Draft Design Specification
ISO 16125 – Generic Security Assurance Management System Standard

INTRODUCTION and SUMMARY

This document identifies users and specifies the need for the content and structure of a new ISO standard for a Generic Security Assurance Management System that addresses all forms of threat to the operations of an organization posed by fraudulent[1], harmful, dishonest and wilfully negligent individuals and organizations. Threats of this type are the result of an organization being in possession or perceived as being in possession of physical items or information items that corrupt individuals and organizations want. These corrupt entities will harm others and disrupt operations to acquire those items of value. Identifying, establishing and maintaining an appropriate level of resistance and countermeasure to these threats that meet the requirements of the organization and its' relying parties provides an assurance of security. Conversely, when an operation is known to have little or no resistance to a serious threat, no recognized method of preventing or deterring an attack and little or no means of mitigating the effects of an attack, a serious security risk is being taken. Serious security risks are not be in the interest of an organization or its' relying parties and will need to be eliminated or reduced to an acceptable level. The purpose of this MSS is to provide the security management team of an organization with a systematic approach and guidelines for identifying and managing security risk in order to assure overall security of an operation to the satisfaction of the organization, its' stakeholders and relying parties. The implementation guideline annex to this standard presents threat profiles that are typical of a number of industries. The guideline then offers "best practice" solutions in terms of security policies, procedures, infrastructure, systems, and tasks to be performed that resist and counter the threats included in each profile. This generic MSS, wherever possible, builds on and compliments existing ISO security related standards such as those that specifically address information, information technology (IT), intellectual property (IP) and supply chain security. Reference to those standards will be made both in the body of this MSS and in the implementation guideline annex.

1. Users, User Needs and User Benefits

The users of this MSS are expected to be individuals and teams of individuals within organizations that have overall responsibility and accountability for the identification and management of all security risk associated with the operation of the organization. Organizations that are likely to use this MSS include :-

i. The global business community;
ii. Manufacturers of brand products;
iii. Manufacturers of high value pharmaceutical products;
iv. Manufacturers and developers of security technologies and solutions;
v. Organizations who for reasons of health and safety must avoid the use of counterfeit replacement parts;
vi. Transportation companies;
vii. Not for Profit Organizations and Foundations;
viii. Educational institutions;
ix. Public Service Agencies;
x. Identity issuing authorities and identity credential producers;
xi. First Responder Organizations;
xii. Government Agencies and Organizations;

[1] This MSS uses the practical (rather than legal) definition of "FRAUD" adopted for use by ISO TC 247 as follows:- TBD

xiii. Professional Practitioners in the disciplines of Security, Emergency Preparedness, Emergency Management, Disaster Management and Business Continuity; Critical Infrastructure;
xiv. Security risk management consultants.
xv. Small to medium enterprises who must demonstrate they are “secure” to their larger customers.

Security Assurance has a strong and growing social and market relevance. This growing demand for security assurance applies to food, water, energy, health care, prescription drugs, travel, transportation, personal identity, personal permission, access permission and all products, services, privileges and entitlements that are subject to serious threats posed by harmful and dishonest individuals and organizations. The situation, in the world today, is that markets everywhere are increasingly being subjected to counterfeiting, alteration, diversion, false claims and other fraudulent acts. A strong, holistic security assurance MSS, if implemented across affected markets and societies, will contribute significantly to reducing their abuse in the same way that adoption of quality assurance has instilled trust in the quality of products and services.
As a result of the need to address these rising levels of threat, the following security related standards and ISO technical committee have emerged:

1. the ANSI/NASPO-SA-2008 security assurance standard
2. the CEN CWA 14641 security management system for security printing.
3. Creation of the ISO TC 247 on fraud countermeasures and controls

The proposed security assurance MSS will enable users and relying parties to unambiguously specify their requirements for security assurance. It will also provide organizations who are relied upon by other entities to supply evidence of their ability to comply with those management requirements. The initial and recurring investment of security assurance implementation can be significant. In general, it is realistic to expect that the higher the resistance and complexity of countermeasures implemented to effectively address the threats then the level of investment in security will also rise. In formulating this MSS and security assurance guidelines, every effort must be made to avoid placing attainment of a satisfactory security assurance beyond the investment reach of small to medium enterprises.

A significant benefit of implementation of this MSS for all sizes of organization is the knowledge gained by a relying party concerning the potential level of security risk it will be exposed to in using the products or services of the supplier organization. This risk has nothing to do with the financial or quality related risks of doing business. It concerns the degree to which the relying party is assured that the supplier or partner organization, through the use of security risk management methods required by this MSS, is able to prevent, detect and control acts and threats posed by the perpetrators of fraud. Those acts and threats, if they are not resisted, could potentially eliminate or substantially degrade the value of products or services offered by a supplier or partner organization. This MSS will provide this knowledge through definition of what is required by an organization or relying party to plan and implement holistic security assurance. This, together with the methods of conformity assessment developed for use with this MSS (to be made available at a later date) can then be used by the supplier/partner organization to assure the relying party (either directly, or by independent conformity assessment) of their compliance with this MSS.

