PACIFIC CERTIFICATIONS

Trusted Global ISO Certification Body

ISO 14298:2021

Graphic technology - Management of security printing processes

Audit Checklist

Website downloadable resource | Editable readiness tool for organizations preparing for certification

www.pacificcert.com | support@pacificcert.com

About this downloadable resource

Area	Guidance
Purpose	Use this resource to review whether security printing processes are planned, controlled, monitored, and improved in line with ISO 14298:2021 readiness expectations.
Recommended users	Security printing organizations, compliance teams, production heads, security managers, quality teams, suppliers, and internal review teams.
Important note	This is an educational readiness resource. It does not reproduce the ISO standard and should be used with the official ISO 14298:2021 document.
How to use	Review each question or requirement area, record objective evidence, define gaps, assign actions, and maintain records for management review and certification preparation.

Suggested scoring

Score	Status	Meaning
0	Not implemented	No defined process or objective evidence available.
1	Partially implemented	Some practices exist but are inconsistent, undocumented, or not fully controlled.
2	Mostly implemented	Controls are defined and operating, with minor gaps or limited evidence.
3	Fully implemented	Controls are implemented, maintained, evidenced, reviewed, and improved.

ISO 14298:2021 audit checklist

Use the checklist to ask consistent readiness questions and record evidence, conformity status, and follow-up actions. Replace generic prompts with organization-specific criteria where needed.

Context and scope

Area	Audit question	Evidence to review	C / PC / NC	Notes / actions
Context and scope	Has the organization determined the scope of security printing operations, including sites, processes, products, systems, and outsourced activities?	Scope statement, process map, site list, product categories, outsourcing register		
Context and scope	Are security printing risks, customer obligations, legal requirements, and stakeholder expectations identified and reviewed?	Risk register, legal register, customer contracts, interested-party review		
Context and scope	Are process interactions defined from customer order through design/prepress, production, finishing, storage, dispatch, and destruction?	Process flow, SOPs, responsibility matrix, interface controls		

Leadership

Area	Audit question	Evidence to review	C / PC / NC	Notes / actions
Leadership	Does top management demonstrate accountability for the security printing management system?	Policy, objectives, review records, meeting minutes, resource approvals		
Leadership	Are security responsibilities, authorities, escalation routes, and segregation of duties clearly assigned?	Organization chart, job descriptions, authorization matrix		
Leadership	Is the policy communicated to employees, contractors, visitors, and relevant suppliers?	Training records, postings, induction materials, supplier requirements		

Planning

Area	Audit question	Evidence to review	C / PC / NC	Notes / actions
Planning	Are threats, vulnerabilities, material sensitivity, information risks, and operational risks assessed and treated?	Risk methodology, risk treatment plans, control reviews		
Planning	Are measurable objectives established for security, production control, incidents, customer requirements, and continual improvement?	Objectives, KPIs, action plans, performance trends		
Planning	Are changes to products, processes, equipment, layouts, suppliers, or systems planned and reviewed for security impact?	Change requests, approvals, validation records, risk updates		

Support

Area	Audit question	Evidence to review	C / PC / NC	Notes / actions
Support	Are people competent for security-sensitive roles and aware of their obligations?	Competence matrix, training plans, assessments, awareness records		
Support	Are personnel screening, confidentiality, access authorization, and disciplinary rules applied where appropriate?	Screening procedure, declarations, access list, HR records		
Support	Are documented procedures and records controlled against unauthorized access, loss, misuse, or obsolete use?	Document register, retention schedule, access permissions, change history		
Support	Are facilities, utilities, IT, equipment, and secure work areas maintained for controlled security printing operations?	Maintenance records, calibration, environmental controls, access maps		

Operation

Area	Audit question	Evidence to review	C / PC / NC	Notes / actions
Operation	Are customer security requirements reviewed before accepting or changing security printing work?	Contract review, specifications, customer approvals, job tickets		
Operation	Are artwork, digital files, plates, dies, substrates, inks, foils, and other sensitive assets identified and protected?	Asset register, inventory records, access controls, secure storage logs		
Operation	Are production jobs authorized, traceable, reconciled, inspected, and released according to defined controls?	Job approvals, batch records, reconciliation sheets, inspection records		
Operation	Are nonconforming product, rejects, waste, samples, and surplus materials segregated and disposed of securely?	Hold records, destruction certificates, waste logs, sample controls		
Operation	Are dispatch, storage, transport, and handover activities controlled to preserve chain of custody?	Dispatch logs, packaging records, transport requirements, delivery confirmations		
Operation	Are security-sensitive suppliers and outsourced providers evaluated, approved, and monitored?	Supplier criteria, contracts, assessments, performance reviews		
Operation	Are incidents, losses, discrepancies, attempted breaches, and suspicious events reported and investigated?	Incident logs, investigation reports, corrective actions, trend analysis		

Performance evaluation

Area	Audit question	Evidence to review	C / PC / NC	Notes / actions
Performance evaluation	Are monitoring methods defined for security objectives, access events, material reconciliation, incidents, suppliers, and process performance?	KPIs, dashboards, logs, review records, sampling plans		
Performance evaluation	Are internal reviews carried out by competent and independent reviewers at planned intervals?	Review schedule, checklists, reviewer competence, reports		
Performance evaluation	Does management review performance, risks, incidents, resources, customer feedback, and improvement needs?	Management review agenda, inputs, decisions, actions		

Improvement

Area	Audit question	Evidence to review	C / PC / NC	Notes / actions
Improvement	Are nonconformities and security failures corrected promptly and investigated for root cause?	NC reports, root-cause analysis, containment, corrective actions		
Improvement	Are corrective actions verified for effectiveness and used to update risks, procedures, training, or controls?	Effectiveness checks, updated controls, lessons learned		
Improvement	Is continual improvement demonstrated through trend review, risk reduction, strengthened controls, and management decisions?	Improvement register, trend analysis, completed projects		

Quick evidence list for ISO 14298:2021 readiness

Evidence category	Examples to collect
Governance	Scope, policy, objectives, roles, risk methodology, management review records
Security controls	Access logs, visitor records, CCTV checks, restricted-area controls, key/badge control records
Production control	Customer approvals, job tickets, process records, inspection records, release records, reconciliation sheets
Material control	Sensitive material register, stock counts, issue/return logs, sample records, waste/destruction evidence
Digital security	User access records, file transfer controls, backup evidence, incident logs, change history
Suppliers	Approved supplier list, contracts, confidentiality clauses, supplier monitoring and review records
Improvement	Nonconformity records, incident investigations, corrective actions, effectiveness verification

For ISO 14298:2021 certification assistance, email support@pacificcert.com or visit www.pacificcert.com