ISO/TC 247
ISO/TC 247 - Fraud countermeasures and controls
Email of secretary: mikeo@naspo.info
Secretariat: ANSI (USA)

ISO PWD 16125 Security Management System - Fraud Counter Measures and Controls

Document type: Working draft

Date of document: 2011-06-29

Expected action: INFO

Background:

Committee URL: http://isotc.iso.org/livelink/livelink/open/tc247

ISO TC 247/WG1 N55

Date: 2011-06-18

ISO/PWD 16125

ISO TC 247/SC /WG 1

Secretariat: ANSI

Security management system — Fraud countermeasures and controls

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage:
Document language: E

C:\Users\Michael\Documents\ISO TC 247\ISO_PWD_16125_(E).doc STD Version 2.1c2

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 16125 was prepared by Technical Committee ISO/TC 247, *Fraud countermeasures and controls*, Subcommittee SC , .

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

Introduction

Organizations of all types and sizes have an interest to minimize risks to their tangible and intangible assets by protecting them from harmful and fraudulent acts. These fraudulent acts include intended acts of individuals or unitended acts facilitating a fraudulent act by others. Protecting tangible and intangible assets includes avoidance of the consequential damage of falling into unauthorized hands and minds because organizations themselves and others rely on them and in some cases are critically dependent upon them. Personally identifiable information that can be used to perpetrate identity theft and special materials that are critical to the unique performance and proprietary characteristics of a product are examples of sensitive information and physical assets that must be protected. To protect sensitive assets and information and avoid consequential damage, organizations should be able to resist all common forms of threat and harmful acts to a greater or lesser extent. Organizations should also be able to resist forms of threat and harmful acts that are unique to the organization because of geographical location, jurisdiction, sector, industry, nature of the product, service or end use. Fraud can also happen outside the direct control of an organization by counterfeiting or diverting its products. The totality of exposure to common and unique threats represents the sensitive asset and information threat profile of an organization. To effectively resist all of the threats, in a profile, requires the use of special security management expertise, management activities, processes, policies, procedures, infrastructure, systems and culture. To this end, this International Standard specifies normative requirements for the performance of general management and security management functions and processes that together enable an organization to plan operate, maintain and improve a comprehensive security management system.

Organizations can use this management system standard to develop and implement a strategy appropriate to their threat profile and business requirements.

An organization that must impose upon itself, or a relying party that must demand threat resistance can use this standard to specify requirements for threat resistance. An organization, stakeholder, business partner, relying party or employee can then assure itself by assessing conformity with the specified security management requirements and associated threat resistance measures.

The relationship of security, safety and quality in this standard is an important concept to be recognized.

A security management system is not a quality management system. A quality management system standard attempts to define and implement the processes necessary to consistently produce a product to specification.

A security management system standard is not a safety standard as it relates to the attributes of a safe product for consumption or use. A safety standard should define those practices and processes that will render a product safe for consumption or use.

The intent of this security management system standard to provide a framework for an organization to manage the risks of fraudulent acts to support the delivery of quality and safe products and services. This difference is significant in the intent of a security management standard versus a quality or safety management system standard.

This International Standard is designed so that it can be integrated with quality, safety, environmental, information security, supply chain security, risk, and other management systems within an organization. A suitably designed management system can thus satisfy the requirements of all these standards. Organizations that have adopted an ISO approach to management systems (e.g., according to ISO 9001:2008, ISO 14001:2004, ISO/IEC 27001:2005, or ISO 28000:2007) may be able to use their existing management system as a foundation for the security assurance management system as prescribed in this International Standard.

This International Standard addresses risks associated with individuals and organizations seeking to disrupt normal operations or to derive unauthorized benefit through dishonest acts.

