ITG

Information Security Management System Manual

This manual describes the ITG Information Security Management system and must be followed closely in order to ensure compliance with the ISO 27001:2005 Standard

Table of Contents

Introduction

This manual documents the ITG Information Security Management System (ISMS), which has been developed to ensure a company-wide process approach for the establishment, implementation, operation, review, maintenance and improvement of organizational information security management. References to related documents and guidance are provided in each section of the manual. The ISMS is operated and maintained by the company Infrastructure Management Review Board.

Scope

The scope of the program is defined as “Protection of company and customer information in the provision of Information Technology equipment, software and services to public and private sector organizations.”

Establishing and managing the ISMS

ITG Executive Management has produced and implemented an approved Information Security Policy that defines the scope and boundaries of the company’s ISMS. The policy defines the scope of the organizational ISMS and defines ISMS policy in terms of the business, its location, assets and technology. This policy provides a general framework for setting information security objectives and establishes an overall sense of direction and principals for action with regard to information security. The company takes its lead from the ISO 27001:2005 standard in further defining ISM policy.

The Information Security Policy aligns with the company’s strategic risk management context in which the establishment and maintenance of the ISMS will take place, and provides for a separate document that establishes criteria against which risk will be evaluated.

Ref: ITG Doc# 959 – ITG Information Security Management System Manual
Ref: ITG Doc #907 – ITG Information Security Policy – Executive Management
Ref: ITG Doc #939 – ITG IT Security Configuration Item Inventory/Registry & Risk Analysis Methodology Document
Ref: ITG Doc #949 – Risk Treatment Scoring and Plan
Ref: ISO 27001:2005 Standard, Section 4.2.1 a) through Section 4.2.1 b)

Risk management approach

The company’s overall risk management approach is defined in the ITG Risk Management Objectives and the ITG Risk Management Plan, which includes specific requirements for information security management.

Ref: ITG Doc #495 – Risk Management Objectives
Ref: ITG Doc # 494 – Risk Management Plan

The ITG IT Security Configuration Item Inventory/Registry & Risk Analysis Methodology document describes the established company risk assessment methodology, the criteria for accepting risks and the acceptable levels of risk. This methodology is employed to ensure that risk assessments produce comparable and reproducible results.

Ref: ITG Doc #939 – ITG IT Security Configuration Item Inventory/Registry & Risk Analysis Methodology
Ref: ISO 27001:2005 Standard, Section 4.2.1 c)

Risk identification and assessment

The assets within the scope of the ITG ISMS are identified in the introduction to the ITG Security Configuration Item Inventory/Registry. Ownership and security responsibilities for the various types of assets within the scope of the ISMS are defined in the ITG Security Policy “Responsibility” section. Ownership and security responsibilities are assigned by executive management to those individuals within the company whose experience, training, job functions and authority levels best fit the responsibility of the assignment.

Ref: ITG Doc # 907 – ITG Information Security Policy
Ref: ITG Doc # 939 – ITG IT Security Configuration Item Inventory/Registry & Risk Analysis Methodology
Ref: ISO 27001:2005 Standard, Section 4.2.1 d)

Parties assigned ownership and security responsibilities for assets within the scope of the ISMS perform Risk Analysis in relation to the assets for which they have been assigned responsibility. The methodology utilized to assess risk and assign classification and security measures is detailed in the ITG IT Security Configuration Item Inventory/Registry & Risk Analysis Methodology document. The methodology provides for the identification of threats, vulnerabilities that might be exploited by the threats and the impacts that losses of confidentiality, integrity and availability may have on specific assets.

Ref: ITG Doc #939 – ITG IT Security Configuration Item Inventory/Registry & Risk Analysis Methodology
Ref: ITG Doc #907 – ITG Information Security Policy
Ref: ISO 27001:2005 Standard, Section 4.2.1 d)

Risk Analysis

Initial assessment of business impacts, likelihood of security failures and risk level are performed by the parties assigned as responsible for assets within the scope of the ISMS. Through the CENTRE Change Management facility, this assessment is submitted to and reviewed by the company Infrastructure Management Review Board (MRB), which is ultimately responsible for overall IT Security.

Ref: ITG Doc # 521 – Procedure: Risk Management, ITG QP-10
Ref: CENTRE Change Management Records
Ref: ISO 27001:2005 Standard, Section 4.2.1 e)

Upon review of a risk assessment, the Infrastructure MRB makes a determination as to whether the identified risk is acceptable, or requires treatment using the criteria for accepting risks as defined by company executive management.

Ref: ITG Doc #939 – ITG IT Security Configuration Item Inventory/Registry & Risk Analysis Methodology
Ref: ITG Doc #949 – Risk Treatment Scoring and Plan (Scoring section)
Ref: ISO 27001:2005 Standard, Section 4.2.1 e)

Risk Treatment

The Infrastructure MRB identifies and evaluates options for treatment of identified risks, including knowingly and objectively accepting the risk, avoiding the risk, transferring the risk to another party, or applying appropriate controls to eliminate or mitigate the risk locally.

Ref: Appendix A, this document
Ref: ITG Doc #939 – ITG IT Security Configuration Item Inventory/Registry & Risk Analysis Methodology
Ref: ITG Doc #949 – Risk Treatment Scoring and Plan (Plan section)
Ref: Infrastructure MRB Meeting minutes
Ref: ISO 27001:2005 Standard, Section 4.2.1 f)

When the Infrastructure MRB determines that a risk is acceptable providing appropriate mitigating controls are applied, control objectives and controls defined in Annex A of the ISO 27001:2005 standard are considered and selected as applicable, along with any special controls that may need to be applied for risks of a unique or particularly unusual nature. ITG has identified additional control objectives and controls necessary for the purposes of its business. These items have been added to the standard list included in Annex A of the standard. The entire list is incorporated as Annex A to this manual.

