standard for implementing and maintaining an effective business continuity plan. It enables an organization to achieve a more effective response and a quicker recovery, thereby reducing any impact on people, products and the organization's bottom line. This will lower costs and lessen any impact on business performance should a disaster or negative incident struck. ISO 22301 also ensures that

organisations with multiple sites can refer to a standardised and consistent approach in managing it.

ISO 22301 emphasizes the need for a well-defined incident response structure. This ensures that when incidents occur, responses are escalated in a timely manner and people are empowered to take the necessary actions as required. The standard is also aligned with several other internationally recognized management system standards, such as ISO 9001 (quality management) and ISO 14001 (environmental management). As such, **ISO 22301** can be integrated into an organization's existing management processes.

Attaining ISO 22301 certification demonstrates that an organization has met its stringent criteria and adopted international best practices. This will reassure clients, suppliers, regulators and other stakeholders that the organization has sound systems and processes in place for business continuity. In turn, this further improves business performance and organizational resilience. More importantly, the journey towards ISO 22301 certification will enhance an organisation's understanding of its business through analysis of critical issues and areas of vulnerability.

Key Components of ISO 22301

ISO 22301 covers the following main areas:

Organization - An organization needs to understand both its internal and external needs, as well as set clear boundaries for the scope of the management system. More specifically, this requires the organization to find out all the requirements of relevant interested parties, such as regulators, customers and employees. It must also understand the applicable legal and regulatory requirements. This will determine the scope of BCMS.

Leadership - ISO 22301 emphasises the need for strong leadership in BCM. Top management ensures sufficient resources, establishes policy and appoints people to implement and maintain the BCMS.

Planning - An organization must identify risks to the implementation of the management system and set clear objectives and criteria that can be used to measure its success.

Support - For business continuity to be successful, it is important for people with relevant knowledge, skills and experience to contribute and respond to incidents when they occur.

Operations - An organization must undertake business impact analysis to understand how its business is affected by disruption and how this changes over time. Steps to avoid or reduce the likelihood of incidents are developed alongside those to be taken when incidents occur. As it is impossible to completely predict and prevent all incidents, the approach of balancing risk reduction and planning for all eventualities is complementary. Essentially, it is about "hoping for the best but planning for the worst".

BCMS for all

The requirements specified in ISO 22301 BCMS are generic. As such, it is applicable to every organization, regardless of industry, size and type. The intention of the standards is to support organizations in effectively managing the impact of a disruption to its normal operation. While

business disruptions are inevitable, some are costly but recoverable, while others are cataclysmic and result in the complete loss of business, such as the recent major flood in Malaysia that hit businesses in Shah Alam.

BCMS is the tool used to manage a situation after a disruption. It helps guide an organization through the steps required to continue its operations. A company needs to understand the extent and type of impact it is willing to accept and develop a business continuity system sized correctly for its need.

ISCB is a department within **CyberSecurity Malaysia** that manages certification services that includes BCMS Certification Scheme based on the ISO 22301 international standard. Through BCMS, an organization can implement and maintain a response structure that will enable timely warning and communication to relevant interested parties.

How to get started?

To consider implementing BCMS and readying it for ISO 22301 certification, one must ascertain which parts within an entity are to be included in BCMS, taking into account location, size, nature and complexity. It is also important to identify which products and services to be included in the BCMS.

The management needs to perform a readiness assessment to know where it stands in relation to the standard's requirements and what level of resources are required to meet them. It must also undertake a business recovery exercise to identify what steps to take should there be a major disruption to its business.

BCMS Certification Steps

Audit by Certification Body (CB)

A 2-stage audit process will be carried out by CB to audit the organisation's BCMS documentation and evaluate the organisation's location and site-specific conditions. Stage 1 entails CB collecting and documenting information on the scope of the management system, processes and location(s) of the organisation; and related statutory and regulatory aspects and compliance.

Stage 2 audit evaluates the implementation, including effectiveness of the organisation's BCMS. 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.

Approval & Issuance of Certificate

All information and audit evidence gathered during audits will be analysed and CB will make a final decision after all non-conformities have been resolved. Once approved for certification, the organisation will be entitled to receive a copy of the BCMS certificate. A CB grants to the organisation, upon receipt of the certificate, a non-exclusive, non-transferable and revocable

license to use a certification mark applicable to the scope that has been certified in the manner described by the CB.

Critical Success Factors

There are several critical success factors in implementing BCMS. First and foremost, it demands strong commitment and support from top management. Implementing BCMS may involve costs for competency development, resource provision and business continuity strategy solutions. A strong engagement by the organisations' leaders is therefore vital in ensuring monetary support and critical resources for developing and maintaining a BCMS. Top management buy-in is also crucial to garner more participation and support across every business unit.

The second factor is competency and knowledge of a BCMS leader. He or she must not only be competent in the technical aspects of BCM but also in management systems. BCM focuses on conducting Business Impact Analysis and Risk Assessment, developing BC Plan and Procedures, identifying BC strategy, developing of recovery procedure as well as planning for BC testing. On the other hand, management system entails establishing a framework to ensure the BCM programme is executed effectively and maintained properly.

Last but not least, periodic testing and review is crucial for implementation success. Since BCM will only be brought into action when a disruption occurs, periodical testing and reviews of the system, its processes and rationale is necessary to ensure it remains effective and aligned to a changing organization.

Is Your Organization Well-Prepared?

Disasters can strike at any time, from large-scale natural catastrophes and acts of terror to technology-related accidents and environmental incidents. BCMS implementation involves clear methodical procedures which must be understood and supported at every level. It compels an organisation to regularly update its disaster response procedures and rehearsing its execution. Through BCMS, each and every member of an organisation needs to constantly ask what steps can be taken to prepare for the future. It forces everyone to be 'ready' for anything during these volatile times.

-END-

About Information Security Certification Body (ISCB)

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.***