

---

---

## Graphic technology — Management of security printing processes

*Technologie graphique — Management des procédés d'impression de  
sécurité*

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO 14298:2013

<https://standards.iteh.ai/catalog/standards/sist/23605595-96bd-4895-a30c-2203b0d66349/iso-14298-2013>



**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO 14298:2013

<https://standards.iteh.ai/catalog/standards/sist/23605595-96bd-4895-a30c-2203b0d66349/iso-14298-2013>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Context of the organization</b> .....	<b>5</b>
4.1 Understanding the organization and its context.....	5
4.2 Understanding the needs and expectations of interested parties.....	5
4.3 Determining the scope of the security printing management system.....	6
4.4 Security printing management system.....	6
<b>5 Leadership</b> .....	<b>7</b>
5.1 Leadership and commitment.....	7
5.2 Policy.....	8
5.3 Organization roles, responsibilities and authorities.....	8
<b>6 Planning</b> .....	<b>9</b>
6.1 Actions to address risks and opportunities.....	9
6.2 Security objectives and planning to achieve them.....	9
6.3 Security printing management system planning.....	10
<b>7 Support</b> .....	<b>10</b>
7.1 Resources.....	10
7.2 Competence.....	10
7.3 Awareness.....	11
7.4 Communication.....	11
7.5 Documented information.....	11
<b>8 Operation</b> .....	<b>13</b>
<b>9 Performance evaluation</b> .....	<b>13</b>
9.1 Monitoring, measurement, analysis and evaluation.....	13
9.2 Internal audit.....	14
9.3 Management review.....	14
<b>10 Improvement</b> .....	<b>15</b>
10.1 Nonconformity, security breaches and corrective actions.....	15
10.2 Preventive actions.....	15
10.3 Continual improvement.....	16
<b>Annex A (normative) Determination of security requirements related to the security printing management system</b> .....	<b>17</b>
<b>Bibliography</b> .....	<b>20</b>

## 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](http://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](http://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*.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO 14298:2013

<https://standards.iteh.ai/catalog/standards/sist/23605595-96bd-4895-a30c-2203b0d66349/iso-14298-2013>

# 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.

## **iTeh STANDARD PREVIEW** **(standards.iteh.ai)**

ISO 14298:2013

<https://standards.iteh.ai/catalog/standards/sist/23605595-96bd-4895-a30c-2203b0d66349/iso-14298-2013>

# 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.