INTERNATIONAL STANDARD

ISO 22388

First edition
2023-11

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for securing physical documents

Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Lignes directrices visant à sécuriser les documents physiques

Reference number
ISO 22388:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

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 document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Documents perform key functions in economic, legal and social transactions, including but not limited to financial interactions, ownership titles, title transfers, transportation, identity verification, customs transactions, academic records, professional licences and gun permits. These roles make them a target for counterfeiting, alteration and other forms of fraud, thereby potentially reducing the reliability of such transactions and creating economic, human and social hazards.

This document is intended to support the review of physical documents used in all kinds of usage contexts and to enable evaluation of physical document designation. Such evaluation also involves assessment to determine risk levels from the most common forms of attack, with consideration of the type and number of security features to be incorporated into documents for authentication. Based on such review and evaluation, these guidelines are expected to serve as guidelines for securing all designated security documents (SDs).

It is important to consider the usage of physical documents for threat and risk assessment and for determining their classification. Common documents can carry a high level of risk when used for critical functions. These guidelines assist in performing risk assessment for various document categories, but they are not intended to identify all potential uses of the documents.

This document is intended to support users and producers in determining security recommendations for documents produced or procured, to establish a relative classification of their documents and to enhance the reliability of transactions supported by such documents.

It should be acknowledged that these guidelines provide guidance on common risks, threats and mitigation treatments at the time of publication. As the security risks to physical documents are constantly changing, so are the mitigating security technologies. Therefore, it is important that users of these guidelines recognize that the risk and mitigation rates are relative and can change based upon a change in risk and the evolution of security technologies to mitigate that risk. It is recommended that the user of these guidelines understands the concepts used in developing a security risk assessment and performs an evaluation of any appropriate newly developed security technologies to establish the most effective solution.

Examples of risks that are not addressed in this document:

— technical risks arising, for example, when applicable security tools are applied improperly;

— management risks relating to document examination from inadequate or no supervision, or lack of training of personnel assigned to examine documents;

— organizational risks, including illegal collection of data from examined documents or insiders who deliberately overlook counterfeit documents in exchange for economic gain or as a part of a criminal enterprise [e.g. security staff allowing under-age entry based on counterfeit identification (ID), internal fraud at licensing agencies where personnel consciously overlook counterfeit ID to issue valid ID];

— external risks meaning impacts outside the control of affected organizations (e.g. power outages or short-term equipment failure);

— compliance risks occurring when a company fails to comply with mandated laws or regulations, which can result in fines or legal actions.

This document has been developed on the basis of concepts and methodologies adapted from Reference [7].

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for securing physical documents

1 Scope

This document gives guidance on how to secure physical documents for specifying entities of physical documents. It establishes a procedure for security design, which includes:

- risk assessment;
- determination of document classes;
- introduction of security features;
- security evaluation;
- document risk mitigation.

This document is applicable to secure physical documents that are used for important actions such as validating value transactions, providing access, demonstrating compliance and securing products.

This document does not apply to banknotes, machine-readable travel documents, driving licences, postage stamps, tax stamps, health cards or national identity cards covered by existing standards and regulations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
document fraud
wrongful or criminal deception that utilizes *security documents* (3.4) for financial or personal gain

Note 1 to entry: Fraud means wrongful or criminal deception intended to result in financial or personal gain that creates social or economic harm.

Note 2 to entry: Fraud includes false use that does not necessarily involve the recreation of documents (e.g. an impostor, using someone else's ID for impersonation).

Note 3 to entry: Fraud related to digitally transmitted electronic media should be considered separately.

3.2
risk communication
exchange or sharing of information about risk between an issuer and other interested parties

Note 1 to entry: The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk.

[SOURCE: ISO 22300:2021, 3.1.220, modified — Definition revised.]

3.3
forensic
<physical document> application of scientific methodologies for authenticating documents by confirming a *security feature* (3.6) or an intrinsic attribute through the use of specialized equipment by a skilled expert with special knowledge

3.4
security document
SD
document protected by a combination of features selected to mitigate the risk of counterfeit

3.5
specifying entity
person or organization who defines the requirements for authentication solution to be applied to a particular *security document* (3.4)

3.6
security feature
feature of a document that is linked to a specific method of verification and thus helps ensure the document's integrity and/or authenticity as a properly issued document, including that it has not been tampered with

[SOURCE: ISO/IEC 18013-1:2018, 3.27]

3.7
blank document
document ready to personalize after uniformed background printing on the substrate

Note 1 to entry: Background printing often includes *security features* (3.6).

4 Document security principles

4.1 User's category

In relation to the document authentication, potential users are categorized as follows:

- General: SD holders and third-party related users performing document processing.
- Specific: counter staff, document checkers and others providing prescribed services, with true-false check, based on issuer-defined document functions.
- Authorities and experts: parties setting SD specifications, staff at official investigative and analytical organizations with verification expertise, and other inspectors with deep knowledge of security specifications.

The specifying entity should specify document security considering the user resources shown in Table 1. See also Table D.1.

Table 1 — Users and resources

Users	Resources		
	Time available for inspection[a]	Expertise or training	Access to inspection tools
General	Limited	Limited or none	Limited or none
Specific	Medium	Medium	Medium
Authorities and experts	Extensive	Extensive	Extensive

[a] For a correct inspection, the inspection time required should match the user availability.

4.2 Document stages

The specifying entity should use the following stages when describing the life cycle of an SD, see also Figure 1:

- Security design, which is the incorporation of security measures against various types of document fraud that threaten each process in the document life cycle. This process includes review and improvement of document security.
- Blank document production, which includes the implementation of specifications related to design and the overall manufacturing process, including the acquisition of raw materials, production, quality checking, testing, storage and, operationally, transportation to a personalization entity.
- Personalization, which incorporates the integration of variable content such as monetary values, personal qualification information and credentials for certification elements on blank documents as required by the issuer.
- Issuance, which is the act of delivering an SD to a validated entity.

  NOTE Delivery involves the secure transportation of the SDs to the intended entity.
- Service lifetime, which is the length of time the document maintains its document function, including its security effectiveness.
- Revocation, which is the intentional discontinuation and disposal of SDs by an authorized entity. Documents are subjected to physical processes, such as stringent disposal to prevent reuse, printing, perforation and other acts, thereby ensuring discontinuation.

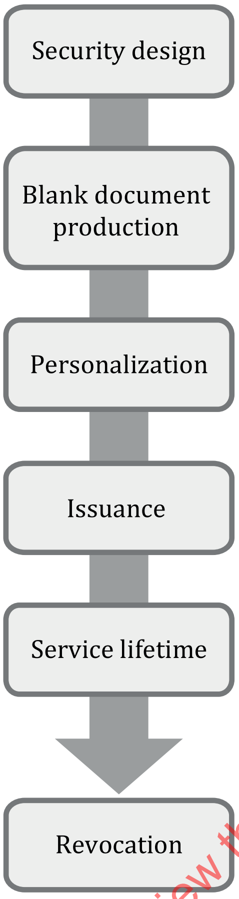

Figure 1 — Document linear progression stages

4.3 Elements to be protected

The specifying entity should protect the following from various threats:

- SDs (during all life cycles): SDs should be highly resistant to counterfeiting and should be verifiable. Official copies of SDs produced by photocopying or other means should be clearly marked as such.
- Manufacturing processes, including production, personalization and issuing processes.
- Integrity of recorded information: information recorded on SDs and related security features should remain in the original state provided by the issuer supported by the appropriate anti-counterfeiting or tampering features, which requires physical and chemical resistance. The counter measures should enable detection of fraudulent alterations such as data deletion, modification and overwriting.