Managing the risks of fraudulent acts is essential to assuring the quality of an organization's products. This International Standard enables an organization to develop the necessary fraud countermeasures and controls to protect itself against internal and external fraudulent acts. It complements the other ISO security risk management standards for information and supply chain security. In order to develop a robust strategy the organization should establish, implement and maintain a management system addressing issues related to managing risks identified in its risk assessment to minimize the likelihood and consequences of fraudulent acts, as well as other intentional acts that may cause harm to the organization and its assets, both tangible and intangible.

This International Standard provides a holistic approach to fraud related security issues by recognizing that fraud is any act perpetrated by individuals or organizations intenteded to cause financial, social or physical harm. It provides a framework for the organization to protect itself against fraudulent acts to support normal operations. This International Standard is applicable to both the public and private sectors. This SMSS is intended to be compatible with and supportive of other ISO security related standards,

This management system Standard (referred to as the "Standard") has applicability to all sizes and types of organizations in the private, not-for-profit, and public sectors. The adoption of a security assurance management system should be a strategic decision of an organization. The design and implementation of an organization's security assurance management system is influenced by:

a) the internal and external context in which it operates,

b) its varying needs and that of its stakeholders,

c) its objectives,

d) the products and services it provides,

e) the sensitivity of its assets and information,

f) its processes and industry sector, and

g) its size and organizational structure.

The management system approach encourages organizations to analyze organizational and stakeholder requirements and define processes that contribute to a robust security assurance strategy. A management system can provide the framework for continual improvement to increase the probability of enhancing security and the integrity of assets. It provides confidence to the organization and its stakeholders that the organization is able to provide a safe and secure environment which fulfills organizational and stakeholder requirements.

This Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's security assurance management system. An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.

The application of a system of processes within an organization, together with the identification and interactions of these processes and their management, can be referred to as a "process approach".

The process approach for security assurance management presented in this Standard encourages its users to emphasize the importance of:

a) Understanding an organization's risk, security, and asset protection requirements;

b) Establishing a policy and objectives to manage risks;

c) Implementing and operating controls to manage an organization's risks within the context of the organization's mission;

d) Monitoring and reviewing the performance and effectiveness of the security assurance management system; and

e) Continual improvement based on objective measurement.

This Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure the security assurance management system processes. Figure 1 (add later) illustrates how a security assurance management system takes as input the security assurance management requirements and expectations of the interested parties and through the necessary actions and processes produces risk management outcomes that meet those requirements and expectations. Figure 1 also illustrates the links in the processes presented in body of the Standard.

Table 1 — Plan-Do-Check-Act Model

Plan (establish the management system)	Establish management system policy, objectives, processes, and procedures relevant to managing risk and improving security assurance and to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the management system)	Implement and operate the management system policy, controls, processes, and procedures.
Check (monitor and review the management system)	Assess and measure process performance against management system policy, objectives, and practical experience and report the results to management for review.
Act (maintain and improve the management system)	Take corrective and preventive actions, based on the results of the internal management system audit and management review, to achieve continual improvement of the management system.

Compliance with this Standard can be verified by an auditing process that is compatible and consistent with the methodology of ISO 9001:2000, ISO 14001:2004, ISO/IEC 27001:2005, or and the PDCA Model.

Security management system — Fraud countermeasures and controls

1 Scope

This International Standard addresses managing the risks of fraudulent acts to an organization's tangible and intangible assets. Including acts of:

a) intended deception

b) malicious intent

c) willful neglect, and

d) unintended facilitation of fraudulent activities

The requirements specified in this International Standard are generic and intended to be applicable to all organizations (or parts thereof), regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment, product and/or service portfolio, threat profile and complexity.

It specifies requirements for a security management system for fraud counter measures and controls to enable an organization to develop and implement policies, objectives, and programs. This International Standard applies to risks and impacts of fraudulent acts that the organization identifies as those to be controlled, influenced, or reduced. It does not itself state specific performance criteria.

This International Standard is intended to facilitate an organization to:

a) Develop a fraud countermeasures and controls management policy;

b) Establish objectives, procedures, and processes to achieve the policy commitments;

c) Demonstrate compliance with legal and other requirements;

d) Assure competency, awareness, and training;

e) Evaluate performance and take action as needed to improve;

g) Demonstrate conformity of the management system to the requirements of this International Standard; and

h) Establish and apply a process for continual improvement.

