INTERNATIONAL STANDARD

ISO 14298

First edition
2013-04-15

Graphic technology — Management of security printing processes

Technologie graphique — Management des procédés d'impression de sécurité

Reference number
ISO 14298:2013(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2. www.iso.org/directives

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received. www.iso.org/patents

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

The committee responsible for this document is ISO/TC 130, *Graphic technology*.

Introduction

General

This International Standard specifies requirements for a security printing management system for security printers.

Current security printing management practices lack sufficient guarantees that effective security controls are maintained to protect the interest of the customer as well as the general public. Using this International Standard the organization establishes, documents, implements and maintains a security printing management system. This security printing management system is regularly reviewed to continually improve its effectiveness. It is recognized that customer requirements sometimes exceed the requirements of this International Standard so the security printing management system also addresses customer requirements that are beyond the scope of this International Standard.

The adoption of a security printing management system is a strategic decision of an organization. The design and implementation of an organization's security printing management system is influenced by varying needs, particular objectives, products provided, processes employed, security environment, cultural issues, legal limitations, risk assessment and by size and structure of the organization.

To achieve the objectives of this security printing management system standard measures are taken to mitigate all of the security threats determined by an organizational risk assessment. Such controls focus upon reducing, eliminating and preventing acts that compromise the security printing management system of the organization.

It is not the intent of this International Standard to obtain uniformity in the structure of the security printing management system or uniformity of documented information. The security printing management system complies with laws and regulations in force. The requirements specified in this International Standard are supplementary to requirements for products and processes of an organization and allow for additional specific requirements from the customer.

This International Standard is intended to apply to security printers. It contains requirements that when implemented by a security printer may be objectively audited for certification/registration purposes.

Process approach

This International Standard promotes the adoption of a process approach when developing, implementing and improving the effectiveness of a security printing management system.

The application of a system of processes within an organization, together with the identification and interaction of these processes, and their management, is referred to as a "process approach". An advantage of a "process approach" is the ongoing control that it provides over the interaction between individual processes within the system of processes, as well as over their combination.

Basic principles

When implemented, the security printing management system:

a) achieves the security of products, processes, means of production, premises, information, raw material supplies;

b) is used to continue to meet demonstrably the requirements, and naturally, the needs of customers;

c) affords management the confidence that the targeted degree of security is actually achieved and remains effective;

d) affords the customers the confidence that the agreed nature and degree of security is or will be attained.

This International Standard prescribes which elements a security printing management system contains and not how a specific organization implements these elements.

Graphic technology — Management of security printing processes

1 Scope

This International Standard specifies requirements for a security printing management system for security printers.

This International Standard specifies a minimum set of security printing management system requirements. Organizations ensure that customer security requirements are met as appropriate provided these do not conflict with the requirements of this International Standard.

2 Normative references

No normative references are cited.

3 Terms and definitions

For the purposes of this document the following terms and definitions apply.

NOTE Italic type in a definition indicates a cross-reference to another term defined in this clause; the number reference for the term is given in parentheses.

3.1
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.8)

Note 1 to entry: The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

3.2
interested party
stakeholder
person or *organization* (3.1) that can affect, be affected by, or perceive themselves to be affected by a decision or activity

3.3
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in documented information.

3.4
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.7) and *objectives* (3.8), and *processes* (3.12) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

Note 4 to entry: A management system contains documented information to direct and control the organization.

3.5
top management
person or group of people who directs and controls an *organization* (3.1) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.4) covers only part of an organization then top management refers to those who direct and control that part of the organization.

3.6
effectiveness
extent to which planned activities are realized and planned results achieved

3.7
policy
intentions and direction of an *organization* (3.1) as formally expressed by its *top management* (3.5)

3.8
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organization-wide, project, product and *process* (3.12)].

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a *security objective* (3.32) or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of security printing management systems *security objectives* (3.32) are set by the organization, consistent with the security policy, to achieve specific results.

3.9
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential *events* (ISO Guide 73, 3.5.1.3) and *consequences* (ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated *likelihood* (ISO Guide 73:2009, 3.6.1.1) of occurrence.

3.10
competence
ability to apply knowledge and skills to achieve intended results

3.11
documented information
information required to be controlled and maintained by an *organization* (3.1) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to the *management system* (3.4), including related *processes* (3.12); information created in order for the organization to operate (documentation); and evidence of results achieved (records).