Personalization impacts privacy; accordingly, designers and developers should apply the requirements of ISO 31700-1. Privacy protection is a matter of regulation in many jurisdictions.

4.4 Considerations for security manufacturing

The specifying entity should consider the following when designing and manufacturing SDs and in the setting of security features:

- Materials: composition, formulation and manufacture of raw materials used for security features should be securely controlled and materials should not be readily available to those attempting to fraud.

- Manufacturing machinery: devices used to provide and produce security features should be securely controlled and should not be readily available.
- Production methods: methods for the production of security features should be securely controlled.

NOTE 1 ISO 14298 provides guidance on the specifying entity for the management of security processes such as manufacture, storage, distribution and accountability.

- Principles: the principles, mechanisms and specifications of security features should be maintained in a secure and confidential manner.
- Quality stability: variances in quality among SDs at the time of security feature implementation and production should be minimized to prevent false counterfeit identification.
- Durability: SD authentication should be possible regardless of changes in appearance through use and aging (including individual differences present at the time of production).

NOTE 2 Securely controlled means materials and processes are controlled under accepted security practices such as ISO 14298 and Reference [8], or equivalent accepted security industry practices.

5 Document security design

5.1 General

The specifying entity should follow the security design procedure outlined in Figure 2 to manage risk associated with misuse or fraud aligned to ISO 31000 when developing the specification for SDs.

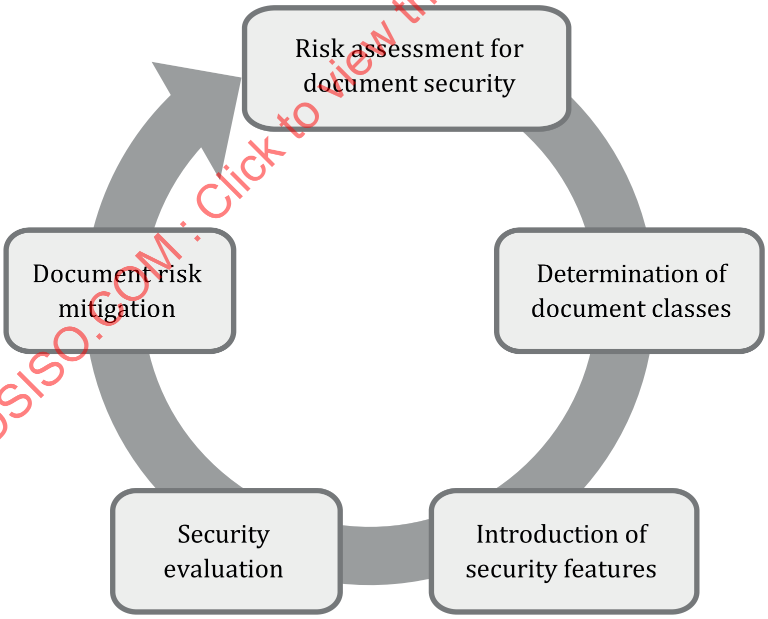
Risk assessment for document security
Determination of document classes
Introduction of security features
Security evaluation
Document risk mitigation

Figure 2 — Security design procedures

5.2 Risk assessment for document security

5.2.1 Estimation of risk

The specifying entity may perform a risk assessment on a document when an initial review indicates the possibility of fraud or misuse and the potential impacts if sources of risk are not mitigated. Where possible, the risk assessment methodology should draw on quantitative data and, where there are degrees of uncertainty, recognize qualitative estimation as a guide for the assessment and be performed in consideration of:

- four modes of document fraud;
- intention and capability of known or potential threat actors;
- specific risk factors derived from document purpose, use, distribution and validity period.

NOTE An example of risk rate estimation for a general SD is provided in Annex A.

5.2.2 Four attack enablers of document fraud

Document fraud is generally divided into the following four modes of attack:

- Cloning: reproduction of original including security features employing the same base components and manufacturing techniques as the original. In this scenario, a party unauthorized to issue the document uses materials equivalent to or similar to the genuine versions, imitates the internal structure and creates a counterfeit with an appearance and characteristics similar to the original. Cloning is usually based on reverse engineering.
- Facsimile: an unauthorized reproduction of the original, including security features made with base components and manufacturing techniques different from those of the original version, but with an appearance being able to mislead the inspector. The internal structure and characteristics are not necessarily similar to those of the original.
- Alteration: changes made to a legitimate item, including deletion and insertion, replacement of genuine content and illegal rewriting of printed information or patterns.
- Theft or public acquisition (PA): the ability to readily obtain original security features by illicit or legitimate means.

NOTE Theft or PA is a protective security measure for physical handling control of the environment, which is not a characteristic of the document but rather an enabler of fraud.

5.2.3 Types of threat

One or more threats occur when a threat actor chooses to attack the document to gain advantage or reward. The success of such an attack is predicated on the threat actor having the intent and capability to cause harm. A potential attack can come from individuals or organized groups of varying size and can include:

- issue-motivated activist organizations;
- politically motivated groups or states;
- criminal organizations;
- opportunists or individuals seeking gain;
- insiders.

A threat actor's intent (motives and objectives) can be multiple or overlap (e.g. a terrorist group seeking both political or national advantage and conducting fraud to finance their operations). Intent can be driven by a range of motivations, including:

- revenge;
- financial gain;
- political advantage;
- reputation of threat actor or victim.

5.2.4 Document-specific risk factors

The following factors affect document risk:

- Frequency of usage: risk depends significantly on how often documents are used.
- Availability: vulnerability and threat depend significantly on whether the documents are accessible and how they are distributed.
- Validity period: risk increases throughout service lifetime.
- Credibility: documents issued by a reputable organization and representing a high perception value can increase the risk of fraud.
- Third-party authentication: verification should be conducted by authorized, trained individuals with the appropriate tools.

5.3 Determination of document classes

The specifying entity should determine the document class of the document:

- high-risk document;
- moderate-risk document;
- low-risk document.

Classes of documents with similar functions provided by different issuers should be uniform to ensure risk communication among interested parties concerning document security. Table 2 includes examples of documents belonging to each class.

Table 2 — Document classes and examples

Document class	Examples
High-risk document	Access to secure or critical resources (security access), important privileges, negotiable instruments
Moderate-risk document	Security-control access documents, certificates of title, certificates of origin, negotiable documents of moderate value, identity credentials, gun permits, professional licences
Low-risk document	Low-value event tickets, loyalty cards, temporary identity documents, low- or medium-value product coupons, gift cards, non-security access documentation

5.4 Security features

5.4.1 Physical security features — Selection and design

The specifying entity should use security features to mitigate the risk of typical document fraud types such as cloning, facsimile, alteration and theft or PA. Security features are categorized as, for example, substrates, printing, inks or personalization, as shown in Annex C. Definitions for each security feature are also provided in Annex E and Reference [7]. The specifying entity should fully consider authentication levels as described in Annex D. It is also important to evaluate resistance against each fraud type and the resources, such as authentication equipment, time and people expertise required. The process diagram that should be used as a further reference when designing the authentication solution is provided in ISO 22383:2020, Figure 2.