This International Standard is applicable to any type, size or complexity of organization that wishes to:

a) Establish, implement, maintain, and improve a security management system for fraud countermeasures and controls;

b) Assure itself of its conformity with its stated fraud countermeasures and control management policy;

c) Demonstrate conformity with this International Standard by:

i. Making a self-determination and self-declaration; or

ii. Seeking confirmation of its conformance by parties having an interest in the organization (such as customers); or

iii. Seeking confirmation of its self-declaration by a party external to the organization; or

iv. Seeking certification/registration of its security management system for fraud countermeasures and controls by an external organization.

2 Normative references

No normative references are cited at this time. This clause is included in order to retain clause numbering identical with other ISO management system standards.

3 Terms and definitions

To be completed later. To reference Aligned definitions + discipline specific ones including: MSS common terms and core definitions of JTCG/TF1/N28 & JTCG/TF3/N086

4 Establishing the framework

4.1 General

The organization shall establish, implement, maintain and improve a security management system for fraud countermeasures and controls.

The organization shall consider:

a) the external and internal factors referred to in 4.2

b) the needs and requirements referred to in 4.4 and 4.5

c) determine issues or concerns to:

i. assure the management system can achieve its expected outcome(s)

ii. prevent undesired effects

iii. address opportunities for improvement.

4.2 Context of the organization

The organization shall identify and evaluate external and internal factors that are relevant to its purpose and that affect its ability to achieve the expected outcomes of its security assurance management system.

These factors shall be taken into account when establishing, implementing, and maintaining and improving the organization's security

In establishing its external context, the organization shall ensure that the objectives and concerns of external interested parties are considered when developing threat resistance or risk reduction criteria. The

organization shall evaluate factors within the organization that can influence the way in which the organization will manage risk.

NOTE Organizations of all types, size and complexity operate in circumstances that are subject to opportunities, change and risk, consequently the organization evaluates such information in order to innovate, maintain and improve the effectiveness of its management system, during its short-term and long-term planning.

4.3 Control of documented information

Documented information required by the security assurance management system and by this International Standard shall be strictly and confidentially monitored.

Controls for documented information shall include as applicable:

a) Distribution

b) Access* and confidentiality

c) Integrity of the documents by ensuring they are tamperproof and securely backed-up

d) Storage and preservation

e) Retrieval and use

f) Identification of version and changes

g) Preservation of legibility (i.e. clear enough to read)

h) Prevention of the unintended use of obsolete information

i) Retention and disposition

Ensure that documented information of external origin determined by the organization to be necessary for the planning and operation of the security assurance management system is identified as appropriate, and controlled.

NOTE 1 Access implies a decision to implement controls regarding the permission and authority to view and/or change documented information.

NOTE 2 Access, retention and distribution controls should consider legal and contractual obligations (including non-disclosure agreements), as well as the confidentiality, sensitivity and proprietary nature of the information.

4.4 Needs and requirements

When establishing its' security assurance management system, the organization shall determine:

a) its relevant interested parties, including contractors, employees and supply chain partners, and

b) their needs and requirements, including applicable legal requirements.

NOTE The balancing of needs can be achieved by an organization by giving due weight to the needs of interested parties, for example, consumers, owners, society etc.

4.5 Defining risk criteria

The organization shall define and document criteria to evaluate the significance of threat and risk. The criteria shall reflect the organization's values, objectives and resources. When defining the threat and risk criteria the organization shall consider:

a) legal and regulatory requirements and other requirements to which the organization subscribes;

b) the organization's overall risk management policy;

c) the nature and types of threats and consequences that can occur to its business and operations;

d) how likelihood, consequences and level of risk will be determined;

e) views of interested parties;

f) level of risk tolerance or risk aversion; and

g) how combinations or multiples of risk will be taken into account.