3.12
process
set of interrelated or interacting activities which transforms inputs into outputs

3.13
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.12), products (including services), systems or *organizations* (3.1).

3.14
outsource (verb)
make an arrangement where an external *organization* (3.1) performs part of an organization's function or *process* (3.12)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.4), although the outsourced function or process is within the scope.

3.15
monitoring
determining the status of a system, a *process* (3.12) or an activity

Note 1 to entry: To determine the status there may be a need to check, measure, supervise or critically observe.

3.16
measurement
process (3.12) to determine a value

3.17
audit
systematic, independent and documented *process* (3.12) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.18
conformity
fulfilment of a *requirement* (3.3)

3.19
nonconformity
non-fulfilment of a *requirement* (3.3)

3.20
correction
action to eliminate a detected *nonconformity* (3.19)

3.21
corrective action
action to eliminate the cause of a *nonconformity* (3.19) and to prevent recurrence

3.22
continual improvement
recurring activity to enhance *performance* (3.13)

3.23
risk assessment
overall process of risk identification, risk analysis and risk evaluation

[ISO Guide 73:2009, 3.4.1]

3.24
security printer
producer of printed documents or products of value or entitlement, ID documents or *security foils* (3.25) which are physically protected against forgery, counterfeiting and alteration by *security features* (3.26)

3.25
security printing
set of *processes* (3.12) which transform raw materials into documents or products of value or entitlement, ID documents or *security foils* (3.25) physically protected by *security features* (3.26)

3.26
security foil
thin film material that contains an optical variable element or similar *security feature* (3.26), which is applied onto documents or products to physically protect them against forgery, counterfeiting and alteration

3.27
security feature
component integrated in the product to protect against forgery, counterfeiting and alteration

3.28
security
protection of products, processes, information, means of production, security features and the supply chain

3.29
threat
action or potential occurrence, whether or not malicious, to breach the *security* (3.27) of the system

3.30
security breach
infraction or violation of security

3.31
documented procedure
established way of working, documented, implemented and maintained

3.32
security objective
result to be achieved with regard to *security* (3.28)

Note 1 to entry: Security objectives are in general based on the security policy of the organization.

Note 2 to entry: Security objectives are in general specified for relevant functions and levels in the organization.

3.33
security management
coordinated activities to direct and control an organization with regard to *security* (3.28)

Note 1 to entry: "Direct and control" in general entails the establishment of the policy, objectives, planning, control, security assurance and improvements with regards to *security* (3.28). Security assurance represents all planned and systematic actions needed to give a sufficient degree of confidence that a product or *process* (3.12) meets the security requirements.

3.34
security plan
documented information that specifies the procedures and resources to satisfy the security requirements of the organization

3.35
security control
aspect of *security management* (3.33) aimed at the fulfilment of the security requirements

3.36
preventive action
action to prevent the cause of a *nonconformity* (3.19)

3.37
traceability
ability to trace the history, application or location of that which is under consideration

Note 1 to entry: When considering product, traceability can relate to the origin of materials and parts, the processing history and the distribution and location of the product after delivery.

(ISO 9000:2005, 3.5.4, modified)

3.38
resource
personnel, information, premises, process equipment (software and hardware) and tools

3.39
supply chain
set of interconnected *processes* (3.12) and *resources* (3.38) that starts with the sourcing of raw materials and ends with the delivery of products and services to the customer

Note 1 to entry: Supply chains include producers, suppliers, manufacturers, distributors, wholesalers, vendors, and logistics providers. They include facilities, plants, offices, warehouses, and branches and can be both internal and external to an organization.

Note 2 to entry: Supply chain management as related to this International Standard includes the vetting of suppliers and customers from the point of initial security value, which is the point at which security is added to the product.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its security printing management system.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

— the interested parties that are relevant to the security printing management system, and

— the requirements of these interested parties.

Certification is only possible if the organization has followed the regulations of the certification procedure and if it has established a security printing management system in accordance with the specifications of this procedure. Furthermore the security printing management system has to comply with laws and regulations in force.

4.3 Determining the scope of the security printing management system

The organization shall determine the boundaries and applicability of the security printing management system to establish its scope.

When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1, and

— the requirements referred to in 4.2.

The scope shall be available as documented information.