The efficiency of the selected security feature depends on several elements that should be taken into account when devising the performance criteria for a secure document. These include but are not limited to the purpose of the document, the number of security features used, the quality of the security feature(s), the quality of the implementation of the feature(s) and the expertise of verification.

Therefore, the specifying entity should make these aspects part of the contractual agreement. A quality indication can be the certification of either the supplier or printer or both according to ISO 14298 or Reference [8]. In any case, it is recommended that a knowledgeable document security expert assists in the selection and use of the features for the specific document.

5.4.2 Digital security features

5.4.2.1 General

The specifying entity should be aware that digital and physical security features can be advantageously combined together on the same document to provide a highly effective resilience capacity document. Information can concern data derived from the physical layer as well as the information related to digitally generated features and/or personalization data.

5.4.2.2 Physical-digital features

The specifying entity should consider that physical documents can also be secured digitally. This is achieved by deriving data from a physical feature of the document. Such a derivation creates an association which can be used effectively to evaluate the relationship between a physical document and a corresponding digital representation.

There are two different categories of digital protection for physical documents that depend on how the data set and physical features of the document are related, as follows:

— Protection via the physical layer of the document: a set of data is derived from one or more naturally occurring distinguishing characteristics of the document.

— Protection via digitally generated features: a set of data is combined with the document in some way (e.g. printed or embedded) at the time of its manufacture. This can be covert or overt.

NOTE The term “phygital” can be used to indicate technologies (including security features) that link a digital entity to its physical counterpart.

5.4.2.3 Data integrity check

The specifying entity should consider that the data set present on the document can be protected from alteration using a data integrity check. A data set is generated by processing information derived from the document or its personalization in a way that these data can be checked against a digital signature or digital seal.

Data corresponding to the information on the document can be included as a personalized mark [e.g. a two-dimensional (2D) barcode, radio-frequency identification (RFID) chip], including or related to a digital signature or linked to an immutable data record (such as, but not limited to, blockchain solutions). Due to this immutability, the data are protected against modification. Any alteration of the data (including information concerning the authoritative source) can be detected by the reading devices.

Such digitally secured documents with protected data can be copied; however, any modification can be easily detected. Thus, each digitally secured copy of the document can act as an original.

The name or reference of the issuer of the document is often included in the digital seal, allowing the reader to authenticate and verify the legitimacy of the issuer.

These digital security features can be combined together on the same document, for example it is possible to include any information concerning the authentication data of the physical layer and hidden digitally generated features within the digital seal. Such combined data can be captured, encrypted and stored as distributed ledger technology or related to a digital signature.

5.5 Developing a risk rating

It is possible to use a model risk assessment process as a representational rating tool to provide an indicative risk rating based on the relationship between:

- the intentions and capabilities of a threat actor;
- the vulnerabilities of a document and any factors from proposed use;
- the likelihood of an attack occurring;
- the degree impact or consequences if an attack were to occur.

Analysis of these relationships provides an estimate of the level of risk of a positive or negative outcome. Figure 3 summarizes the process of the evaluation of the risk levels.

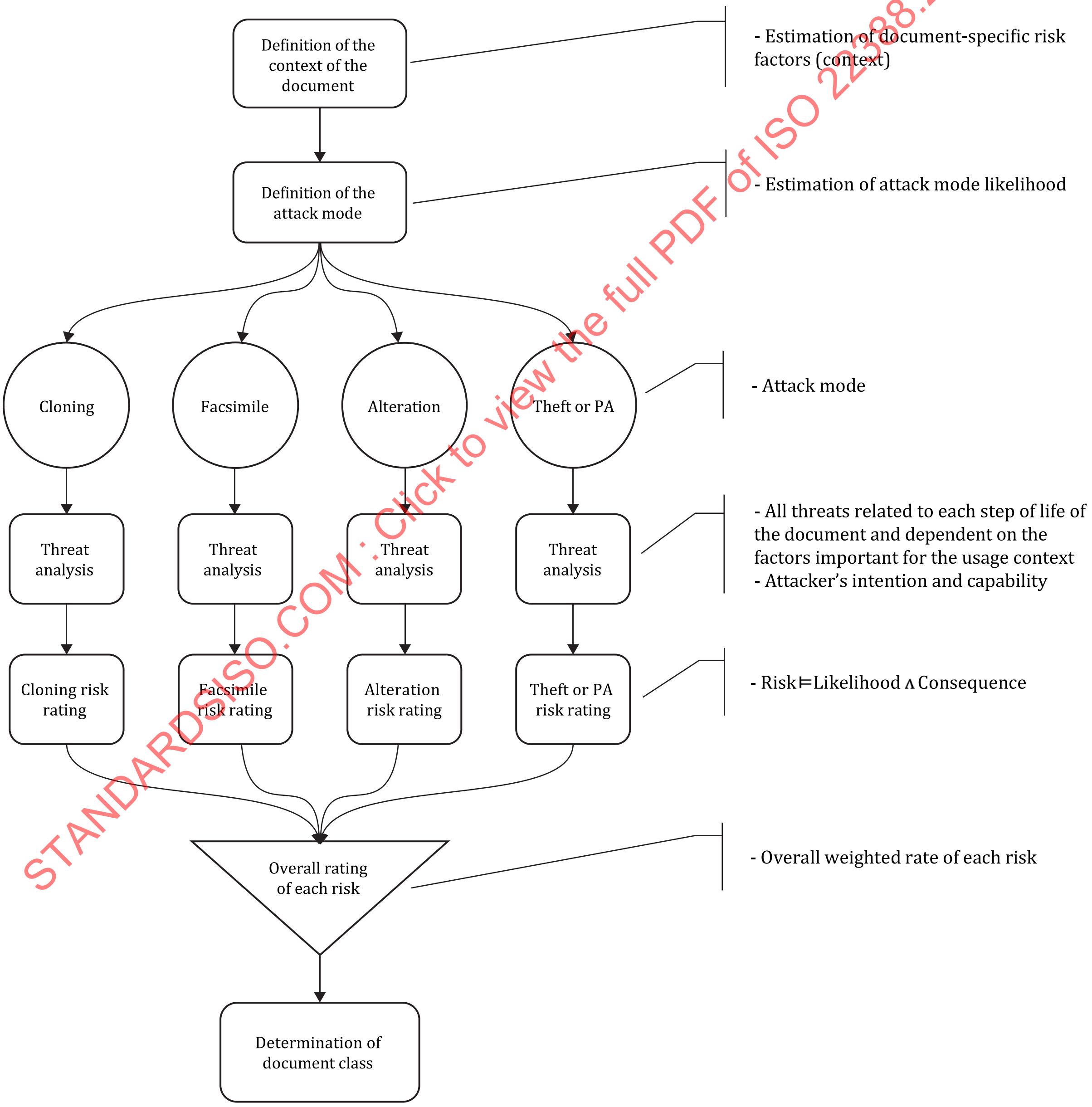
Definition of the context of the document
- Estimation of document-specific risk factors (context)
Definition of the attack mode
- Estimation of attack mode likelihood
Cloning
Facsimile
Alteration
Theft or PA
- Attack mode
Threat analysis
Threat analysis
Threat analysis
Threat analysis
- All threats related to each step of life of the document and dependent on the factors important for the usage context
- Attacker's intention and capability
Cloning risk rating
Facsimile risk rating
Alteration risk rating
Theft or PA risk rating
- Risk⊨Likelihood ∧ Consequence
Overall rating of each risk
- Overall weighted rate of each risk
Determination of document class

Figure 3 — Evaluation of the risk levels

The specifying entity should determine a level for the resistance of security features for each of the four attack modes in order to establish the appropriate set of security features for the corresponding document class. Figure 4 explains the process that should be used to determine a proper set of security features in order to ensure a good protection of the document, well adapted to the document class.