When addressing risks associated with fraudulent acts or negligence the organization shall establish risk assessment based programs for:

a) Customer related risks

b) Information and computer related risks

c) Material related risks

d) Supply chain related risks

e) Physical intrusion related risks

f) Personnel related risks

g) Disaster related risks

h) Security failure related risks

i) Security management related risks

4.6 Scope of the management system

The organization shall define and retain documented information on the scope of the security assurance management system, such that the boundaries and applicability of the security management system can be clearly communicated to internal and external parties. This communication shall consider the limitation to information judged as having strategic value to harmful or dishonest individuals and organizations, protected by laws or under the scope of non-disclosure agreements.

In defining the scope, the organization shall:

a) Define the boundaries of the organization to be included in the scope of its security assurance management system, being the whole organization or one or more of its constituent parts.

b) Establish the requirements for security assurance management, considering the organization's mission, goals, internal and external obligations (including those related to interested parties), and legal responsibilities.

c) Consider critical operational objectives, assets, functions, services, and products.

d) Determine risk scenarios, based both on potential internal and external events, that could adversely affect the critical operations, products and functions of the organization.

e) Define scope of the security assurance management system in terms of and appropriate to the size, nature, and complexity of the organization from a perspective of continual improvement.

The organization shall define the scope consistent with protecting and preserving the integrity of the organization and its relationships with interested parties, including interactions with key suppliers, contractors, outsourcing and supply chain partners, and other interested parties (for example, customers, stockholders, employees and the community in which it operates, etc.). Where an organization chooses to outsource any process that affects conformity with these requirements, the organization shall ensure that conformity with needs and/or requirements are monitored.

5 Leadership

5.1 General

Top management shall demonstrate leadership with respect to the security assurance management system by:

a) visibly directing and controlling its overall direction and operation

b) motivating persons to ensure the security assurance management system supports the security assurance performance of the organization.

NOTE Leadership is not restricted to just top management.

5.2 Management commitment

Top management shall demonstrate its commitment by:

a) ensuring the security assurance management system is compatible with the strategic direction of the organization;

b) integrating the security assurance management system requirements into the organization's business processes;

c) providing the resources to establish, implement, maintain and continually improve the security assurance management system (see 7.1)

d) communicating the importance of effective security assurance management and conformance to the security assurance management system processes;

e) setting the criteria for accepting risks and the acceptable levels of risk;

f) performing effective management reviews to ensure that the security assurance management system achieves its expected outcomes;

g) directing and supporting continual improvement

NOTE Reference to "business" in this International Standard should be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.3 Policy

1Top management shall establish and communicate a security assurance policy. The policy shall:

a) be appropriate to the purpose of the organization;

b) provide the framework for setting objectives;

c) define the requirements of a risk and threat analysis methodology;

d) include a commitment to satisfy applicable interested party needs and requirements;

e) Includes a commitment to threat resistance, risk avoidance, prevention, and reduction;

f) include a commitment to continual improvement of the security assurance management system;

g) be implemented and maintained;

h) be reviewed for continuing suitability; and

i) be available to interested parties with consideration for the limitation to information judged as having strategic value to harmful or dishonest individuals and organizations, protected by laws or under the scope of non-disclosure agreements.

NOTE Organizations may choose to have a detailed security management policy for internal use which would provide sufficient information and direction to drive the security management system (parts of which may be confidential) and have a summarized (non-confidential) version containing the broad objectives for dissemination to its stakeholders and other interested parties.

The organization shall retain documented information on the policy.

The policy shall be reviewed at planned intervals and when significant changes occur.

5.4 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the management system is established and implemented in accordance with the needs and/or requirements of this International Standard; and

b) reporting on the performance evaluation of the security assurance management system to top management.

6 Planning

6.1 Legal and other requirement

The organization shall establish and maintain procedure:

a) To identify legal, regulatory, and other requirements to which the organization subscribes that are related to the organization's hazards, threats, and risks.

b) To determine how these requirements apply to its operations.