4.4 Security printing management system

The organization shall establish, implement, maintain and continually improve a security printing management system in accordance with the requirements of this International Standard including the processes needed as outlined in normative Annex A and their interactions.

It is recognized that customer requirements may exceed the requirements of this International Standard so the security printing management system also addresses customer requirements that are beyond the scope of this International Standard.

The organization shall conduct a risk assessment on at least the following:

a) Customer-related risk

EXAMPLE Unauthorized purchase, distribution or illegal use of a product by a customer.

b) Information-related risk

EXAMPLE Unwanted, unintended, prompted or unprompted disclosure of information.

c) Security material, product and waste-related risk

EXAMPLE Theft, damage, sabotage or loss of security materials.

d) Supply chain-related risk

EXAMPLE Any subversion or compromise of the security of the organization's security products and related services at any point in the supply chain.

e) Physical intrusion and access-related risk

EXAMPLE Intrusion into sensitive physical areas.

f) Personnel-related risk

EXAMPLE Personnel fraud or unauthorized actions.

g) Disaster-related risk

EXAMPLE Security breakdowns that result from either man-made or natural disasters.

h) Security failure-related risk

EXAMPLE Occurrence of security breaches.

i) Security management-related risk

EXAMPLE Lack of security management competences.

j) Use of machinery-related risk

EXAMPLE Unauthorized use of the means of production.

k) Sales of equipment-related risk

EXAMPLE Sale, distribution of any equipment or component for illegal use.

l) Transportation-related risk

EXAMPLE Theft, modification, damage or destruction of products, security raw materials and security features during loading, unloading, storage and transportation.

m) Any additional security-related risks unique to the organization

This risk assessment shall be the basis for the establishment of a security plan (see 6.3).

NOTE ISO 31000 contains guidance for risk assessment.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the security printing management system by:

a) ensuring that the security policy and security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the security printing management system requirements into the organization's business processes;

c) ensuring that the resources needed for the security printing management system are available;

d) communicating the importance of effective security printing management and of conforming to the security printing management system requirements, including customer, legal, and regulatory requirements;

e) ensuring that the security printing management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the security printing management system;

g) promoting continual improvement;

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility;

i) developing and implementing the security printing management system and continually improving its effectiveness;

j) ensuring that a risk assessment is conducted on a continuous basis to ascertain any needed changes in the security printing management system;

k) ensuring that security requirements are understood and met;

l) reviewing the operation of the security printing management system;

m) assuring conformance to the requirements of this International Standard.

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.

5.2 Policy

Top management shall establish a security policy that:

a) is appropriate to the purpose of the organization and its products and services;

b) provides a framework for setting and reviewing security objectives;

c) includes a commitment to satisfy applicable customer, legal and regulatory requirements; and

d) includes a commitment to continual improvement of the security printing management system.

The security policy shall:

— be available as documented information;

— be communicated and understood within the organization;

— be available to interested parties, as appropriate;

— be reviewed for ongoing suitability to the needs with regard to security of the organization and its customers.

NOTE This policy has to be consistent with other policies within the organization and made known and understood at each level of the organization.

5.3 Organization roles, responsibilities and authorities

Security printing management depends on a clear understanding of each person's task, responsibility and authority with regards to security. Therefore top management shall ensure that the responsibilities and authorities for relevant roles with regards to security are assigned and communicated within the organization.

NOTE The role of reporting on the performance of the security printing management system is often assigned to a "Management Representative" who, irrespective of other responsibilities, has the responsibility for the security printing management system.

The top management shall assign the responsibility and authority for:

a) ensuring that the security printing management system conforms to the requirements of this International Standard;

b) reporting on the performance of the security printing management system and on any needed improvements to top management;

c) promoting awareness of security requirements throughout the organization;

d) conducting a continuous risk assessment according to 4.4 and ensuring the results of the analysis are implemented into the security printing management system.

6 Planning

6.1 Actions to address risks and opportunities

When planning for the security printing management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed in order to:

— ensure the security printing management system can achieve its intended outcome(s);

— prevent, or reduce, undesired effects;

— achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities, and

b) how to

1) integrate and implement these actions into its security printing management system processes;

2) evaluate the effectiveness of these actions.

The results of the planning for the security printing management system shall be retained in the security plan.

6.2 Security objectives and planning to achieve them

The organization shall establish security objectives at relevant functions and levels.