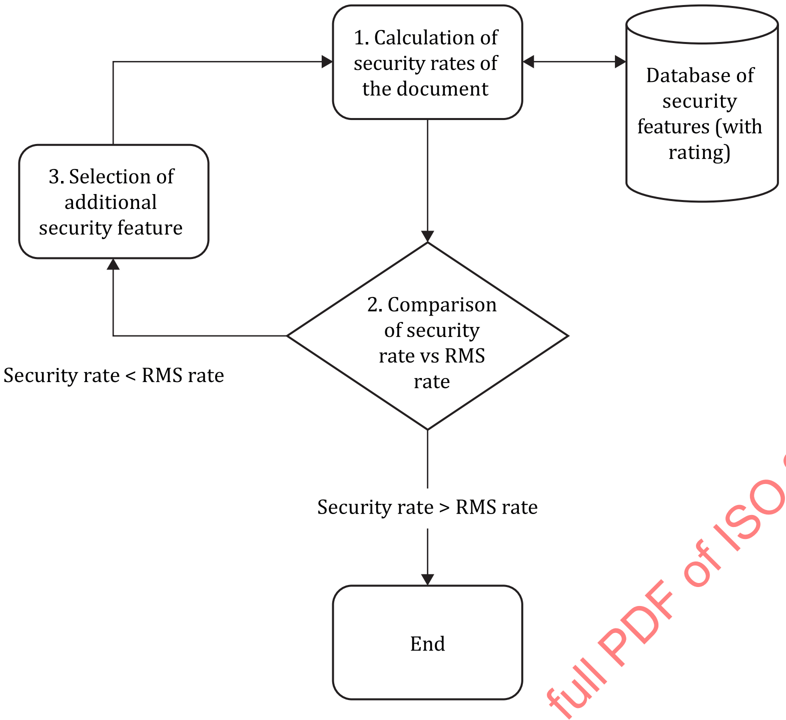
1. Calculation of security rates of the document
Database of security features (with rating)
3. Selection of additional security feature
2. Comparison of security rate vs RMS rate
Security rate < RMS rate
Security rate > RMS rate
End

Figure 4 — Security design process

The recommended minimum security (RMS) rates are the overall resistance by attack mode of selected security features that should be implemented in a given document. The specifying entity and the manufacturer should fully agree on the RMS rates with reference to the results of the risk rating. Examples of a selection of security features and RMS rates are given in Annex B.

Annex C provides an example of rating criteria for security features, the process and rates by attack mode for each of the categorized security features. The specifying entity should use Annex C as a reference for rating the emerging technologies that are not on the list or for features with special resistance to some attack type.

Resistance provided by security features is a function of the application of controls to reduce vulnerability. This rating should be either a qualitative rating from estimation or a semi-quantified rating derived from testing the level of protection of the types of controls from attack. Such security ratings should be considered against the likelihood and impact of an attack by one or more of the attack modes. Where the control, alone or in combination, provides reduction of risk to an acceptable level, the control should be adopted. See the examples given in Annex B.

5.6 Security evaluation

In addition to the specifying entity, multiple parties with relevant expertise in security evaluation and analysis or judgement should evaluate how the completed SDs (including prototypes and security design plans) conform to various security performance criteria. This should include an adversarial testing process based on estimated counterfeiting resources such as person-hours, equipment, materials and counterfeiting expertise considering various document fraud types. Results should be shared with issuers as appropriate to establish risk communication.

Security considerations should include the following:

- Layering of technologies: a technique in which single security features can incorporate a combination of overt, covert and forensic authentication capabilities.

- Complementary implementation: the use of multiple technologies to achieve a degree of mitigation greater than the individual technologies.
- Multi-modal methods: embossing, laser processing, pressure bonding (e.g. lamination, foil pressing) and other techniques, in addition to production with printing techniques based on inks and form plates.

5.7 Document risk mitigation

The security specifications based on this document are intended to mitigate the counterfeit risk to the SD. Since it is difficult to predict the emerging types of document fraud that can reduce the reliability of SDs, specifying entities should take appropriate actions guided by their risk analysis, such as updating each security feature and renewing the security design of the document.

Annex A
(informative)

Risk assessment for security documents

A.1 General

When developing an SD or physical document, the specifying entity should identify the associated risks, utilizing their organization's risk framework (described in this annex for reference) and the attack enablers in this document to determine the document class and then select appropriate treatments or controls to minimize the risk to an acceptable level. This annex provides guidance to the application of risk assessment methodologies and is derived from the process model in ISO 31000 outlined in Clause A.2 and Figure A.1. Each element of the process should be addressed effectively to manage document risk and the outline given in Clause A.2 should be expanded for the specific document context. The matrix examples provided in this annex are not directly related to the assessment established in this document and are demonstrated as examples of the methodology.

Some of these elements, such as organizational operating environment, organizational management and assets, risk criteria and records policy, should already be done as part of the specifying entity's risk framework and are not specific elements for each document. Also, what the specifying entity identifies under their risk framework does not necessarily reflect the consumers expectations or criteria, for example tolerance and appetite levels.

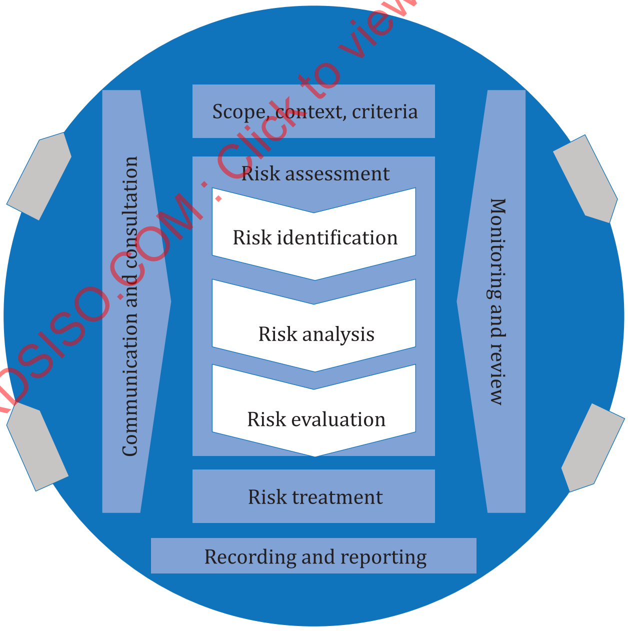

Figure A.1 — ISO 31000 risk management process element

A.2 Process model in ISO 31000

A.2.1 General

The outline of the process model in ISO 31000 is as follows:

- Scope:
  - security applications to achieve document objectives;
  - governance, policy and processes.
- Context:
  - organizational operating environment;
  - organizational management;
  - the organization's assets;
  - validation of internal and external interested parties.
- Risk criteria:
  - determination of agreed levels of risk acceptance and tolerance.
- Communication and consultation:
  - communications strategy;
  - client and interested party requirements;
  - privacy;
  - confidentiality;
  - sources of validation;
  - process guidance;
  - roles;
  - information access and use.
- Document recording and reporting:
  - records policy;
  - records management system;
  - access to documentation;
  - reporting channels.
- Document monitoring and review:
  - accountability;
  - responsibility;
  - consistency;
  - audit;
  - assurance;

- policy and process review.