The organization shall document this information and keep it up to date.

The organization shall ensure that applicable legal, regulatory, and other requirements to which the organization subscribes are considered in developing, implementing, and maintaining its security assurance management system.

6.2 Risk assessment

The organization shall establish, implement and maintain a formal and documented risk assessment process for security risk identification, risk analysis and risk evaluation:

a) To identify risks due to intentional threats that have a potential for direct or indirect consequences on the organization's activities, assets, operations, functions, and interested parties (threat, vulnerability, and criticality analysis);

b) To systematically analyze security risk (likelihood and consequence analysis);

c) To determine those security risks that have a significant impact on activities, functions, services, products, supply chain, interested party relationships, and the environment (evaluation of significant risks and impacts); and

d) To systematically evaluate and prioritize security risk controls and treatments and their related costs.

The organization shall:

a) Document and keep this information up to date and confidential, as is appropriate;

b) Periodically review whether the security assurance management scope, policy, and security risk assessment are still appropriate given the organizations' internal and external context;

c) Re-evaluate security risks within the context of changes within the organization or made to the organization's operating environment, procedures, functions, services, partnerships, and supply chains;

d) Evaluate the direct and indirect benefits and costs of options to reduce security risk and enhance reliability and resilience;

e) Ensure that the prioritized risks and impacts are taken into account in establishing, implementing, and operating its security assurance management system; and

f) Evaluate the effectiveness of security risk controls and treatments.

6.3 Objectives and plans to achieve them

Top management shall ensure that security assurance management objectives are established for relevant functions and levels within the organization.

The security assurance management objectives shall :

a) be consistent with the policy,

b) be measurable,

c) have time frames for their achievement,

d) take account of applicable needs and requirements of all interested parties,

e) enable opportunities to maintain or improve performance,

f) be monitored and updated as appropriate.

The organization shall retain documented information on the objectives.

To achieve its objectives, the organization shall determine:

a) who is responsible

b) what will be done, and when it will be completed

c) how the results will be evaluated

6.4 Action to address issues and concerns

The organization shall establish, implement and maintain a formal and documented security risk treatment process, which considers:

a) removing the threat or risk source, where possible;

b) avoiding the risk by temporarily halting activities that give rise to the risk;

c) removing or reducing the likelihood of harm;

d) removing or reducing harmful consequences;

e) sharing the risk with other parties, including risk insurance; and

f) retaining risk by informed decision.

Top management shall :

a) assess the benefits and costs of options to remove, reduce or retain risk; and

b) periodically review the security risk treatment to reflect changes to the external environment, including legal, regulatory and other requirements, and changes to the organization's policy, facilities, information management system(s), activities, functions, products, services and supply chain.

The organization shall establish, implement and maintain security assurance programs for achieving its objectives and security risk treatment goals. The programs shall be optimized and prioritized in order to control and treat risks associated with threats of disruptions to the organization and its supply chain.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the security assurance management system.

7.2 Competence

The organization shall :

a) determine the necessary competence of person(s) doing work under its control that affects its security assurance performance;

b) ensure these persons are competent on the basis of appropriate education, training, and experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and

d) retain appropriate documented information as evidence of competence and any actions taken.

NOTE Applicable actions may include the provision of training, the hiring of new persons, or the contracting of competent persons.

7.3 Awareness

Persons doing work under the organization’s control shall be aware of:

a) the security assurance policy,

b) their contribution to the effectiveness of the security assurance management system, including the benefits of improved security assurance performance,

c) the effects of their divergence from the security assurance management system requirements.

