ISO 27001 Security Assesment Service

Information Security Management System based on ISO 27001

Corporate information and intellectual property are important assets that every organization must protect from unauthorized users. Developing and maintaining a sound security strategy can help an organization to manage its risks associated with network intrusion, data theft, system misuses, privilege abuse, tampering, fraud, or service interruption.

Typically, organizations tend to implement and audit security or privacy program requirements in individual silos. This approach is costly, ineffective, time-consuming and lacks continuity. An Information Security Management System (ISMS) serves as an overlay for multiple data protection regulations such as Sarbanes-Oxley, EU Data Privacy Directive, PCI and any other security or compliance initiatives.

BESECURE Security Assessment Services will assist you in identifying the combination of technical, resource, and process controls that your company can use to manage security risks. Conducted by a BESECURE security consultant, these in-depth assessments identify the strengths and weaknesses of your current security posture as well as vulnerabilities to security threats. BESECURE consultant works with you to determine the appropriate mix of security assessments to address your business needs.

Benefits of adapting an ISMS based on International Standards

- Provides a common framework enabling you to develop, implement, and effectively measure information security management practices.
- Ensures the right people, processes, procedures and technologies are in place to protect information assets and demonstrate that applicable laws and regulations are observed.
- Provides a competitive edge by meeting contractual requirements and demonstrating to your customers that the security of their information is paramount.
- Independently verifies that your risks are properly identified, assessed and managed, while formalizing information security processes, procedures and documentation.
- The regular assessment process helps you continually monitor and improve your ISMS.

ISO 27001 Security Assessment Service benefits

- Realistic view of current corporate security procedures and controls.
- Highlights strengths of weaknesses of current information security framework
- Provides an in-depth analysis of your current security posture
- Helps you to understand how your security measures compare to industry standards
- Enables more informed decisions, allowing you to better manage your company's exposure to threats associated with doing business over the Internet
- Provides recommendations for reducing exposure to currently identified security risks
- Cost effective way of preparing for ISO 27001 implementation.

besecure
Managed E-Business Security™

BESECURE Service Approach

ISO 27001 Security Assessment Service is a consultancy service for those organizations who want to measure their current information security framework against the ISO 27001 standard. It is relevant to organizations who are either embarking on a formal certification strategy or who want to gauge current information security controls and practices against a recognized standard.

Typical service activities include:

- Analysis of overall security posture and procedures, including policy analysis, process and procedure review, and staff training and awareness
- Review of physical security controls, including access controls, system location, security monitoring, and site security and layout
- Review of internal and network boundary security, including dial-up access control, intrusion detection, existence of known vulnerabilities, network configuration issues, and traffic-related issues
- Review of firewall and defenses, including rule configuration, monitoring for alarms, virus protection, and real-time intrusion detection
- Review of application and database security, including hardening, password and user authentication, data integrity, backup procedures, and software development
- Review of client security, including desktop security, PDA and mobile management, access to the Internet, remote working practices, permissions, and virus protection
- Identification of security deficiencies based on a combination of interviews with key IT and security staff and audits, which may include assessment of compliance with the organization's security policies and procedures, configuration audit, and onsite review of physical security.

A report will be provided within ten (10) business days following the on-site visit. BESECURE produces an executive summary document and the gap analysis report. The executive summary describes the following in a non-technical fashion suitable for senior management:

- Purpose of the engagement
- Project scope and approach
- Major steps that were taken to perform the engagement
- Positive security aspects that were identified
- Primary types of gaps encountered and their business impact
- General recommendations - both policy and technical

The gap analysis report contains a more technical description of the project's activities, findings and recommendations. The detailed gap findings are categorized and structured to facilitate immediate corrective action by the responsible staff

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.