ISO 14298:2021 Implementation Guide

Graphic technology - Management of security printing processes

Implementation Guide

Standard	ISO 14298:2021
Subject	Graphic technology - Management of security printing processes
Prepared for	Security printers, secure document producers, anti-counterfeit printing providers and organizations handling sensitive printed products
Format	Clean old-format guide - no logo

A practical implementation guide for organizations seeking to establish, operate and improve a security printing management system in line with ISO 14298:2021.

Note: This guide is a practical implementation aid and is not a replacement for the official ISO 14298:2021 standard. Organizations should use the official standard for certification and formal compliance decisions.

Contents

1. Purpose of this Guide

This guide is designed to help security printing organizations understand how to implement an effective management system for security printing processes in line with ISO 14298:2021.

It translates the intent of the standard into practical implementation steps, controls, records and readiness checks. It is intended for organizations involved in security printing, protected print production, anti-counterfeit printing, secure document production, financial instruments, certificates, ballots, licences, tax stamps, identity-related documents, brand-protection labels, secure packaging and other sensitive printed products.

Note: This guide is an implementation aid and is not a replacement for the official ISO 14298:2021 standard. Organizations should use the official standard for certification, contractual and formal compliance decisions.

2. Applicability and Scope Control

The first implementation decision is to define which printing activities, sites, departments, processes, secure zones, products and outsourced activities are included in the Security Printing Management System.

- Define the legal organization and all physical sites included in the scope.
- Identify security printing products and services covered by the system.
- State whether design, prepress, plate-making, printing, finishing, storage, dispatch, destruction and digital data handling are included.
- Document any outsourced process that can affect security or customer requirements.
- Identify any exclusions and justify them carefully.

The scope should be specific enough to make the certification boundary clear. A generic statement such as “printing services” is usually not sufficient for a security printing management system.

3. ISO 14298:2021 at a Glance

ISO 14298:2021 is focused on the management of security printing processes. It supports organizations in establishing a structured system to meet security printing requirements and customer security requirements where applicable.

Element	Implementation Meaning
Management system focus	The organization must plan, control, monitor and improve security printing processes through a defined system.
Security printing process focus	Controls must cover how sensitive printed products, data, materials, equipment, waste and records are handled.
Customer security requirements	Customer specifications and security conditions must be reviewed, controlled and protected where they do not conflict with the standard.
Risk-based operation	Threats to product security, process security, data security and physical security should be identified and controlled.
Evidence focus	Implementation should be supported by controlled procedures, registers, logs, approvals, inspections, reconciliations and review records.

4. Core Implementation Principles

A strong security printing management system is built on strict control, traceability, segregation and accountability. Each stage of production should reduce the possibility of unauthorized access, loss, substitution, leakage, counterfeiting or misuse.

- Clear ownership of security responsibilities
- Controlled access to sensitive areas and information
- Approved procedures for secure production and handling
- Traceability of controlled materials and products
- Segregation between sensitive and non-sensitive activities
- Personnel screening, confidentiality and awareness
- Incident reporting and corrective action
- Independent review through internal audits and management review

5. Security Printing Management Framework

Implementation should start with a documented framework that explains how the organization governs security printing activities. The framework should connect policy, objectives, roles, risks, operational procedures and performance review.

Framework Area	Typical Evidence
Policy and objectives	Security printing policy, objectives, measurable targets and management approval.
Roles and authority	Organization chart, security officer appointment, process responsibilities and escalation rules.
Risk and threat controls	Risk register, threat matrix, treatment actions and periodic review records.
Operational security	Secure production procedures, access logs, reconciliation records and dispatch controls.
Monitoring and improvement	Internal audits, incident logs, management review and corrective action records.

6. Context of the Organization

The organization should determine the internal and external issues that can affect its ability to manage security printing processes. These may include legal requirements, client specifications, criminal threats, supply chain risks, technology changes, equipment capability, workforce stability, cybersecurity risks and location-related security factors.

Interested parties typically include customers, regulators, law enforcement bodies where relevant, employees, contractors, secure material suppliers, logistics providers, certification bodies and shareholders or owners.

- Maintain a context and interested-party register.
- Identify customer-specific security requirements before accepting work.
- Review changes in the threat environment at planned intervals.
- Update the scope when sites, products, customers or processes change.

7. Leadership and Security Culture

Top management must create a culture where security is treated as a core operational requirement, not an administrative formality. In a security printing environment, leadership commitment should be visible through resource allocation, security enforcement, disciplinary rules, training, infrastructure investment and regular review.