A.2.2 Document risk assessment and treatment

The processes that the specifying entity should apply when assessing document risk and identifying risk treatments.

A.2.3 Risk identification and evaluation

In identifying and evaluating risks, the specifying entity should consider:

- the value and criticality of sensitive or valuable documents;
- vulnerability of documents and sources of threat;
- the likelihood and the potential for risks to occur.

A.2.4 Risk analysis

In analysing risks, the organization should include:

- impact analysis of harm to, or compromise of, sensitive or valuable assets, including in relation to:
  - economic or financial (e.g. impact on operating budget);
  - legal and regulatory (e.g. non-compliance with legislation, commercial confidentiality, legal privilege);
  - personal (e.g. impact on the personal safety, dignity, finances, liberty or the identity of a person or persons);
  - service delivery (e.g. capacity to operate, deliver services or programmes, reputation, confidence and utilization of services);
- level of certainty in relation to the credibility and timeliness of the available information;
- volatility or rate of change in these variables.

A.3 Semiquantitative risk assessment

A.3.1 General

This annex further provides an example of the application of a semiquantitative risk assessment for an SD derived from quantitative data and allocation of a representational rate to qualitative information. It assumes four attack modes by five threat actor types while considering the document-specific risks assumed in the operation, such as frequency of usage or, validity period.

All the rates indicated in the various tables in this annex result from semiquantitative risk analysis, which is a risk analysis methodology characterized by speed, simplicity of design, a lower requirement on the input data and smaller demands on the resources, including some degree of quantification of consequence, likelihood and/or risk level.

In order to produce an indicative rate for risk, the following factors should be considered:

- intentions and capability of the threat actor;
- vulnerability of the document prior to treatment;
- opportunity for attack;
- impact of an attack should it be successful, and likelihood that such an attack will occur.

This can be represented in a process model where the risk equation is considered from two perspectives of risk management, achieving objectives and avoiding failure, and can be summarized by the following models, noting that any risk accepted can have a blend of positive and negative outcomes:

- risk: likelihood for a beneficial outcome is a function (⊨) of the interaction (∧) of capability and circumstances or opportunity;
- risk: likelihood for a negative outcome is a function of (⊨) of the interaction (∧) of vulnerability and threat or hazard.

NOTE Any of the variables can be modified by application of relevant controls to mitigate the likelihood of a negative outcome.

In generating representative rates for risk, Tables A.1 to A.4 show the application of the matrix approach. They use a five by five matrix, which allows for a distribution of rates on an arithmetic sequence, since there is a common difference between each term. In this case, adding 1 to the previous term in the sequence gives the next term. In other words, $a_n = a_1 + (n - 1)\,d$, with an arithmetic sequence of $d = 1$. This is the formula of a single unit arithmetic sequence. This approach avoids a misleading exponential scale in rating with sufficient differentiation to provide representative difference when considering both the threat levels in Table A.1 and the risk levels in Table A.4.

A.3.2 Threat matrix

A threat matrix may be used to generate a representative rate for the convergence of intentions of an attack and their capability to exercise the threat. For example, a threat actor with a low rate on intention (2) and a medium rate on capability (3) will rate 4 for threat, and an actor with a high rate on intention (4) and a high rate on capability (4) will rate 7, see Table A.1. The rating on the matrix can be colour coded to illustrate the threat levels, see Table A.2.

Table A.1 — Threat matrix example

Intention	Capability				
	Negligible – 1	Low – 2	Medium – 3	High – 4	Very high – 5
Very high – 5	5	6	7	8	9
High – 4	4	5	6	7	8
Medium – 3	3	4	5	6	7
Low – 2	2	3	4	5	6
Negligible – 1	1	2	3	4	5

Table A.2 — Threat matrix colour-coded example

Intention	Capability				
	Negligible – 1	Low – 2	Medium – 3	High – 4	Very high – 5
Very high – 5	5	6	7	8	9
High – 4	4	5	6	7	8
Medium – 3	3	4	5	6	7
Low – 2	2	3	4	5	6
Negligible – 1	1	2	3	4	5

A.3.3 Likelihood model

The likelihood of an event is derived from the estimated percentage of potential occurrence and its chance of success. Table A.3 provides the rating model. On the basis of observation, a representative rate can be estimated and used in combination with the threat rate to populate a risk matrix. When a control is allocated to decrease vulnerability or reduce the threat it will cause variation to the likelihood rate.

Table A.3 — Likelihood model

Intention	Representative rate	Expected or actual frequency
Very high – 5	5	Can be expected to occur in most circumstances
High – 4	4	Will probably occur in most circumstances: 50 % to 75 % chance of occurring
Medium – 3	3	Can occur: 25 % to 50 % chance of occurring
Low – 2	2	Can occur sometimes: 25 % chance of occurring
Negligible – 1	1	Can only occur in exceptional circumstances

A.3.4 Risk matrix model

To establish an initial risk measure, the representative rates for likelihood and impact or consequence are entered into the risk matrix. In this case, the likelihood rate is multiplied by the impact rate to provide a rating for risk to differentiate levels. This is representational and a rate of 25 means that the risk is of order requiring attention compared to a rating of 4. These rates are not real numbers and should not be aggregated. For example, where a document has variable levels of risk depending on the nature of the attack, the highest rate remaining after the application of controls is the risk rating.

Table A.4 — Risk matrix example

Likelihood	Impact				
	Negligible – 1	Minor – 2	Moderate – 3	Major – 4	Catastrophic – 5
Certain – 5	5	10	15	20	25
Very likely – 4	4	8	12	16	20
Likely – 3	3	6	9	12	15
Unlikely – 2	2	4	6	8	10
Negligible – 1	1	2	3	4	5

The risk rate (R) for each attack of an SD is a result of the relationship between the likelihood (L) and its impact (I) of each attack as shown in Formula (A.1):

$$R \vDash L \wedge I \tag{A.1}$$

It is sometimes expressed as $R = L \times I$, but high-numbered numerical scales lead to misleading results.

