Information Security Management System (ISMS) Implementation Services

What is an Information Security Management System (ISMS)

Organizations of all types and sizes:
a) collect, process, store, and transmit information;
b) recognize that information, and related processes, systems, networks and people are important assets for achieving organization objectives;
c) face a range of risks that may affect the functioning of assets; and
d) address their perceived risk exposure by implementing information security controls.
All information held and processed by an organization is subject to threats of attack, error, nature and is subject to vulnerabilities inherent in its use.

Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its objectives, and maintain and enhance its legal compliance and image. These coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are generally known as elements of information security management.

An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based upon a risk assessment and the organization's risk acceptance
levels designed to effectively treat and manage risks.

ISMS Implementation Practice

BESECURE ISMS Implementation Practice is a structured approach to develop an ISO 27001 compliant management system that includes following steps:

- Conduct an analysis of existing policies and procedures against industry benchmark standards
- Conduct a "structured" risk assessment using proprietary tools and methodologies.
- Define or assist in definition of security policies and procedures
- Build a security culture within the organization through education, training and awareness campaigns
- Monitor internal compliance to security policies and procedures through audits
- Coordinates the certification of defined ISMS according to international reference standard ISO27001
- Provide tools for supporting the ISMS including management of the documentation, management of the audit process, risk assessment etc.

We approach ISMS implementation as a time bound project with intermittent milestones, budgets and resources. A typical deployment is typically divided into four phases.

besecure
Managed E-Business Security™

Phase A – Plan

The Phase A of ISM Practice will addresses the PLAN requirements of the PLAN-DOCHECK- ACT cycle on which the standard is based . Indicative tasks include Project Initiation, Security Awareness Briefing, Information Security Forum establishment e.a

Phase B - Do,Check,Act

During Phase B we address the DO, CHECK and ACT requirements. Indicative tasks include ISMS Policy establishment, Risk Assessment, Risk Treatment and Selection of Controls, Statement of Applicability, Documented Procedures e.a.

Phase C - Certification

During Phase C the initial audit is conducted by the Certification Body. BESECURE supports you during the whole certification process. Following a successful audit the Certification Body issues a certificate of conformity.

Phase D - ISMS Support

The objective of this phase is to assist you during the first six - twelve months following certification. In addition to general support , there are four particular areas where additional support is likely to be required;

- Internal ISMS audits
- ISMS effectiveness measurements
- the second Management System Review
- first "surveillance" audit

This support may be extended, subject to further contractual arrangements, if you so wish.

Holistic Approach

BESECURE employees HISP & CISSP Certified Professionals to address specific security and compliance requirements of large enterprise customers. BESECURE implements an ISO/IEC 27002 specific security framework aligned with best practices of COBIT, COSO and ITIL. Through HISP approach BESECURE maps regulations such as UK Data Protection Act, EU Directive on Privacy, HIPAA Security, FFIEC, GLB Act, FISMA (NIST 800-53/FIPS 200), Sarbanes-Oxley Act (Security), FACT Act, PCI Data Security (Visa CISP), California SB-1386, Canadian Bill C-198, OSFI, PIPEDA, PIPA, PHIPA that organizations needs to comply with, to the 27001 framework.

About BESECURE

BESECURE, is a leading provider of Governance, Risk & Compliance (GRC) services, Cyber Security solutions, Managed Security services, Certification Training and Awareness programs, ISO 27001 and ISO 9001 certified, trusted by global organizations across telecommunication, financial services, energy industries and other medium - large enterprises to safeguard their information assets including financial information, intellectual property, trade secrets, Personally Identifiable Information (PII) or information entrusted to them by customers or third parties. For more information, please visit http://www.besecuregroup.com.