- Approve the security printing policy and objectives.
- Nominate responsible personnel for security management and incident escalation.
- Ensure supervisors enforce secure working practices consistently.
- Promote confidential reporting of suspicious events, violations or weaknesses.
- Review security performance and corrective actions at management level.

8. Security Policy and Objectives

The security printing policy should state the organization’s commitment to maintaining controlled, traceable and secure printing operations. It should be communicated to employees and relevant external providers and reviewed when significant changes occur.

Objective Area	Possible Measure
Access control	Unauthorized access attempts, access review completion and visitor log accuracy.
Material security	Reconciliation accuracy for controlled materials, spoilage and waste.
Information security	Secure file handling, access review results and data deletion evidence.
Incident control	Incident closure time, repeated issues and corrective action effectiveness.
Awareness	Training completion, security briefings and confidentiality acknowledgement status.

9. Planning, Risks and Threat Assessment

Security printing risks should be assessed using a method that reflects the nature of secure print production. The assessment should consider physical, procedural, personnel, digital, supplier, logistics and product-specific threats.

- Unauthorized access to secure production areas
- Loss, theft or substitution of controlled materials
- Unauthorized copying or extraction of customer files
- Misuse of printing plates, cylinders, dies, templates or digital artwork
- Uncontrolled waste, spoiled sheets or defective security items
- Insider threats, collusion or social engineering
- Cyber incidents affecting customer data or production files
- Supplier or logistics failure affecting secure custody

The risk assessment should produce a treatment plan with owners, deadlines, controls and effectiveness reviews. The plan should also consider climate-related disruptions where these could affect security printing operations, storage, energy supply, transport or site resilience.

10. Legal, Regulatory and Customer Requirements

Security printers often operate under contractual, legal, regulatory or customer-specific security conditions. These requirements should be identified before accepting work and translated into controlled operational instructions.

- Maintain a register of applicable legal, regulatory and contractual requirements.
- Review customer security specifications before order acceptance.
- Confirm requirements for confidential artwork, prototypes, proofs, samples and customer-owned materials.
- Define retention, return and destruction requirements for customer information and materials.
- Ensure any conflict between customer requirements and the management system is escalated before production begins.

11. Organizational Roles and Security Responsibilities

Security responsibilities should be defined for top management, security officer, production manager, quality manager, IT owner, stores, prepress, dispatch, HR, maintenance, supervisors and outsourced service coordinators.

Role	Typical Security Responsibility
Top management	Policy approval, resources, strategic direction and management review.
Security officer	Security monitoring, incident reporting, access rules and visitor controls.
Production manager	Secure production execution, job controls and material reconciliation.
Prepress or IT owner	Secure handling of digital files, templates and access rights.
Stores or warehouse	Secure receipt, storage, issue and return of controlled materials.
HR	Personnel screening, confidentiality agreements, induction and disciplinary support.

12. Personnel Security and Competence

People controls are central to ISO 14298 implementation. Organizations should define screening, competence, confidentiality, access authorization, training and termination controls based on the sensitivity of each role.

- Complete pre-employment checks before granting access to sensitive areas or information.
- Ensure employees sign confidentiality or non-disclosure commitments before work begins.
- Define role-based security competence requirements.
- Provide induction on secure behaviour, reporting channels and prohibited actions.
- Review access rights when personnel change roles or leave the organization.
- Maintain training and awareness records.

13. Physical Security and Site Controls

The security of the premises should be designed around controlled access, secure zoning, monitoring, visitor control, perimeter protection and protection of high-risk process areas.

- Define restricted, controlled and general areas.
- Use access authorization based on role and need-to-enter principles.
- Maintain visitor identification, escort and sign-in records.
- Control keys, access cards, combinations and alarm codes.
- Monitor sensitive areas using appropriate surveillance and inspection practices.
- Control storage of plates, dies, tools, master files, secure substrates and finished goods.

14. Documented Information and Record Control

Documented information should be controlled to prevent unauthorized use, disclosure, alteration or loss. This is especially important for customer designs, proofs, specifications, job tickets, process routes, artwork, plate files, secure procedures and reconciliation records.

- Classify sensitive documents and files.
- Use controlled issue and revision rules.
- Restrict access to security-sensitive documents.
- Maintain a master document register.
- Protect electronic files using access rights, backup and change control.
- Define retention, archiving and destruction rules.

15. Security Classification and Information Protection

Organizations should classify information according to sensitivity. This allows consistent handling rules for ordinary business information, internal process information, customer-sensitive files and highly restricted security printing data.