L is evaluated in relative terms using the following subjective expressions and numerical values, with 5 as the maximum:

—	certain	5
—	very likely	4
—	likely	3
—	unlikely	2
—	negligible	1

I is evaluated in relative terms using the following subjective expressions and numerical values, with 5 as the maximum:

—	catastrophic	5
—	major	4
—	moderate	3
—	minor	2
—	negligible	1

A.3.5 Risk treatment

In considering allocation of the residual risk rate to a document, each control chosen should be applied on the basis of the reduction of likelihood of an unwanted outcome.

Where a document is at risk from an attack, including cloning, facsimile, alteration and theft or PA, the application of a control as outlined in Annex B will reduce the overall risk rate either with the application of a single control or multiple controls. In order to consider the risk posed by each form of attack, a threat matrix for the attack on document should be conducted.

For example, an attack using cloning can have an intention of 3 but and a capability of 5, leading to a likelihood rate of 7, a high level of threat. The same threat actor intending to use forgery can have an intention of 4 and a capability of 1 (as a result of low level of access to the document materials), giving a risk rate of 4, a low to moderate likelihood.

The rates thus derived are reviewed and, depending on the level of risk acceptance, those with a high rate should be treated.

NOTE Rates thus derived are not aggregated to produce an overall rate.

A.4 Examples of risk rate and class determination

An example of using the risk matrix (see Table A.4) to calculate the risk rate for each document class is shown in Tables A.5, A.6 and A.7.

Table A.5 — Calculation of an example risk rate for a high-risk document

Attack mode	Likelihood	Impact	Risk rate	Consequences
	L	I	R	
Cloning	4	5	20	Human harm, liability, financial loss, loss of credibility, compromised identity, systems failures
Facsimile	3	5	15	
Alteration	3	4	12	
Theft or PA	3	4	12	

Table A.6 — Calculation of an example risk rate for a moderate-risk document

Attack mode	Likelihood	Impact	Risk rate	Consequences
	L	I	R	
Cloning	3	3	9	Human harm, liability, financial loss, loss of credibility, compromised identity, systems failures
Facsimile	3	3	9	
Alteration	3	3	9	
Theft or PA	2	3	6	

Table A.7 — Calculation of an example risk rate for a low-risk document

Attack mode	Likelihood *L*	Impact *I*	Risk rate *R*	Consequences
Cloning	2	2	4	Liability, financial loss, compromised identity
Facsimile	2	2	4	
Alteration	2	2	4	
Theft or PA	1	2	2	

The document class may be determined by taking into account which risk level the highest risk rate for each attack mode belongs to. Table A.8 is an example of three-levelling with risk rates from 12 to 25, 5 to 10 and 1 to 4.

Table A.8 — Three-levelled risk matrix

Likelihood	Impact				
	Negligible – 1	Minor – 2	Moderate – 3	Major – 4	Catastrophic – 5
Certain – 5	🟨 5	🟨 10	🟥 15	🟥 20	🟥 25
Very likely – 4	🟩 4	🟨 8	🟥 12	🟥 16	🟥 20
Likely – 3	🟩 3	🟨 6	🟨 9	🟥 12	🟥 15
Unlikely – 2	🟩 2	🟩 4	🟨 6	🟨 8	🟨 10
Negligible – 1	🟩 1	🟩 2	🟩 3	🟩 4	🟨 5

Key

red: high-risk document

yellow: moderate-risk document

green: low-risk document

Annex B
(informative)

Rating system for security controls

B.1 General

This annex provides a way to understand the semiquantitative performance of security features. The performance of a set of security features should be compared and balanced with the RMS described in Table B.1.

Some security technologies require specific expertise for the inspection process, while others do not. It should be considered that the selection of security features should take into account expected inspectors' knowledge, skills and abilities with related documents and technologies. Also, the speed of inspection depends on the use case, such as type and value of the document, risk assessment, ease of control and inspector's resources.

B.2 Rating system

The performance of the security features is expressed as five rates. These correspond to the resistance strength of the four attack modes: cloning, facsimile, alteration and theft or PA. The rates range from 0 to 10, relative to the following subjective expressions:

—	very high	from 9 to 10
—	high	from 7 to 8
—	moderate	from 5 to 6
—	low	from 3 to 4
—	very low	from 1 to 2
—	not applicable	0

Each rating is conducted based on the security considerations described in 4.4. For more details, see the assessment grid in ISO 22383:2020, Annex A. Table C.1 provides an example of rating criteria for technology classification by attack mode. The detailed rating criteria are shown in Table C.1.

B.3 Considerations for security features effectiveness and selection

The quality levels of security features should be established between the specifying entity and the manufacturer through contractual obligations.

The indicative effectiveness of security technologies has been established based upon a class of documents. The class of documents is a direct reflection of the use of a document and the risks associated with those documents. In addition, the established effectiveness levels are based upon a perceived ability of the technology to mitigate the modes of attack described in the risk assessment.

Consideration should also be given to the evaluation of emerging security features and the consequences of evolving threats. This evaluation and rating of technologies can be challenging. In such cases, unique or additional security rating can be done based on the criteria given in Table C.1 by agreement between the specifying entity and the manufacturer, with consideration of similarity to existing technologies.

B.4 Recommended minimum security rate

To ensure a global chain of document security, the specifying entity creating SDs should achieve the RMS rate for each document class listed in Table B.1.

In selecting security features, it is not appropriate to think that simply exceeding the minimum rate is sufficient. The specifying entity should establish security criteria as described in 5.6, taking into account variables such as the authentication level, tools and user resources as described in Annex D.

Table B.1 — RMS rate

Type	Cloning	Facsimile	Alteration	Theft or PA
High-risk document	35 to 55	35 to 55	35 to 55	35 to 55
Moderate-risk document	20 to 40	20 to 40	20 to 40	20 to 40
Low-risk document	10 to 15	10 to 15	10 to 15	10 to 15

B.5 Example of calculating security rates for all document classes

Examples of security rate calculation are shown in Tables B.2 to B.4. At the bottom of each table is the cumulative security rate. The rate is recommended to exceed the RMS rate of the corresponding document class.

Table B.2 — Example of a security rate for a high-risk document (e.g. birth certificate)

Category	Selected technologies	Cloning	Facsimile	Alteration	Theft or PA
Substrate technologies	Two-tone watermark	9	4	3	4
	Chemical sensitivity	5	2	5	3
	Ultraviolet (UV) features	5	2	2	2
Security printing	Duplex patterns	7	4	2	6
	Microprinting or nanoprinting	7	6	0	8
	Copy evident anti-copy pantograph	7	2	5	2
	Optical variable or latent image	8	5	0	8
Security inks	Infrared or UV fluorescent	5	3	5	3
Personalization techniques and technologies	Machine-readable technology	2	2	7	1
	Redundant data	0	0	5	0
	Frequency line modulation image survivable security feature	7	6	4	8
Taggants	Rare earth	8	0	0	8
Diffractive optically variable image devices (DOVIDs)	Transparent DOVIDs	6	5	4	5
Sub-features of DOVIDs	Diffractive watermark	1	1	0	0
Digital security features	Digitally verifiable physical layer protection	9	9	6	9
Cumulative security rates		**86**	**51**	**48**	**67**

Table B.3 — Example of a security rate for a moderate-risk document (e.g. professional certificate)

