PACIFIC CERTIFICATIONS

Trusted Global ISO Certification Body

ISO 14298:2021

Graphic technology - Management of security printing processes

Gap Analysis Template

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

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 gap analysis worksheet

Record the current state, objective evidence, gaps, action owner, and target completion date for each security printing management system requirement area.

Context and scope

Clause / area	Requirement focus	Current evidence	Gap / risk	Score	Owner / due date
4	**Organization context** Internal and external security printing risks, interested parties, applicable legal and customer requirements, and the defined scope of the security printing management system.				
4	**Process interaction** Core, support, outsourced, and controlled security printing processes are identified with inputs, outputs, responsibilities, security controls, and interfaces.				

Leadership and governance

Clause / area	Requirement focus	Current evidence	Gap / risk	Score	Owner / due date
5	**Leadership commitment** Top management demonstrates accountability for security printing controls, risk-based planning, ethics, confidentiality, and continual improvement.				
5	**Policy and responsibilities** Security printing policy, roles, authorities, segregation of duties, escalation routes, and decision rights are defined and communicated.				

Planning and risk control

Clause / area	Requirement focus	Current evidence	Gap / risk	Score	Owner / due date
6	**Risk assessment** Threats, vulnerabilities, asset value, customer requirements, regulatory duties, and process risks are identified and evaluated.				
6	**Objectives and plans** Measurable objectives support protection of secure products, controlled materials, sensitive information, quality, delivery, and incident reduction.				

Support and resources

Clause / area	Requirement focus	Current evidence	Gap / risk	Score	Owner / due date
7	**People and competence** Personnel are screened as applicable, trained, authorized, supervised, and made aware of security responsibilities.				
7	**Infrastructure and environment** Facilities, equipment, secure storage, IT systems, access points, utilities, and work areas are suitable for controlled operations.				

Clause / area	Requirement focus	Current evidence	Gap / risk	Score	Owner / due date
7	**Documented information** Procedures, forms, records, approvals, versions, retention, access permissions, and disposal of sensitive documents are controlled.				

Operational control

Clause / area	Requirement focus	Current evidence	Gap / risk	Score	Owner / due date
8	**Customer and product security requirements** Secure product requirements, specifications, artwork, serialized items, anti-counterfeit features, and customer approvals are controlled.				
8	**Physical security** Access control, visitor management, surveillance, restricted zones, secure receiving, dispatch, and perimeter controls are implemented.				
8	**Material control** Security substrates, inks, foils, plates, dies, waste, samples, rejects, and controlled stock are identified, counted, reconciled, and protected.				
8	**Production and traceability** Jobs are authorized, controlled during prepress/press/postpress, traceable, inspected, reconciled, and released by authorized personnel.				
8	**Information security** Digital files, customer data, artwork, production data, system access, backups, removable media, and transmission channels are protected.				
8	**Suppliers and outsourced work** Security-sensitive suppliers and subcontractors are evaluated, approved, contractually controlled, monitored, and reviewed.				
8	**Nonconforming and suspicious items** Nonconforming product, missing materials, tampering signs, inventory discrepancies, and suspicious activity are isolated and investigated.				

Performance evaluation and improvement

Clause / area	Requirement focus	Current evidence	Gap / risk	Score	Owner / due date
9	**Monitoring and measurement** Security controls, production performance, incidents, discrepancies, supplier performance, customer feedback, and objectives are monitored.				

Clause / area	Requirement focus	Current evidence	Gap / risk	Score	Owner / due date
9	**Internal review and management review** Internal reviews are planned and management evaluates performance, risks, resources, incidents, improvement actions, and certification readiness.				
10	**Corrective action and improvement** Incidents, complaints, control failures, and gaps are investigated for root cause and followed through with effective corrective actions.				

Security printing control focus areas

Control focus	Readiness expectation	Evidence	Gap / risk	Score	Action owner
Access control	Restricted areas, visitor movement, personnel authorization, keys, badges, and access logs are controlled and periodically reviewed.				
Secure inventory	Sensitive materials, semi-finished goods, finished secure items, samples, rejects, and waste are counted, reconciled, and protected.				
Prepress and digital files	Artwork, plates, dies, files, approvals, revisions, and digital transfer points are secured and traceable.				
Production authorization	Security print jobs are released only against approved instructions, customer specifications, and defined acceptance controls.				
Waste and destruction	Security-sensitive waste is identified, segregated, counted where required, destroyed securely, and recorded.				
Dispatch and chain of custody	Packaging, labeling, dispatch authorization, transport controls, handover records, and customer delivery verification are controlled.				
Incident management	Loss, theft, attempted breach, information leakage, tampering, discrepancies, and suspicious behavior are reported, investigated, and closed.				

Action plan summary

Action required	Priority	Owner	Target date	Status

Need ISO 14298:2021 certification support? Contact Pacific Certifications at support@pacificcert.com or visit www.pacificcert.com