7.4 Communication and consultations

Communication and consultation with internal and external interested parties shall take place during all stages of the security assurance management process

The organization shall establish, implement, and maintain a formal and documented communication and consultation process with internal and external interested parties to ensure that:

a) it protects the integrity and confidentiality of sensitive and proprietary information, as appropriate;

b) assets, risks, and obligations are adequately identified;

c) interests of interested parties, as well as dependencies and linkages with external resources and interested parties are understood;

d) the security assurance management process interfaces with other management disciplines;

e) different views are appropriately considered when defining security risk criteria and evaluating risks; and

f) the security assurance management process is being conducted within the appropriate internal and external context and parameters relevant to the organization and its interested parties.

7.5 Documented information

7.5.1 General

The organization's security assurance management system shall include:

a) documented information required by this International Standard,

b) documented information determined by the organization as being required for the effectiveness of the security assurance management system.

7.5.2 Create and update

The process for creating or updating documented information (see 7.5.1) shall include:

a) its identification and description (e.g. a title, name, date, author, number, revision reference etc.)

b) consideration of how the information will be captured and presented

c) its review and approval for adequacy, when applicable

NOTE 1 The capture and presentation includes what format is to be used (e.g. language, software version, graphics) or media is to be used (e.g. paper, electronic document)

NOTE 2 The extent of documented information for a security assurance management system can differ from one organization to another due to:

a) the size of organization and its type of activities, processes, products and services,

b) the complexity of processes and their interactions, and

c) the competence of persons

8 Operation

8.1 Operational planning and control

The organization shall determine, plan, implement and control those operational activities and/or processes needed to:

a) fulfill its security assurance policy and security assurance objectives, and

b) meet applicable needs and requirements of all interested parties.

This shall include:

a) establishing criteria for those activities and/or processes;

b) establishing performance measurements;

c) implementing controls, in accordance with the criteria and performance measurements;

d) keeping documented information to demonstrate that the activities and/or processes have been carried out as planned.

The organization shall ensure that planned changes are controlled and that unintended changes are reviewed and appropriate action is taken.

NOTE Operational activities and/or processes may include activities and/or processes that are contracted out or outsourced, or related to products.

8.2 Resources, roles, responsibility, and authority for security assurance management

Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective security assurance management, consistent with the achievement of its security assurance management policy, objectives and programs.

The organization shall establish planning, security, incident command, response team(s) with defined roles, appropriate authority, adequate resources including effective and safe equipment, and rehearsed operational plans and procedures.

8.3 Competence, training and awareness

The organization shall ensure that people performing tasks who have the potential to prevent, cause, respond to, mitigate, or be affected by significant threats and risks are competent (on the basis of appropriate education, training and experience), and shall retain associated records.

The organization shall identify competencies and training needs associated with security assurance management. It shall provide training or take other action to meet these needs, and shall retain associated records.

The organization shall establish, implement, and maintain controls to ensure that persons working for or on behalf of the organization who are assigned responsibilities defined in this MSS are aware of :

a) the significant threats and risks associated with their work and the benefits of improved personal performance;

b) the procedures to reduce the likelihood and/or consequences of a disruption to the organization;

c) the importance of conformity with the security assurance management policy and procedures, and with the needs and/or requirements of the security assurance management system;

d) their roles and responsibilities in achieving conformity with the requirements of the security assurance management system; and

e) the potential consequences of departure from specified procedures.

8.4 Communication

The organization shall establish, implement and maintain controls for:

a) protection of the integrity and confidentiality of sensitive and proprietary information, as appropriate

b) communicating with persons working for or on behalf of the organization who are assigned responsibilities defined in this MSS

c) communicating with external parties including supply chain and outsource partners, contractors, the local emergency services, local forums, and the media;

d) receiving, documenting, and responding to communications from internal and external interested parties;

e) defining and assuring availability of the means of communication during atypical situations and disruptions and

f) regular testing of security assurance communications system for normal and abnormal conditions.

NOTE In certain circumstances, for example to prevent false alarm or for reasons of commercial security, the organization's top managers may decide not to communicate all or parts of its risk assessment, or its security assurance plans. In such circumstances, the organization should document the reasons for so doing.

All communications shall take into consideration the limitation on information judged as having strategic value to harmful or dishonest individuals and organizations, protected by laws or under the scope of non-disclosure agreements.