Category	Selected technologies	Cloning	Facsimile	Alteration	Theft or PA
Substrate technologies	Watermark	8	3	2	2
Security printing	Fine line background (Guilloche pattern)	5	3	2	1
	Copy-evident anti-copy pantograph	7	2	5	2
Security inks	Colour shifting inks	9	3	1	5
Personalization techniques and technologies	Deliberate errors or known flaws	5	3	2	2
	Screen-decoded images	6	5	8	5
DOVIDs	De-metallized DOVID	6	5	2	5
Sub-features of DOVIDs	Overlay ultra-thin security layer (7 µm to 12 µm)	0	0	2	0
Digital security features	Digitally generated protection	9	6	8	8
Cumulative security rates		**55**	**30**	**32**	**30**

Table B.4 — Example of a security rate for a low-risk document (e.g. low value event ticket)

Category	Selected technologies	Cloning	Facsimile	Alteration	Theft or PA
Substrate technologies	Artificial watermarks	4	1	1	1
Security printing	Fine line background (Guilloche pattern)	5	3	2	1
Security inks	Metameric	4	2	1	3
Personalization techniques and technologies	Protective laminate or coating	5	3	3	1
DOVIDs	Metallized DOVID	5	4	1	3
Cumulative security rates		**23**	**13**	**8**	**9**

Annex C
(informative)

Rating criteria for security features

C.1 General

This annex gives rating criteria and security rates to guide the selection of security technologies. The efficiency of the selected security feature depends on several elements that should be taken into account when devising the performance criteria for a secure document. These include but are not limited to the purpose of the document, the number of security features used, the quality of the security feature(s), the quality of the implementation of the feature(s) and the expertise of verification.

Therefore, these aspects should be part of the contractual agreement. A quality and security indication can be the certification of either the supplier or printer, or both, according to ISO 14298 or Reference [8] to the security printing industry or equivalent security-industry-recognized certifications. In any case, it is recommended that a knowledgeable security expert assists in the selection and use of the features for the specific document.

C.2 Security rating criteria

Table C.1 provides rating criteria for each technology category by attack mode. Using these criteria, a grid assuming rating of security technologies is shown in Table C.2.

Table C.1 — Selected rating criteria

Technology category	Cloning	Facsimile	Alteration	Theft or PA
Substrate technologies	a, b, c, h	d, g	e, f	l, m, n, o
Security printing (not variable data)	a, b, c, d, h	d, g	e, f, k	l, m, n, o
Security inks	a, b, c, h	d, g	e, f	l, m, n, o
Personalization techniques and technologies	a, b, c, d, h	d, g	e, f, k	l, m, n, o
Taggants	b, c, k	g	e, f, k	l, m, n, o
DOVIDs	a, b, c, d, h	d, g	e, f,	l, m, n, o
Digital security features	b, c, j, k	d, k	b, c, j, k	m, o

Table C.1 *(continued)*

Technology category	Cloning	Facsimile	Alteration	Theft or PA

Key

a limitations in materials and manufacturing machinery

b limitations in production methods and principles (information asymmetry)

c reverse engineering resistance

d technical superiority for complexity and granularity of design

e tamper evidence or detection or tangible or intangible interdependence

f integral robustness or tamper resistance, including unity or continuity of printing media

g authentication easiness (e.g. expertise knowledge, time, motion, environment, tool)

h authentication accuracy or reliability

i information symmetry

j obsolescence

k side channel resistance or adversarial attack analysis

l padding and diversion

m process control

n internal collusion

o robbery

C.3 Security rating example

Table C.2 shows the qualitative evaluation results (from not applicable to very high) with multi-criteria for each attack mode of security features. In the final rating (from 0 to 10), the specifying entity should consider, for example, detailed comparisons with characteristics of similar security features or their relative position in terms of performance among all technologies in the same category. This process is provided in Figure C.1.

Table C.2 — Rating process

Technology category	Security features	Cloning			Facsimile			Alteration			Theft or PA		
		C	S	R	C	S	R	C	S	R	C	S	R
Substrate technologies	Two-tone watermark	a	VH	9	d	M	4	e	L	3	l	L	4
		b	VH		g	L		f	L		m	L	
		c	VH								n	L	
		h	VH								o	L	

Key

C criterion

S scale

R rate

VL very low

L low

M moderate

H high

VH very high

N/A not applicable

Table C.2 *(continued)*

Technology category	Security features	Cloning			Facsimile			Alteration			Theft or PA		
		C	S	R	C	S	R	C	S	R	C	S	R
Security printing (not variable data)	Duplex patterns	a	H	7	d	L	4	e	VL	2	l	M	6
		b	H		g	L		f	VL		m	M	
		c	H					k	L		n	H	
		d	H								o	H	
		h	H										
Security inks	Colour shift inks	a	VH	9	d	L	3	e	VL	1	l	M	5
		b	VH		g	L		f	VL		m	M	
		c	VH								n	M	
		h	VH								o	M	
Personalization techniques and technologies	Screen-decoded images	a	H	6	d	M	5	e	H	8	l	L	5
		b	M		g	M		f	VH		m	M	
		c	H					k	H		n	L	
		d	H								o	M	
		h	M										
Taggants	Rare earth	b	H	8	g	N/A	0	e	N/A	0	l	H	8
		c	H					f	N/A		m	H	
		k	H					k	N/A		n	H	
											o	VH	
DOVIDs	De-metallized DOVIDs	a	H	6	d	M	5	e	VL	2	l	M	5
		b	M		g	M		f	VL		m	M	
		c	M								n	M	
		d	M								o	M	
		h	M										
Digital security features	Data integrity protection	b	N/A	0	d	N/A	0	b	VH	10	m	M	6
		c	N/A		k	N/A		c	VH		o	M	
		j	N/A					j	VH				
		k	N/A					k	VH				

Key

C criterion

S scale

R rate

VL very low

L low

M moderate

H high

VH very high

N/A not applicable

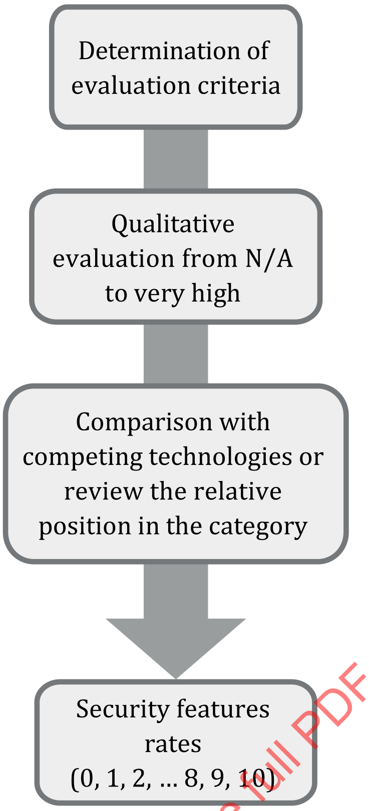
Determination of evaluation criteria
Qualitative evaluation from N/A to very high
Comparison with competing technologies or review the relative position in the category
Security features rates (0, 1, 2, ... 8, 9, 10)

Figure C.1 — Security rating process

C.4 Security rate tables

Tables C.3 to C.11 list security rates and substrate suitability (paper, card and synthetic) categorized by security features and technologies. Table C.9 lists DOVID sub-features. It should be recognized that these lists are not inclusive of all possible security technologies and that some in the same category can have different security efficiency.

