CONSULTING

Compliance Services

Gap Analysis

The gap analysis is a fast track assessment to establish understanding on an organization's current capabilities. The purpose of this step is to evaluate the current capabilities of organizations against relevant areas of relevant ISO standard(s), so that missing components and/or weaknesses can be identified. This exercise is designed to give Senior Management a better indication of where their organization stands in terms of the relevant standard, and roughly what effort is required to achieve compliance.

I(TS)^2 provides Gap Analysis for following standards:

- ISO/IEC 20000 - Service Delivery Management
- ISO 27001 - Information Security Management System
- ISO 22301 - Business Continuity

Internal Audit

Internal auditing is an independent, objective assurance and consulting activity designed to evaluate compliance, improve an organization's governance, risk management, and management controls. This service involves on-site independent assessment, and fact finding to generate a report that provides key insight and recommendations based on analyses and assessments of data and business processes.

I(TS)^2 provides Internal Audits for the following standards:

- ISO/IEC 20000 - Service Delivery Management
- ISO 27001 - Information Security Management System
- ISO 22301 - Business Continuity

CONSULTING

Compliance Services

ISO Establishment, Implementation & Certification

This service involves facilitating corporations to design, establish, implement, manage, and maintain the following management systems:

- ISO/IEC 20000 - Service Delivery Management
- ISO 27001 - Information Security Management System
- ISO 22301 - Business Continuity

We ensure that all the requirements for certification are met and facilitate the organization to achieve the desired management system certification.

Physical Security Review

The objective of this activity is to assess and evaluate an organization's physical security controls, identify any shortcomings, and to provide recommendations. Typically, it is comprised of a review of Physical Access Controls, Vehicle Access Controls, Security Guards Controls, Environmental Controls, Life Safety Controls, Equipment Controls, and other relevant security concerns.

CONSULTING

Information Security Governance

Risk Assessment & Management

This Service is comprised of establishing a tailored risk methodology to assess, evaluate, modify, and mitigate risks for an organization.

During risk assessment, critical organizational services are identified, related information security threats and vulnerabilities are determined, and then all risks are evaluated. A mitigation plan is established to address the information security risks which are not acceptable. At the end of engagement, a comprehensive report will be created to summarize all risks, their values, mitigation plans, risk owners and due dates.

Information Security Policies & Procedures

I(TS)² helps organizations develop policies and procedures that set out a framework of governance and accountability for information security management commitment across an organization. Listed below are some typical information security policies:

- Acceptable Use Policy
- Information Security Policy
- Organizing Information Security Policy
- Human Resources Security Policy
- Asset Management Policy
- Cryptographic Policy
- Physical and Environmental Security Policy

CONSULTING

Information Security Governance

Information Security Policies & Procedures

- Operational Security Policy
- Communications Security Policy
- Access Control Security Policy
- System Acquisition Development and Maintenance Policy
- Supplier Management Policy
- Information security incident management Policy
- Business Continuity Management Policy
- Compliance Policy
- Risk Management Policy

Procedures describe how each policy will be put into action in the organization, and gives a systematic guide on how to fulfil a specific task or activity. Listed below are some information security procedures:

- Risk Assessment Procedure
- Change Management Procedure
- User Access Management Procedure
- Backup and Restoration Procedure
- Management Review Procedure
- System Acquisition Development and Maintenance Procedure
- Personnel Security Procedure
- Corrective and Preventive Action Procedure
- Document and Record Control Procedure
- Internal Audit Procedure
- Information Security Incident Handling Procedure

CONSULTING

Information Security Governance

Information Security Organization

This service aims at addressing:

- Establishing organizational structure and hierarchy in an organization
- Establishing roles and responsibilities and explicit assignments for the employees
- Identifying key roles and responsibilities for main roles in security program such as CIO, Security Manager, Application developer, database administration, Internal audit, Security Unit,
end users, etc.

Technical Security Assesment

Vulnerability Assessment

The objective of a vulnerability assessment service is to identify and assess all present vulnerabilities in the IT network or infrastructure and report it to the customer. The result is a report, which produces a prioritized list of vulnerabilities & suggests remediation.