2. Scope

This international standard specifies the requirements with guidance for use of an overall security assurance management system. This standard specifies requirements for planning, establishing, implementing, operating, monitoring, reviewing, exercising, maintaining and improving a security assurance management system. 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 organisation. The extent of application of these requirements depends on the organization's operating environment, product and/or service portfolio, threat profile and complexity.

This international standard is focused on the prevention, detection and control of fraudulent acts related to the disruption of organizations caused by known or unknown perpetrators including;

- intentional acts of deception
- malicious intent
- unintended acts or wilful neglect

that create human, economic, environmental and other forms of tangible harm and loss.

This international standard is applicable to all sizes and types of organization wishing to;

- establish, implement, maintain and improve a comprehensive security assurance management system
- assure conformance with stated security assurance management policy
- demonstrate conformance by first, second or third party conformity assessment.

It is the intent of this international standard to support uniformity in the structure of a comprehensive management system, emphasizing the functional relations between the various disciplines addressing the management of all forms of threat posed by harmful individuals and organizations. It enables an organization to design a holistic and unified security assurance management system that is appropriate to its needs, and those of its' stakeholders and business partners. To ensure a robust strategy, an organization should consider the range of risk reduction options outlined in the accompanying implementation guideline annex. These options are shaped by the threat and vulnerability profile of the organization which include;

- regulations
- customer and organizational requirements
- the organization's products and services
- the processes employed
- the size and structure of the organization
- and the requirements of its' stakeholders.

In addition to management system elements, this MSS will address, as a minimum, the following areas of threat;

- Customer
- Information and computer intrusion
- Material
- Supply chain
- Physical intrusion
- Personnel
- Disasters
- Security system failures and breaches
- Security Management

This international standard can be used by internal and external parties, including certification bodies, to assess an organization's ability to meet its own security assurance needs, as well as any customer, legal or regulatory needs.

3. Compatibility

Normative reference will be made whenever possible to minimize the need for duplication. In particular, we recognize the need to;

- emphasize that implementation of security assurance measures must follow the PDCA principles in other ISO management system standards,
- work closely with ISO committees working on management system standards.

ISO 16125 will be consistent with ISO Guide 72 and aligned with ISO 9001, ISO 14001, ISO 22001, ISO27001 and ISO 28000.

4. Consistency

5. Consistency will be assured by taking into account the following national and international standards:-

a) ANSI/NASPO-SA-2008 Security Assurance Standard
b) The ISO/IEC 27000 series – Information Technology Security
c) The ISO 28000 series – Supply Chain Security
d) ISO/DIS 26000 – Social Responsibility
e) ISO/PAS 22399 Societal Security – Guideline for Incident Preparedness and Operational Continuity Managment
f) ISO 31000 Risk Management
g) ISO 19011 Guidelines for Quality and/or Environmental Management Systems Auditing (To be Revised)
h) ISO 17021 Conformity Assessment - Requirements for Bodies Providing Audit and Certification of Management Systems
i) ISO 17024 Conformity Assessment - General Requirements for Bodies Operation Certification of Persons
j) CEN-CWA 14641:(2003) Security Management System for the Printing Industry
k) CEN-CWA 15374 Security Management System for Suppliers to the Printing Industry
l) ISO/IEC TR 15443 (Series 1, 2 and 3) Information Technology- Security Techniques – a Framework for IT Security Assurance
m) IEC 62443-2 Security Assurance Principles and Practice

6. Model

ISO 16125 will be based on the common elements of MSS's described in ISO Guide 72:

a) Policy
b) Planning
c) Implementation and operation
d) Performance assessment
e) Improvement
f) Managerial review

7. Structure

ISO 16125 will follow new MSS structure proposed by the ISO/TMB/TAG13 - Joint Technical Co-ordination Group (JTCG). Accordingly ISO 16125 will have the following table of contents:

Introduction *Note: Unique to the discipline*
1. Scope *Note: Specific to the discipline; possibly some identical text*
2. Normative references *Note: Clause Title shall be used. Unique to the discipline*
3. Terms and definitions *Note: Clause Title shall be used. Terms and definitions may either be within the standard or in a separate document. To reference Aligned definitions + discipline specific ones*
4. Context of the organization
4.1 Understanding of the organization and its context The organization shall determine 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 the organization's security assurance management system, and assigning priorities. 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/or improve the effectiveness of its management system, during its short-term and long-term planning
4.2 Needs and requirements When establishing its security assurance management system, the organization shall determine - its relevant interested parties and - 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.
4.3 Management system and scope The organization shall establish, implement, maintain and improve an security assurance management system in accordance with the requirements of this International Standard. The organization shall consider: - the external and internal factors referred to in 4.1 - the needs and requirements referred to in 4.2, and determine issues or concerns to - assure the management system can achieve its expected outcome(s) - prevent undesired effects

- address opportunities for improvement.