Classification	Examples of Controls
General	Normal filing, approved sharing and basic document control.
Internal controlled	Access limited to relevant personnel and current revision only.
Customer confidential	Restricted access, secure transfer, retention control and deletion evidence.
Security restricted	Need-to-know access, logging, approval, secure storage and controlled destruction.

16. Secure Order Review and Prepress Control

Before production begins, the organization should verify the customer requirements, security features, artwork status, approval route, proofing method, production authorization and secure file transfer method.

- Review customer security requirements before order acceptance.
- Confirm authorized customer representatives for approvals and changes.
- Control artwork receipt, design changes, proof approval and version history.
- Restrict access to digital files, templates and design elements.
- Control output to plates, cylinders, dies, screens or digital production systems.
- Maintain evidence of customer approvals and internal release authorization.

17. Production Process Security

Production controls should ensure that only authorized jobs are produced, only approved materials are used and output is traceable from receipt through production, inspection, finishing, storage, dispatch and destruction.

- Use approved job tickets or production instructions.
- Verify materials issued against authorized production quantities.
- Restrict production runs to approved quantities and approved personnel.
- Control machine setup, samples, trial runs and retained specimens.
- Record nonconforming, spoiled and excess output.

- Segregate secure products from non-secure products.
- Apply final verification before release to storage or dispatch.

18. Controlled Materials, Waste and Reconciliation

Reconciliation is one of the most important evidence areas for security printing. The organization should account for controlled substrates, secure inks, foils, holograms, plates, dies, job samples, spoiled sheets, defective goods, work-in-progress and finished products.

Control Point	Expected Evidence
Receipt	Delivery note, quantity check, supplier approval and secure storage entry.
Issue to production	Material issue note, authorized quantity and job reference.
In-process control	WIP count, spoilage log, supervisor verification and secure segregation.
Finished goods	Final count, release approval, storage log and dispatch instruction.
Waste and destruction	Waste register, destruction authorization, witness record and reconciliation closure.

19. Supplier and Outsourced Process Control

External providers can create security vulnerabilities when they handle secure materials, confidential files, maintenance activities, IT systems, transport or destruction services. Supplier controls should reflect the sensitivity of the outsourced activity.

- Approve suppliers based on capability, security controls and contractual requirements.
- Include confidentiality and security obligations in supplier agreements.
- Define secure transport, chain-of-custody and handover rules.
- Control maintenance contractors and temporary workers entering secure areas.
- Verify destruction, disposal or recycling providers where security waste is involved.
- Monitor supplier performance and investigate security-related supplier failures.

20. Monitoring, Inspection and Internal Controls

The organization should monitor whether security controls are being followed. Monitoring can include security inspections, access review, camera review where legally allowed, reconciliation checks, job close-out reviews, file access checks, supplier reviews and supervisory verification.

- Define the frequency of security inspections.
- Review access permissions periodically.
- Check reconciliation logs for completeness and accuracy.
- Confirm document control and file control compliance.
- Record deviations and corrective actions.
- Report security performance to management.

21. Incident Reporting and Investigation

A security printing organization should treat actual and potential security incidents seriously. Incidents may include unauthorized access, missing controlled materials, unexplained production variance, file leakage, suspicious employee behaviour, breached packaging, counterfeit indicators, IT compromise or transport irregularity.

Incident Process	Expected Activity
Report	Immediate reporting route and escalation to responsible personnel.
Contain	Secure affected area, stop process where needed and preserve evidence.
Investigate	Determine what happened, root cause, affected items and customer impact.
Correct	Take corrective action, recover materials and strengthen controls.
Review	Verify effectiveness and communicate lessons learned to relevant personnel.

22. Internal Audit and Management Review

Internal audits should evaluate whether the security printing management system is implemented, maintained and effective. Audits should cover operational practice and not only document availability.

- Audit secure order review, prepress, production, storage, dispatch and waste destruction.
- Verify access control and visitor control evidence.
- Sample production jobs and check reconciliation from material receipt to job closure.
- Review incident logs, corrective actions and effectiveness checks.
- Evaluate supplier control and outsourced-process arrangements.
- Confirm management review includes security performance, risks, incidents, resources and improvement needs.

23. Documented Information Toolkit

The following documents and records are typically useful when implementing ISO 14298:2021. The exact set should be adjusted to the size, risk and complexity of the organization.