Table C.3 — Security rates for substrate technologies

Substrate technologies	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Multitone watermark	9	4	3	5	P
Two-tone watermark	9	4	3	4	P
Registered watermark	8	3	2	3	P
Watermark	8	3	2	2	P
Artificial watermarks	4	1	1	1	P
Card watermarking	8	3	2	3	C
Chemical sensitivity	5	2	5	3	P
Embedded and windowed threads	8	4	4	5	P/C
Visible fibres	8	2	4	2	P/S
Key P paper C card S synthetic					

Table C.3 *(continued)*

Substrate technologies	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Invisible (covert) fibres, particles and planchettes	5	4	5	4	P/C/S
UV features	5	2	2	2	P/C/S
Toner anchorage	5	1	3	1	P/S
Tactile features	7	3	3	2	P/C/S
Pen reactive responses	4	2	3	2	P
Laser perforation	8	4	3	4	P/C/S
Key P paper C card S synthetic					

Table C.4 — Security rates for security printing

Security printing (not variable data)	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Duplex patterns	7	4	2	6	P/S
Fine line background (Guilloche pattern)	5	3	2	1	P/C/S
Microprinting or nanoprinting	7	6	0	8	P/C/S
Secure or reserved type fonts	1	0	3	0	P/C/S
Rainbow print	7	3	2	2	P/C/S
Copy evident anti-copy pantograph	7	2	5	2	P/C/S
Optical variable or latent image	8	5	0	8	P/S
Optically variable print	7	7	5	6	P/C/S
Tactile images, intaglio printing, code for visually impaired	8	3	0	8	P/S
UV covert image	7	6	6	6	P/C/S
Embossing	1	1	1	1	P/C
Retro-reflective device	8	7	5	8	P/C/S
Laser encoded optical image	8	5	6	8	P/C/S
Microstructure or nanostructure modulated image	7	6	2	8	P/C/S
Micro-structured taggants	8	2	5	8	P/C/S
Deliberate errors or known flaws	4	3	1	2	P/C/S

Table C.5 — Security rates for security inks

Security inks	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Colour shifting inks	9	3	1	5	P/C/S
Chemical reactive	7	4	7	4	P
Fugitive inks	7	4	7	4	P
Infrared or UV fluorescent	5	3	5	3	P/C/S
Infrared dropout	7	4	5	4	P/C/S

Table C.5 *(continued)*

Security inks	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Metallic, pearlescent and iridescent	4	2	1	2	P/C/S
Metameric	4	2	1	3	P/C/S
Thermochromics	8	2	2	2	P/S
Tagged inks	8	2	2	7	P/S
Erasable inks	5	3	5	3	P
Penetrating inks	6	4	6	3	P
Photochromic inks	8	3	3	3	P/S
Phosphorescent inks	8	3	3	4	P/S

Table C.6 — Security rates for personalization techniques and technologies

Personalization techniques and technologies	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Deliberate errors or known flaws	5	3	2	2	P/C/S
Protective laminate or coating	5	3	3	1	C/S
Laser perforation	5	2	6	2	P/C/S
Laser engraving or etching	5	3	5	2	C
Machine-readable technology[a]	2	2	7	1	P/C/S
Invisible polychromatic printing	8	7	7	8	P/C/S
Micro-optical imaging	9	6	7	9	C
Redundant data	0	0	5	0	P/C/S
Mass-serialization	9	3	8	8	P/C/S
Thin film interference filters	8	6	7	5	P/C/S
Screen decoded images	6	5	8	5	P/C/S
Frequency line modulation image	7	6	4	8	P/C/S

[a] The category and rate evaluation greatly vary depending on applications, including:

— reading the characteristics of hidden or covert materials for authentication;

— identification of some variable data, such as RFID, near-field communication (NFC), visible or invisible, standardized or proprietary machine-readable codes.

Table C.7 — Security rates for taggants

Taggants	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Infrared	6	2	1	6	P/C/S
UV	4	3	3	2	P/C/S
Rare earth	8	0	0	8	P/C/S
DNA	8	0	0	8	P/C/S

Table C.8 — Security rates for traditional DOVIDs

DOVIDs	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Metallized DOVIDs	5	4	1	3	P/C/S
De-metallized DOVIDs	6	5	2	5	P/C/S
Transparent DOVIDs	6	5	4	5	P/C/S
Hybrid DOVIDs	7	7	4	7	P/C/S

Table C.9 — Security rates for sub features of the DOVIDs

Sub features of DOVIDs	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Overlay ultra-thin security layer (7 µm to 12 µm)	0	0	2	0	P/C/S
Surface relief effect	1	1	0	0	P/C/S
Diffractive watermark	1	1	0	0	P/C/S
Diffractive nanofeatures	3	0	0	2	P/C/S
Diffractive microfeatures	2	0	0	0	P/C/S
Virtual image DOVIDs	1	1	0	0	P/C/S
Variable surface reflectance	3	2	3	3	P/C/S
Covert confirmed DOVIDs	3	2	2	3	P/C/S
Laser etched personalized optical variable device (OVD)	3	2	3	2	P/C/S

NOTE The rates are added to the base DOVIDs rate, with a maximum of 10 rates in each attack mode.

Table C.10 — Security rates for advanced DOVIDs

DOVIDs	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Precision metallized DOVIDs	8	6	3	7	P/C/S
Zero order diffraction colour permutation DOVIDs	9	8	5	7	P/C/S
Personalized image DOVIDs	8	7	7	7	P/C/S

Table C.11 — Security rates for digital security features

Types of digital security features	Cloning	Facsimile	Alteration	Theft or PA	Substrate: P, C or S
Digitally verifiable physical layer protection	9	9	6	9	P/C/S
Digitally generated protection	9	6	8	8	P/C/S
Data integrity protection	N/A	N/A	10	9/6[a]	P/C/S

[a] Depending on the level of security of certificate used.

Annex D
(informative)

Categorization of security features by authentication level and associated method

D.1 General

Categorization of security features by authentication method with overt and covert consideration is described in ISO 22382 and ISO 22383. Levels from one to four are prescribed from related characteristics.

Overt security features are detectable and verifiable using one or more of the human senses without the need for tools (other than those commonly used to correct human senses, such as spectacles or hearing aids). Covert security features are imperceptible to human senses and require competent use of equipment for automated interpretation. Forensic examination can also demonstrate document authenticity via analysis of composition and intrinsic attributes.

D.2 Authentication-level overview

Methods, tools and users corresponding to authentication levels are summarized in Table D.1.

Table D.1 — Authentication levels and characteristics

Authentication level	**1**	**2**	**3**	**4**
Methods	Inspection using human senses based on easily identifiable overt features with quick check capacity	Examination of covert features by specified and other users[a] with specific tools and devices	Authentication of coded covert security features and encoded data	Forensic examination
Tools	None	Off-the-shelf[b]	Purpose-built	—
General users	OVERT	COVERT	—	—
Specified users	OVERT	COVERT	COVERT	—
Authorities	OVERT	COVERT	COVERT	COVERT

[a] This can include general users.

[b] This can include smart consumer devices (e.g. smartphones, tablets).