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 assurance management system can be clearly communicated to internal and external parties.

5. Leadership

5.1 General

Top management shall demonstrate leadership with respect to the security assurance management system by
- visibly directing and controlling its overall direction and operation
- 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

- ensuring the security assurance management system is compatible with the strategic direction of the organization
- integrating the security assurance management system requirements into the organization's business processes;
- providing the resources to establish, implement, maintain and continually improve the security assurance management system (see 7.1)
- communicating the importance of effective security assurance management and conformance to the security assurance management system processes;
- performing effective management reviews to ensure that the security assurance management system achieves its expected outcomes
- 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

Top 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) include a commitment to satisfy applicable needs and requirements,

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

e) be implemented

f) be reviewed for continuing suitability; and

g) be available to interested parties.

The organization shall retain documented information on the policy.

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 requirements of this International Standard

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

6 Planning

6.1 Objectives and plans to achieve them

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

The security assurance objectives shall:

- be consistent with the policy

- be measurable (if practical)

- have time frames for their achievement.

- take account of applicable needs and requirements

- enable opportunities to maintain or improve performance,

- 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

d) how the results will be evaluated

6.2 Action to address issues and concerns

The organization shall determine how to address the issues and concerns identified in 4.3 that may affect its ability to achieve the expected outcomes of the security assurance management system.

The organization shall:

a) evaluate the need to plan action to address these issues and concerns

b) if necessary
- integrate and implement these actions into its security assurance management system processes
- ensure information will be available to evaluate if the actions have been effective (see 9.1)

7. Support

7.1Resources

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 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: - the security assurance policy - their contribution to the effectiveness of the security assurance management system, including the benefits of improved security assurance performance - the effects of their divergence from the security assurance management system requirements
7.4 Communication
7.4.1 External communication The organization shall establish, implement and maintain arrangements for communicating with relevant external interested parties.
7.4.2 Internal communication The organization shall establish, implement and maintain arrangements for internal communication within the organization
7.5 Documented information
7.5.1 General The organization's security assurance management system shall include: - documented information required by this International Standard - 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 Note1The 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

7.5.3 Control of documented Information

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

Controls for documented information shall include as applicable:

a) Distribution

b) Access

c) Storage and preservation

d) Retrieval and use

e) Identification of version and changes

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

g) Prevention of the unintended use of obsolete information

h) 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 Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8. Operation

8.1 Operational planning and control

The organization shall determine, plan, implement and control those operational activities and/or processes needed to:
- fulfil its security assurance policy and security assurance objectives, and
- meet applicable needs and requirements.

This shall include

a) establishing criteria for those activities and /or processes

b) implementing controls, in accordance with the criteria

c) 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 the supply of goods and services

9. Performance Evaluation

9.1 Monitoring and measurement

The security assurance performance of the organization shall be monitored, measured, and analysed in order

to evaluate the effectiveness of the security assurance management system

The organization shall determine:

- what shall be monitored and measured

- how and when the monitoring and measuring shall be performed

- 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 equipment, as applicable, to ensure valid results.

Take action when necessary to address adverse trends or results (see 6.2).

The organization shall retain relevant documented information as evidence of the results.

9.2 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
- the organization's own requirements for its security assurance management system
- the requirements of this International Standard.

b) is effectively implemented and maintained.

The organization shall
a) plan, establish, implement and maintain an audit programme(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

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

9.3 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:

- communicate the results of management review to relevant interested parties

- take appropriate action relating to those results

- retain documented information as evidence of the results of management reviews.

10. Improvement

10.1 Nonconformity and corrective action

The organization shall:

a) identify nonconformity(ies),

b) react to the nonconformity, and as applicable
- take action to control, contain and correct it,
- deal with the consequences

The organization shall also evaluate the need for action to eliminate the causes of nonconformities, including:

a) reviewing nonconformities,

b) determining the causes of nonconformities,

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

d) determining and implementing action needed, and

e) reviewing the effectiveness of the corrective action taken.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

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
- the nature of the nonconformity of any subsequent actions taken, and
- the corrective actions and their results

10.3 Continual improvement

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