Information Security Management System

ISO 27001

Information Security: Ensuring confidentiality, integrity, and availability of information assets and supporting IT Infrastructure – Network, Operating System, Application, and Database.

Need for ISMS:

- December 2013: Target reported compromise of approximately 70 million customers' payment card information from their computer system
- June 2014: Home Depot reported compromise of approximately 53 million customers' information from their computer systems
- August 2014: Apple's iCloud was hacked; about 500 celebrities' private pictures were stolen
- May 2015: Care First Blue Cross Blue Shield reported breach of 1.1 million subscribers' personal information

These are not histories. Some of these events are happening right now!

The US economy is losing about a trillion dollars every year due to cyber security incidents.

Analysis of all the high profile security breaches revealed lack of senior management involvement in the ISMS is the root cause of these problems. In this context, ISO IEC 27001 seems more relevant than ever because it provides a management system framework.

ISO/IEC 27000

- Is a standard for ISMS. The standard has two parts:
- ISO/IEC 27001:2013 provides specifications for ISMS
- ISO/IEC 27002: 2013 provides code of practice
- ISO/IEC 27001:2013 Annex A provides 114 controls
- Aligned to ISO 9001 and ISO 14000
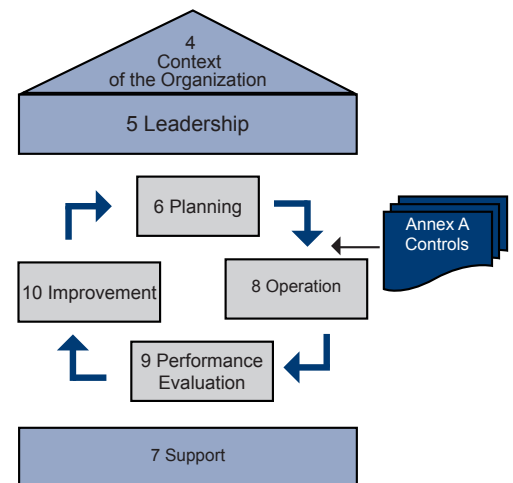- Adopts a systematic approach to ISMS

Why ISO/IEC 27001?

- Establishes general controls required for SOX, SSAE 16 type audits
- Globally recognized as a standard for ISMS
- Applicable to all organizations regardless of size, type or nature
- Continual assessment helps to keep security controls effective

Scope of ISO/IEC 27001
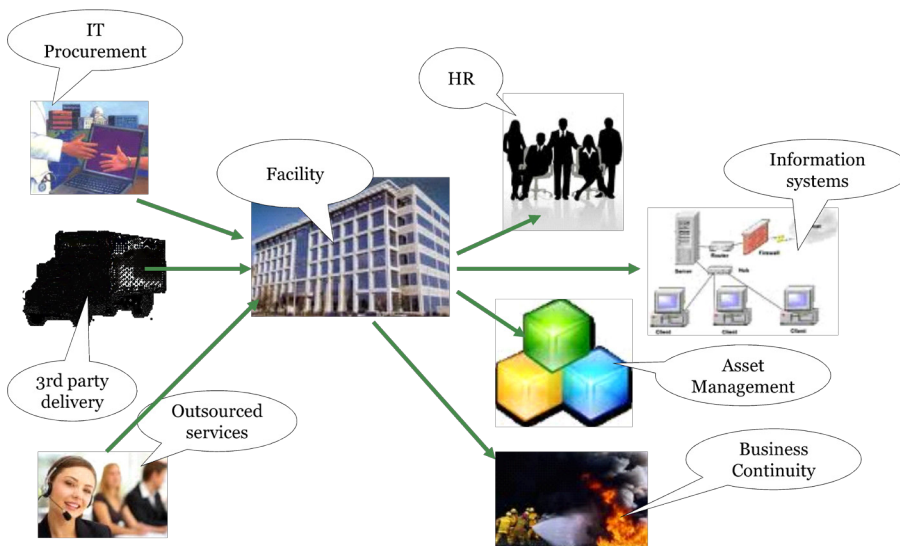
ISO/IEC 27001:2013 Framework

Training

ISO 27001 Awareness: DQS Inc. will deliver a two-hour web seminar. The objective of this session is to create basic awareness about ISO 27001 standard.

ISO 27001 Training: DQS Inc. will conduct this one-day training on-site for process owners and practitioners. Objective of this training is to create an in-depth understanding of ISO 27001 and risk assessment.

Risk Assessment: Organization should conduct comprehensive risk assessment immediately after the ISO 27001 workshop. This result will be reviewed by DQS Inc. in the following phase.

Initial Assessment

DQS Inc. will perform a Preliminary Evaluation (Gap assessment) of the "as-is" system against the requirements of ISO 27001. This stage would provide feedback to your team on their readiness and would likely increase the chances of a successful Registration Audit.

Readiness Review

DQS Inc. will review the documented procedures, policies and plans to verify compliance to the requirements with ISO 27001. This stage would provide feedback to your team on the adequacy of your documented system. Dates of the **Stage 2** audit will be determined based on the outcome of this audit. This stage is also known as **Stage 1** assessment.

Registration Audit

DQS Inc. will conduct a comprehensive Registration Assessment of your company according to the requirements of the ISO 27001 Standard. A successful Registration Assessment will lead to the issuance of an Accredited Certificate with **three-year** validity. An audit will be conducted using interviews, document reviews and observations of ISMS tools.

Continuous Assessments (sometimes referred to as Surveillance Assessments or Audits) are required to maintain your Registered Firm status. DQS Inc. will offer you the choice of semi-annual or annual Continuous Assessment visits. Whichever you choose, these carefully planned "spot checks" of your Quality System ensure continuing compliance with the ISO Standard. The lead assessor at the end of the Registration Assessment makes the formal decision for the number of Continuous Assessment days.

Quick Facts about DQS Inc.

· Formed with partnership between The Underwriters Laboratories Inc. (UL) and DQS (German Registrar of Management Systems,) which was founded by DGQ (German Society of Quality) and DIN (German Institute of standardization).

· Global presence: 80 offices in 60 countries

· Best in class auditors: over 2,500 competent auditors worldwide

· Large customer base: over 59,000 certifications

Evaluation and certificate issue

· Evaluation of system assessment results and certification decision by DQS Inc.

· Following a positive decision, issuance of certificate with a validity of three years

For more information, please call: 800-285-4476 or email: Info.IT@dqsus.com

DQS Inc.