CONSULTING

Technical Security Assesment

External Penetration Testing

External penetration testing is an offensive security analysis of an IT infrastructure's defenses against attacks from the Internet. External penetration testing involves mimicking the actions of an external hacker, with the purpose of simulating a cyber-attack or gaining access to confidential information through the Internet. This type of testing checks for vulnerabilities in the IT infrastructure's external perimeter that may lead to a breach of confidentiality, integrity and accessibility of data.

Internal Penetration Testing

Internal penetration testing is an analysis of IT infrastructure security within a corporate network. Internal penetration testing involves simulation of actions of a malicious employee. This type of testing checks for vulnerabilities in the internal network that may lead to a breach of confidentiality, integrity and accessibility of data.

Business Application Penetration Testing

Our application Penetration testing of business applications is an analysis of the security of various applications:

- Web applications
- Mobile applications (Android, iOS, Blackberry and Windows Phone operating systems)
- Third-party product solutions (ERP, CRM, etc.).

Penetration testing of business applications involves mimicking the actions of an attacker, with the purpose of obtaining unauthorized access to application data or functionality. The tests are conducted using the following models:

- Black Box – a model in which only the address or location of the application is known
- Gray Box – a model in which the address or the location of an application is known and certain access to the functionality of the application is available.

CONSULTING

Technical Security Assesment

Source Code Review

This service enables review of application source code and identification of vulnerabilities in the source code of an application. We analyze the code for different types of applications (web, mobile, corporate).

Security Analysis Of Industrial Systems (Apcs, Scada)

The purpose of the security analysis of industrial systems is to provide an objective and independent assessment of the current level of protection of an industrial system. The scope of this process includes verification of the network demarcation, security of applications, the ability to upgrade the operator's access rights, security of operating systems, the safety of controllers and other system components.

Forensic Investigations

The Forensic Investigation service examines digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing, and presenting facts and opinions about the digital information incident.

CONSULTING

Information Security Awareness

Information Security Need Assessment

Need Assessment service provide a comprehensive analysis of the current state and effectiveness of organizations present security awareness program (if any). Centered on interviews with leadership, surveys and testing of your employees, the service identifies gaps and areas for improvement for security awareness.

Awareness Campaigns

This service involves establishing and implementing a full awareness Campaigns for an organization. Depending on the requirement of organization this service can comprise of services, such as:

- Content /messages development,
- Workshops (Senior Management, IT department, General users)
- Banners/ brochures/posters design,
- Booklet
- Video, etc.

It's all about TRUST

CONSULTING

Information Security Awareness

Learning Management Systems

Our information security awareness Learning Management system is designed to strengthen the first line of information security defense within your organization: Your people. Our courses enable participants to understand and know how to implement the best information security practices. It provides following features:

- The System will be configurable, to meets customer's requirements, such as customer's logo, font, color, picture, adding/modifying/deleting content.
- Authentication capabilities
- Quiz/Exam
- Conforms to industry standards and laws (ISO 27001 & PCI-DSS).
- Issuing and printing Certificate (Delivered by Email)
- Report (per users and departments)
- Short videos at the start of each topic (English with Arabic subtitles)
- Audio narration

Course Characteristics

- Modular and customizable content
- All subjects can be deployed individually, per group of topics (module) or per course
- Available in English and/or Arabic languages

CONSULTING

Information Security Awareness

Promotional Items

This service involves developing a unique set of security awareness products, with catchy images and clever slogans, which will attract the attention of individuals and assist in establishing a security positive environment within the organization, where staff will act and think instinctively in a way which promotes good information security practice. All of the products can be delivered in English and Arabic.

The focus on this stage is to develop not only specific contents for the materials but also high quality promotional items that which would be based on the customer's organization theme. These designs of the contents would reflect organizations brand and image, and would be made to fit not only content but the context also.

Some examples of promotional items are:

- Cups/ pens/ USB with messages
- Posters
- Booklets