The security objectives shall:

— be consistent with the security policy;

— be measurable (if practicable);

— take into account applicable requirements;

— take into account results of the risk assessment;

— be monitored,

— be communicated, and

— be updated as appropriate.

When planning how to achieve its security objectives, the organization shall determine:

a) what will be done;

b) what resources will be required;

c) who will be responsible;

d) when it will be completed;

e) how the results will be evaluated.

The organization shall retain documented information on the security objectives and planning to achieve them.

6.3 Security printing management system planning

Top management shall ensure that:

a) the planning of the security printing management system is carried out in order to meet the security objectives and requirements;

b) the integrity of the security printing management system is maintained when it is changed.

To ensure that the security requirements are met, the organization shall establish a security plan based upon the risk assessment established in 4.4.

The security plan shall:

— document the processes needed for implementation and maintenance of the security printing management system;

— document security requirements related to the organization's processes;

— document criteria and methods to ensure that the operation and control of these processes are effective;

— ensure the availability of resources and information necessary to support security;

— ensure these processes are monitored and analysed;

— ensure the continuous evaluation and mitigation of the threats and risks to the organization.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for:

a) the establishment, implementation, maintenance and continual improvement of the security printing management system;

b) meeting security requirements.

7.2 Competence

The organization shall:

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

b) ensure that these persons are competent on the basis of appropriate education, training, skills or 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;

e) determine the talents, skills, knowledge, and capabilities each person needs to carry out his or her assigned responsibilities;

f) make sure each person understands how his or her work contributes to meeting security objectives and requirements;

g) keep documented information of each person's education, training, skills and experience.

NOTE Applicable actions may include, for example: the provision of training to, the mentoring of, or the re-assignment of current employed persons; or the hiring or contracting of competent persons.

EXAMPLE Suitable and competent personnel has knowledge on rules and procedures in the organization concerning security.

7.3 Awareness

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

a) the security policy;

b) updates and changes of the policy in a timely manner;

c) their contribution to the effectiveness of the security printing management system, including the benefits of improved security printing performance;

d) the implications of not conforming with the security printing management system requirements.

7.4 Communication

The organization shall determine the need for internal and external communication relevant to the security printing management system including:

— on what it will communicate;

— when to communicate;

— to whom it will communicate.

Top management shall set up an effective system of communication to ensure effective operation of the security printing management system.

7.5 Documented information

7.5.1 General

The organization's security printing management system shall include:

— documented information required by this International Standard;

— documented information determined by the organization as being necessary for the effectiveness of the security printing management system.

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

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

— the complexity of processes and their interactions, and

— the competence of persons.

The security printing management system documented information shall include:

a) documented statements of the security policy and security objectives;

b) a security manual containing the security plan;

c) documented procedures required by this International Standard;

d) documented information required by this International Standard.

EXAMPLE Such documented information includes but is not limited to logbooks, visitor forms, confidentiality statements, key receipts, delivery notes, etc.

The security manual shall describe:

1) the extent of the security printing management system, including details and justification for exclusions of certain sections of this International Standard that do not pertain to the organization;

2) the security plan established for the security printing management system or references to the documented information where the security plan is specified;

3) a description of the interaction between processes making up the security printing management system.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic);

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the security printing management system and by this International Standard shall be controlled to ensure:

— it is available and suitable for use, where and when it is needed;

— it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

a) distribution, access, retrieval and use;

b) storage and preservation, including preservation of legibility;

c) control of changes (e.g. version control);

d) retention and disposition;

e) prevention of the unintended use of obsolete information.

Documented information of external origin defined by the organization to be necessary for the planning and operation of the security printing management system shall be identified as appropriate, and controlled.

When establishing control of documented information, the organization shall ensure that there is adequate protection for the documented information (e.g. protection against compromise, unauthorized modification or deletion).

A documented procedure shall be defined to ensure that all documented information in the security printing management system is legible, identified, reviewed, authorized, up-to-date, issued, distributed, periodically updated and kept in restricted areas.

Documented information shall be kept to demonstrate how the security printing management system is operating. This documented information shall be legible, and easy to identify and retrieve.

A documented procedure shall describe how documented information is identified, stored, protected, retrieved, and shall define its retention and disposal times.

It shall also be stipulated who has access to this documented information.