Ref: Annex A to this ISMS manual
Ref: ITG Doc #949 – Risk Treatment Scoring and Plan
Ref: ISO 27001:2005 Standard, Section 4.2.1 g)

Acceptance of Residual Risk

Approval authority for proposed residual risks resides with the Infrastructure MRB, which includes within its membership highest-level executive management and representatives at appropriate management levels from all areas of the company, as well as the named IT security team.

Ref: ITG Doc #538 – Charter: Infrastructure Management Review Board
Ref: ITG Doc #937 – Procedure: IT Security Management, ITG QP-22
Ref: ITG Doc #949 – Risk Treatment Scoring and Plan
Ref: Infrastructure MRB meeting minutes
Ref: CENTRE Change Request Records
Ref: ISO 27001:2005 Standard, Section 4.2.1 h)

Management authorization to implement and operate the ISMS

Management commitment to IT Security and Information Security Management is strong throughout the company. Authorization to implement and operate the company ISMS comes directly from the President of ITG, supported fully by all other executive and mid-level management. Executive management actively participates on the Infrastructure MRB and in design, application and continuing maintenance of the ISMS.

Ref: Infrastructure MRB meeting minutes
Ref: Executive management ownership and maintenance of many ISMS documents
Ref: ISO 27001:2005 Standard, Section 4.2.1 i)

Cryptographic Controls

ITG's policy is to use cryptographic controls where needed to provide for the confidentiality, integrity, and availability of information in accordance with regulatory, statutory, and contractual requirements.

Ref: Annex A: Section 12.3.1 'Policy on the use of cryptographic controls'.

Access Control

It is the policy of ITG to manage access to systems and information based upon business and security requirements, this, in accordance with our 'on-boarding' workflow, access requests, and user needs, facilitates authorized access to systems and information.

As needed or as scheduled, management has the responsibility of reviewing and ensuring for the adequacy of subordinate access to systems, applications, and information.

Ref: Annex A: Section 11.1.1 'Access control policy'.

Statement of Applicability

In compliance with the ISO 27001:2005 standard for information security, ITG has prepared a Statement of Applicability that includes:

- the control objectives and controls selected for risk treatment and the reasons for their selection
- the control objectives and controls currently implemented
- the exclusion of any control objectives and controls in Annex A and the justification for their exclusion.
- NOTE: The statement of Applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross-check that no controls have been inadvertently omitted.

ITG's Statement of Applicability is maintained in a separate DCS document to facilitate ease of document maintenance.

Ref: DCS #958 – ISO 27001:2005 Statement of Applicability
Ref: ISO 27001:2005 Standard, Section 4.2.1 j)

Implementation and operation of the ISMS

ITG has formulated a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information Security Risks, and has implemented this plan in order to achieve the identified control objectives. This risk treatment plan is owned and operated by the Infrastructure MRB. Since company executive management maintains active membership in the Infrastructure MRB, funding considerations and approval thereof, as well as risk treatment roles and responsibilities, are approved in the normal process of board review and improvement activities.

The Infrastructure MRB performs a quarterly review of security-related events and compares the results to measurements from previous quarters in order to assess the effectiveness of selected security controls or groups of controls. Any negative increase in security-related events, or identification of new threats or vulnerabilities is answered by appropriate MRB action to reassess applicable existing controls or implement new controls to eliminate or mitigate risk to the integrity of company information security. The Infrastructure MRB Information Security Team is dedicated to the daily operation and maintenance of the company ISMS.

Ref: ITG Doc # 538 – Charter, Infrastructure Management Review Board
Ref: ITG Doc #949 – Risk Treatment Scoring and Plan
Ref: Infrastructure MRB meeting minutes
Ref: ISO 27001:2005 Standard, Section 4.2.2 a) through 4.2.2 d)

Training and awareness

Training and awareness are critical for the success of any security management system. Only personnel who have been properly introduced to security requirements and the processes necessary to carry them out can be truly effective in security management. ITG has rolled out an employee information security training course to ensure all employees are made aware of company IS requirements. This course is mandatory for all employees. Supplemental training from external sources, i.e. government-sponsored Security Officer training, etc., is accomplished as necessary to achieve the company's IS goals.

Ref: ITG Doc #944 – IS101 Course outline
Ref: ITG Doc #948 – IS101 Course Presentation
Ref: Informational e-mails from executive management to Staff
Ref: Company Security Officer external training
Ref: HR employee training records
Ref: ISO 27001:2005 Standard, Section 4.2.2 e)

As mentioned previously in this manual, the ITG Infrastructure Management Review Board is responsible for managing the operation of the company ISMS, including the assignment and management of resources required to operate and improve the system. Training and awareness activity is accomplished by the Training and Certifications MRB, working in cooperation with the Infrastructure MRB.

Ref: ISO 27001:2005 Standard, Section 4.2.2 f) and 4.2.2 g)

--- End of Excerpt ---

This document contains sensitive, proprietary and privileged information which may not be disclosed, copied, distributed or used in any manner by other parties without the expressed written consent of Integration Technologies Group, Inc.