8.5 Incident prevention and management

The organization shall establish, implement and maintain controls to prevent and manage an incident that has the potential to harm the organization, its employees, partners and interested parties. The controls shall document how the organization will:

a) avoid, remove or reduce the likelihood of an incident;

b) reduce and manage the consequences of an incident;

c) protect people, physical assets, critical and sensitive information including records from immediate harm;

d) maintain continuity of essential services; and

e) recover from an incident.

The organization shall periodically review and, where necessary, revise its incident prevention and management controls. All reviews and revisions shall be documented.

9 Performance evaluation

9.1 Monitoring and measurement

The security assurance management performance of the organization shall be monitored, measured, and analyzed in order to evaluate the effectiveness of the security assurance management system. This monitoring and measurement system shall be in accordance with the performance measurements established.

The organization shall determine:

a) what shall be monitored and measured

b) how and when the monitoring and measuring shall be performed

c) how and when the analysis and evaluation of the results of monitoring and measurement shall be performed

The organization shall determine the controls needed for the monitoring and measurement system, as applicable, to ensure:

a) Valid results.

b) Take action when necessary to address adverse trends or results (see 6.4).

c) The organization shall retain relevant documented information as evidence of the results while respecting the limitation on information judged as having strategic value to harmful or dishonest individuals and organizations, protected by laws or under the scope of non-disclosure agreements.

9.2 Evaluation of compliance

The organization shall establish, implement and maintain procedures for periodically evaluating compliance with legal, regulatory and other requirements. The organization shall keep records of the results of the evaluations.

9.3 Exercises and testing

The organization shall use exercises and other means to test the appropriateness and efficacy of its security assurance management system plans, processes and procedures, including interested party relationships and infrastructure interdependencies. Exercises should be designed and conducted in a manner that limits disruption to operations and exposes people, assets and information to minimum risk.

Exercises should be conducted regularly, or following significant changes to the organization's mission and/or structure, or following significant changes to the external environment. A formal report should be written after each exercise. The report should assess the appropriateness and efficacy of the organization’s security assurance management system plans, processes and procedures including nonconformities, and should propose corrective and preventative action (9.4).

Post-exercise reports should form part of top management reviews (9.5).

9.4 Nonconformities, corrective and preventive action

The organization shall establish, implement and maintain procedures for dealing with nonconformities and for taking corrective and preventive action. The procedures shall define requirements for:

a) identifying and correcting nonconformities and taking actions to mitigate their impacts;

b) investigating nonconformities, determining their causes and taking actions in order to avoid their recurrence;

c) evaluating the need for actions to prevent nonconformities and implementing appropriate actions designed to avoid their occurrence;

d) recording the results of corrective and preventive actions taken; and

e) reviewing the effectiveness of corrective and preventive actions taken.

The organization shall ensure that proposed changes are made to the security assurance management system documentation.

9.5 Internal Audit

The organization shall conduct internal audits at planned intervals to provide information to assist in the determination of whether the security assurance management system:

a) conforms to

i. the organization’s own requirements for its security assurance management system

ii. the requirements of this International Standard, and

b) is effectively implemented and maintained.

The organization shall :

a) plan, establish, implement and maintain an audit program(s), taking into consideration the importance of the activities and processes concerned and the results of previous audits;

b) define the audit criteria, scope, frequency, methods, responsibilities, planning requirements and reporting;

c) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

d) ensure that the results of the audits are reported to the management responsible for the area being audited; and

e) retain relevant documented information as evidence of the results.

9.6 Management review

Top management shall review the organization's security assurance management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

Management reviews shall consider the security assurance performance of the organization, including:

a) follow-up actions from previous management reviews;

b) the need for changes to the security assurance management system, including the policy and objectives; and

c) opportunities for improvement.

The organization shall :

a) communicate the results of management review to relevant interested parties;

b) take appropriate action relating to those results;

c) retain documented information as evidence of the results of management reviews.