NOTE 1 In addition to manuals, system documented information can also include non-order related protocols and a list of employees with specific competences. Order-related documented information can, for example, include: confidentiality declarations geared to an order, a list of employees involved in an order, and order-related instructions.

NOTE 2 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

The organization shall plan, implement and control the processes needed to meet security requirements, and to implement the actions determined in 6.1, by:

a) establishing criteria for the processes;

b) implementing control of the processes in accordance with the criteria;

c) keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are controlled.

This control needs to be identified within the security printing management system.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

c) when the monitoring and measuring shall be performed;

d) when the results from monitoring and measurement shall be analysed and evaluated.

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

The organization shall evaluate the security printing performance and the effectiveness of the security printing management system.

The organization shall plan and implement the inspection, test, measurement, analysis and evaluation needed to:

— ensure processes meet security requirements;

— ensure the security printing management system works as planned;

— improve the operation and results of the security printing management system.

Additionally, the organization shall:

1) take action when necessary to address adverse trends or results before a nonconformity occurs;

2) monitor customers' opinion on the fulfilment of security requirements and determine how to gather and use this information;

3) 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 on whether the security printing management system

a) conforms to

   1) the security manual,

   2) the organization's own requirements for its security printing management system,

   3) the requirements of this International Standard;

b) is effectively implemented and maintained.

The organization shall:

— plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting; the audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;

— define the audit criteria and scope for each audit;

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

— ensure that the results of the audits are reported to relevant management, and

— retain documented information as evidence of the implementation of the audit programme and the audit results.

NOTE ISO 19011 contains guidance for internal auditors.

The organization shall define in a documented procedure:

— the responsibilities and requirements for planning and conducting audits;

— how results are reported; and

— how documented information is maintained.

Top management has the responsibility to take corrective actions without undue delay.

Follow-up activities shall include verification of the actions taken and the reporting of the verification results.

9.3 Management review

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

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the security printing management system;

c) information on the security printing performance, including trends in

   1) nonconformities, preventive actions and corrective actions,

2) monitoring and measurement results,

3) audit results, and

4) customer feedback;

d) opportunities for continual improvement and necessary changes to the security printing management system, security policy and security objectives.

The outputs of the management review shall include decisions and actions related to continual improvement opportunities and any need for changes to the security printing management system.

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

10 Improvement

10.1 Nonconformity, security breaches and corrective actions

When a nonconformity or a security breach occurs, the organization shall:

a) identify nonconformity and security breaches;

b) react to the nonconformity, and as applicable

1) take action to control and correct it,

2) deal with the consequences, and

3) inform the customer;

c) react to the security breaches, and as applicable

1) deal with the consequences,

2) inform the customer;

d) implement any action needed;

e) review the effectiveness of any corrective action taken; and

f) make changes to the security printing management system, if necessary.

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

The organization shall retain documented information as evidence of

— the nature of nonconformities and security breaches and any subsequent actions taken, and

— the results of any corrective action.

10.2 Preventive actions

The organization shall take action to eliminate the causes of potential nonconformities and security breaches in the processes in order to prevent their occurrence.

Preventive actions shall be appropriate to the effects of the potential nonconformities and security breaches.

The organization shall retain documented information as evidence of:

a) the nature of the potential nonconformities and security breaches and their causes;

b) the need for subsequent actions to prevent occurrence of nonconformities and security breaches;

c) the results of any preventive actions.

NOTE It may be useful or necessary in certain cases to take preventive actions based on a risk assessment.

10.3 Continual improvement

The organization shall continually improve the suitability, adequacy or effectiveness of the security printing management system.

The organization shall strive to continually improve the effectiveness of the security printing management system through the use of the security policy, security objectives, audit results, data analysis, corrective and preventive actions and management review.

Annex A
(normative)

Determination of security requirements related to the security printing management system

A.1 Infrastructure

The organization shall determine, provide and maintain the infrastructure needed to achieve conformity to security requirements.

Infrastructure includes, as applicable:

a) buildings, workspace and associated utilities;

b) process equipment (both software and hardware); and

c) supporting services (like transport or communication).

A.2 Work environment

The work environment of the organization shall not interfere with the ability of employees to perform effectively in order to meet security requirements.

NOTE An appropriate work environment refers to an area that is secured against breaking in and entering, eavesdropping, scrutinizing (from the outside) or the presence of unauthorized personnel.