Document or Record	Purpose
Scope statement	Defines site, products, processes and boundaries.
Security printing policy	Confirms management commitment and security direction.
Risk and threat register	Identifies threats and planned controls.
Security objectives	Defines measurable security performance targets.
Access control procedure	Controls entry into secure areas and systems.
Secure production procedure	Controls prepress, production, finishing and storage.
Material reconciliation log	Tracks controlled materials, WIP, spoilage and finished goods.
Waste destruction record	Evidences secure destruction and closure of balances.
Incident report and investigation form	Captures security events and corrective action.
Internal audit and management review records	Evidence monitoring and continual improvement.

24. ISO 14298 Implementation Roadmap

A structured implementation roadmap helps the organization move from documentation to practical control. The roadmap below should be adapted to operational risk and project urgency.

Phase	Main Activities
Initiation	Confirm scope, leadership ownership, security officer and implementation team.
Assessment	Review current site controls, process controls, information controls and customer requirements.
Planning	Complete risk and threat assessment, objectives and action plan.
System development	Create or update procedures, registers, logs and control forms.
Implementation	Train personnel and apply controls across secure production processes.
Validation	Test reconciliation, access controls, incident reporting and file protection.
Review	Conduct internal audit, management review and corrective action closure.
Certification readiness	Verify evidence and prepare for Stage 1 and Stage 2 assessments.

25. 90-Day Implementation Plan

Time Period	Focus Area
Days 1-15	Define scope, appoint responsibilities and approve implementation plan.
Days 16-30	Review customer, legal and security requirements; define policy and objectives.
Days 31-45	Complete risk and threat assessment; identify treatment actions.
Days 46-60	Develop or update security procedures, registers and logs.
Days 61-75	Train personnel and implement production, access, material and waste controls.
Days 76-85	Complete security inspections, job-traceability checks and evidence review.
Days 86-90	Conduct internal audit, management review and corrective action closure.

26. Certification Readiness Checklist

Readiness Question	Status
Is the scope specific to security printing activities, products and sites?	
Has top management approved the security printing policy and objectives?	
Are roles, responsibilities and authorities clearly assigned?	
Has a risk and threat assessment been completed?	
Are customer security requirements reviewed before order acceptance?	
Are access rights controlled for secure areas and systems?	
Are personnel screened, trained and bound by confidentiality controls?	
Are secure materials, WIP, spoilage, waste and finished goods reconciled?	
Are customer files, artwork and production data protected?	
Are suppliers and outsourced processes controlled according to risk?	
Are incidents reported, investigated and closed with corrective action?	
Has an internal audit been completed?	
Has management review been completed?	
Are records complete, current and retrievable?	

27. Common Implementation Mistakes

- Using generic ISO 9001 procedures without adding security-specific controls.
- Defining the scope too broadly without site and product boundaries.
- Failing to reconcile controlled materials, spoiled output and security waste.
- Allowing uncontrolled access to prepress files, templates or production data.
- Treating confidentiality agreements as a replacement for active personnel controls.
- Not differentiating ordinary print jobs from security printing jobs.
- Not controlling outsourced transport, destruction, IT or maintenance providers.
- Keeping incident logs but not investigating root cause or checking effectiveness.
- Completing internal audits as paperwork reviews only instead of process verification.

28. Frequently Asked Questions

Q: Is ISO 14298 only for government document printers?

A: No. It is relevant to security printers producing sensitive printed products. Some organizations may operate at governmental or non-governmental security levels depending on product type, customer requirements and certification arrangements.

Q: Can ISO 14298 be integrated with ISO 9001?

A: Yes. Many security printers integrate ISO 14298 with ISO 9001 because process control, competence, documented information, corrective action and management review can be aligned. Security-specific controls must still be clearly added.

Q: Is a generic printing procedure enough?

A: No. Security printing requires controls for access, sensitive information, controlled materials, secure production, reconciliation, waste, incident handling and confidentiality.

Q: What evidence is usually important during assessment?

A: Assessors usually look for controlled procedures, risk assessment, access logs, reconciliation records, training records, job records, waste destruction records, incident logs, internal audit and management review records.

Q: Does ISO 14298 cover cybersecurity?

A: The standard is focused on security printing management, but digital files, artwork, templates, customer data and production systems should be protected where they affect security printing processes.

Q: Should climate-related issues be considered?

A: Where climate-related disruptions can affect security printing processes, materials, premises, power, transport, storage or continuity, they should be considered as part of the management system context and risk planning.

29. Final Implementation Note

ISO 14298:2021 implementation should be treated as a security discipline supported by a management system. The organization should be able to show that security rules are not only documented but actively applied during order review, prepress, production, storage, dispatch, destruction, supplier control and incident response.

A security printing management system becomes stronger when employees understand the reason behind every control, supervisors verify daily discipline and top management reviews the effectiveness of the system at planned intervals.