10 Opportunities for improvement

10.1 Opportunities for improvement

The organization shall also evaluate the need for action to exploit opportunities for improvement in security assurance management system performance and eliminate the causes of nonconformities, including:

a) reviewing nonconformities;

b) determining the root causes of nonconformities;

c) evaluating the need for action to ensure that nonconformities do not recur;

d) determining and implementing action needed to improve security assurance performance and

e) reviewing the effectiveness of the action taken to improve performance.

Actions to improve security assurance management system performance shall be appropriate to the effects of the nonconformities encountered, the organization's obligations and resource realities.

The organization shall ensure that any necessary changes are made to the security assurance management system.

The organization shall retain documented information as evidence of:

a) the nature of the nonconformities and any subsequent actions taken, and

b) the actions to improve performance and their results

10.2 Continual improvement

The organization shall continually improve the effectiveness of the security assurance management system.

Annex A
(informativ)

General Guidance

A.1 Procedures to prevent and manage fraud and other disruptive events

The organization should establish, implement and maintain procedures to prevent and manage fraud and other disruptive events which have the potential to harm the organization, its key interested parties including contractors, customers, supply chain partners, and the environment.

Procedures should be concise and accessible to those responsible for their implementation. Flow charts, diagrams, tables and lists of action should be used rather than expansive text.

The purpose and scope of each procedure should be agreed by top management and understood by those responsible for its implementation. Critical interdependencies should be identified, and the relationships between procedures, including those of partners, first responders, the emergency services and local authorities, should be stated and understood.

A.2 Procedures for prevention and management of fraud and other disruptive events

The purpose of a prevention or mitigation procedure is to define the measures to be taken by the organization to minimize the likelihood of fraud and other disruptive events or to minimize the potential for the severity of the consequences of the fraud.

Prevention procedures should describe how the organization will take proactive steps to protect its assets, technologies, products, and services by establishing architectural, administrative, design, operational and technological approaches to avoid, eliminate or reduce the likelihood of risks materializing, including the protection of assets from unforeseen threats and risks.

Mitigation procedures should describe how the organization will take proactive steps to protect its assets, prior to and following an incident of fraud or other disruptive events, by establishing immediate, interim and long-term approaches to reduce the consequences of fraud or other disruptive events before and after they materialize, including the protection of assets from unforeseen threats and risks.

Organizations may chose to have a single procedure with sections and/or annexes dealing with different types of fraud and other disruptive events. Alternatively, separate procedures may be written for each type of fraud and other disruptive events.

Each procedure should specify as a minimum:

a) the purpose and scope of the procedure;

b) assets, technologies, products and/or services to be protected from fraud and other disruptive events;

c) objectives and measures of success;

d) implementation steps and the frequency with which the procedure is carried out;

e) roles, responsibilities and authorities;

f) communication requirements and procedures;

g) internal and external interdependencies and interactions;

h) resource, competency and training requirements; and

i) information flow and documentation processes.

The organization should identify the primary individual responsible for each prevention and mitigation procedure, and should state who is responsible for reviewing, amending and updating the procedure. The process of reviewing, amending, updating and distributing procedures should be controlled.

Examples of prevention and management procedures for fraud and other disruptive events include:

a) Eliminate the risk by complete removal of the threat, or risk exposure;

b) Reduce the risk by modifying activities, processes, equipment, technologies or materials;

c) Isolation or separation of the risk from assets (physical or human);

d) Engineering controls to detect, deter and delay a potential threat agent;

e) Administrative controls such as work practices or procedures that reduce risk; and

f) Protection of the asset if the threat or risk cannot be eliminated or reduced.

NOTE The organization should also develop response, continuity and recovery procedures to define the measures to be taken by the organization to manage fraudulent and other disruptive events. Plans should describe how the organization will respond to one or more types of fraud and other disruptive events.

Part 2: May be determined at a future date (for example this could contain a set of informative guidelines)