A.3 Organizational processes

A.3.1 Determination of security requirements

The organization shall ascertain:

a) security requirements specified by the customer, including the security requirements for delivery activities;

b) security requirements not stated by the customer but necessary for specified or intended use, where known;

c) security requirements set by law and regulations related to the product;

d) any additional security requirements determined by the organization.

A.3.2 Review of security requirements related to the production process

The organization shall review security requirements related to the production process. These security requirements shall be reviewed prior to the organization's commitment to supply the product to the customer. At least specific arrangements with regards to security are made between the organization and the customer.

This review shall ensure that:

a) the customer is authorized to order the product;

b) product and security requirements are defined;

c) these security requirements are known and understood;

d) any changes from the original contract or discussions are understood;

e) the organization has the ability to meet the security requirements;

f) the identity and reliability of the potential customer is checked.

Documented information of the results of the review and actions arising from the review shall be maintained.

Where the customer provides no documented statement of security requirements, the security requirements shall be confirmed by the organization before acceptance.

Where changes are made to orders that have a consequence on the implementation and scope of security, the relevant documented information is amended and personnel involved in the organization shall be informed about these changes.

A.3.3 Communication

The organization shall put in place effective secure communication channels, to allow dialogue regarding:

a) product information related to security;

b) enquiries, contracts, order handling, changes; and

c) customer feedback, including complaints.

Unauthorized disclosure of information shall be avoided.

A.4 Purchasing

A.4.1 Purchasing process

The organization shall ensure that purchased security products and services meet the specified security requirements. The type and extent of control applied to the supplier and purchased product shall depend upon the security requirements established by the procuring organization.

The organization shall evaluate and select suppliers based on the suppliers' ability to provide products and services that meet order specifications and security requirements.

The organization shall establish security criteria for selection, evaluation and re-evaluation of suppliers.

Documented information of evaluations with regards to security and actions arising from the evaluations shall be securely maintained.

A.4.2 Purchasing information

When contracting any outside sources, an organization shall describe clearly and unequivocally:

a) security requirements for the products, procedures, processes, personnel and equipment;

b) requirements for the supplier's security management system.

The organization shall ensure adequacy of purchasing requirements before sending them out to the supplier.

A.4.3 Verification of purchased products

The organization shall establish and implement the inspection or other activities necessary for ensuring that the purchased product meets specified security requirements.

If the organization or its customer intends to perform verification at the supplier's premises or other activities necessary for ensuring that specified security requirements are met, the way in which this is carried out shall be specified in the product information.

A.5 Production and service provision

A.5.1 Control of production and service provision

The organization shall plan and carry out production and service provision under controlled security conditions.

These controlled security conditions should include, but are not limited to:

a) physical security of production;

b) information security;

c) availability of information regarding product and security requirements;

d) the implementation of monitoring regarding security;

e) criteria for product release regarding security.

A.5.2 Identification and traceability

The organization shall establish procedures to identify a product and determine what security requirements pertain to it as it moves through the production process.

The organization shall identify the product status with respect to security requirements.

If traceability is a requirement, the organization shall control and record the unique identification of the product.

A.5.3 Customer supplied material and information

The organization shall maintain security-related customer supplied material and information for use or incorporation into the product in a secure manner relative to its security value. The organization shall report to the customer if any customer supplied material and information is lost, damaged or found to be unsuitable for use and shall maintain documented information.

Customer information of a secure nature shall be maintained in a similar manner.

Customer supplied material and information shall be stored, destroyed or returned to the customer as directed.

A.5.4 Preservation and delivery of product

The organization shall preserve the product, including identification, handling, storage, packaging, protection, and secure delivery of parts and products throughout all processes.

A.5.5 Waste management

To prevent unauthorized use, the organization shall set up a documented procedure which establishes the handling, identification, control and destruction of nonconforming products, semi finished products and waste. The controls, related responsibilities and authorities for dealing with the destruction of waste shall be defined.

Documented information shall be kept to provide evidence that the waste was destroyed in appropriate method unless otherwise specified by the customer.

Bibliography

[1] ISO Guide 73:2009, *Risk management — Vocabulary*

[2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 19011, *Guidelines for auditing management systems*

[4] ISO 31000, *Risk management — Principles and guidelines*

ICS 37.100.01

Price based on 20 pages