Certification of Information Security Management System based on ISO/IEC 27001:2013

INFORMATION SECURITY MANAGEMENT SYSTEM (ISO 27001:2013)

Due to increased dependability upon information and information systems, both information & its associated infrastructure is a vital asset for most businesses in this age of globalization. For some businesses it is a matter of survival while others also have to have some mechanism of information security to meet the expectations of their customers, saving image of the business and other regulatory requirements.

Information Security (IS)

Information security is based on three core principles, confidenciality, integrity & availability (CIA). Information security deals every risk associated with CIA of information. ISO 27001:2013 provides 14 control areas to achieve CIA of the critical information. These are;

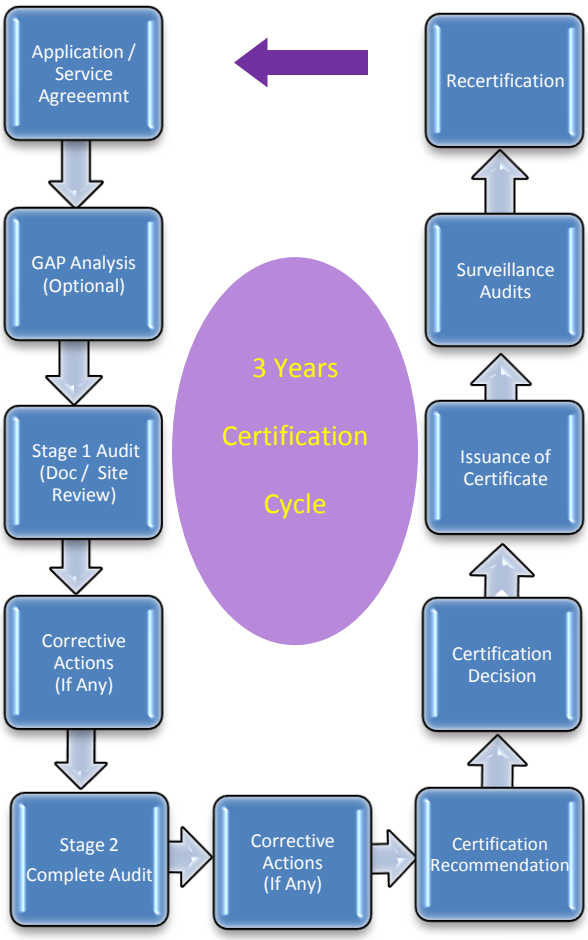
- Information Security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations Security
- Communication Security
- Systems acquisition, development and maintenance
- Supplier Relationship
- Information security incident management
- Information security aspects of business continuity management
- Compliance

ISMS uses 35 control objectives and 114 specific controls to achive the goal of information security.

BENEFITS OF ISO 27001:2013

- Internationally acceptable standard for IS
- Applicable to all organizations irrespective of size
- Increase the good name and reputation of company
- Increase the credibility of the organization in the eyes of customers and stake holders
- Increase the ability to minimize financial loss
- Identify critical assets and better planing to save them from threats
- Increased physical and environmental security of the business
- Ensure timely IS incident reporting
- Ensure business continuity even in natural disaster like earthquake, flood, storm etc. as well as in special circumstances such as hacking, data loss, power failure and terrorism

CERTIFICATION PROCESS FOR ISO 27001:2013



INFORMATION SECURITY MANAGEMENT SYSTEM

Web Site: www.cesp.com.pk
E-mail: info@cesp.com.pk

Certification of Information Security Management System based on ISO/IEC 27001:2013

CERTIFICATION PROCESS (Contd.)

1. **Application** is filled by the client and Certification **Service Agreement** is finalized with the client.
2. **GAP Analysis**: An optional analysis may be performed if agreed by the client in the Service Agreement.
3. **Stage 1 audit (Document Review)** is conducted to assess the organization's readiness for the stage 2 audit. Auditor(s) assesses documented system with the requirements of the ISO 27001:2013 standard. The document review is normally conducted on-site. Audit report is provided at the end of Stage 1 audit identifying audit findings/observed non conformances (if any). The client is required to take corrective actions so that stage 2 audit can be planned.
4. **Stage-2 Audit:** This second stage is conducted to determine the extent of implementation and effectiveness of the information security management system. The auditor(s) will execute an extensive review of records and interview a significant portion of the employees – at all levels of the organization. Audit findings are provided at the end of Stage 2 audit identifying observations, non conformances and opportunities for improvement (if any). The client is required to close the non conformances within agreed time frame. After closing of non conformances the independent technical review of audit is conducted and certificate is issued to the client.
5. **Surveillance Audits** are conducted as per defined frequency as specified in Service Agreement (minimum annually), to observe the ongoing assessment for maintenance of certification requirements and continual improvement.

Recertification Audit is conducted before expiry of certification as per revised Service Agreement. Surveillance visits will then continue, as before, on a 3-year cycle.

Why CeSP

Certification Services Pakistan is established with a view to develop and excel as internationally recognized Pakistan's leading Conformity Assessment Body to assess companies in all areas of manufacturing and services. Based on impartiality, confidentiality, responsibility competence, openness and customer focus as guiding principles, our success depends on honesty, courtesy and professionalism leading towards the consistent delivery of high quality third party accredited and non-accredited certification, inspection and training services. Under the guidance of experienced lead auditors and technical experts, having wide expertise in system implementation and assessment, CeSP strives to provide the best certification services in Pakistan.

Related Services

- GAP Analysis

Certifications

- EMS ISO 14001:2015
- OH&SMS 45001:2018
- QMS ISO 9001:2015
- FSMS ISO 22000:2018

Trainings Courses

- IRCA-UK registered Lead Auditor
- Internal Auditing
- Awareness & Introduction to Certification Standards
- Lab Management as per requirements of ISO/IEC 17025:2017
- Measurement Uncertainty, Method Validation, Quality Control of Testing & Calibration Labs as per ISO/IEC 17025:2017

CeSP
Certification Services Pakistan (Pvt) Ltd.
Certifications, Trainings, Inspections

Web Site: www.cesp.com.pk
E-mail: info@cesp.com.pk

INFORMATION SECURITY MANAGEMENT SYSTEM