Pacific Certifications
Trusted Global ISO Certification Body

ISO 18788:2015 Gap Analysis Template

Management System for Private Security Operations

Downloadable Website Resource

For preliminary self-assessment, preparation, and internal readiness review

About ISO 18788:2015

ISO 18788:2015 specifies requirements with guidance for a management system for private security operations. It supports organizations conducting or contracting security operations by providing a structured framework for governance, risk management, legal and regulatory compliance, respect for human rights, operational control, performance evaluation, and continual improvement.

Use this gap analysis template as a practical preparation tool before certification assessment. It is intended to help organizations identify documented information, operational evidence, responsibilities, and improvement actions relevant to private security operations.

Need support with ISO 18788:2015 certification?

Contact Pacific Certifications at support@pacificcert.com or visit www.pacificcert.com to request certification details, application forms, and cost guidance.

How to Use This Gap Analysis Template

- Review each clause and operational area against current documented information and actual field practices.
- Record the current level of implementation: Fully Implemented, Partially Implemented, Not Implemented, or Not Applicable.
- Capture objective evidence such as policies, procedures, deployment records, risk assessments, training records, legal registers, incident logs, and management review outputs.
- Prioritize gaps according to operational risk, legal exposure, human rights impact, client requirements, and certification readiness.
- Assign action owners and target dates before moving into certification assessment stages.

Rating	Meaning	Typical Action
Fully Implemented	Requirement is addressed, evidence is available, and practice is consistently followed.	Maintain records and verify ongoing effectiveness.
Partially Implemented	Some controls or records exist, but coverage, consistency, or effectiveness is incomplete.	Define corrective actions, responsibilities, and completion dates.
Not Implemented	No adequate process, document, record, or operational control is available.	Develop and implement the required process and retain evidence.
Not Applicable	Requirement is not applicable to the organization after justified evaluation.	Document the justification and review when scope changes.

Clause-Wise Gap Analysis Matrix

Clause	Area	What to Evaluate	Current Status	Evidence / Gap Notes	Priority	Action Owner / Target Date
4	**Context of the organization**	Determine internal/external issues, interested parties, scope, system boundaries, outsourced/security activities, and governance context.	☐ Fully ☐ Partial ☐ Not Implemented ☐ N/A		☐ High ☐ Medium ☐ Low	
5	**Leadership**	Confirm leadership commitment, policy, roles, accountability, legal compliance, human rights expectations, and integration with security operations.	☐ Fully ☐ Partial ☐ Not Implemented ☐ N/A		☐ High ☐ Medium ☐ Low	
6	**Planning**	Identify risks and opportunities, legal and other requirements, security risk assessment, objectives, plans, and change considerations.	☐ Fully ☐ Partial ☐ Not Implemented ☐ N/A		☐ High ☐ Medium ☐ Low	
7	**Support**	Evaluate resources, competence, awareness, communication, documented information, training, and operational support arrangements.	☐ Fully ☐ Partial ☐ Not Implemented ☐ N/A		☐ High ☐ Medium ☐ Low	
8	**Operation**	Review operational planning and control, risk treatment, client requirements, subcontractor controls, incident preparedness, use-of-force controls, weapons controls where applicable, and emergency response.	☐ Fully ☐ Partial ☐ Not Implemented ☐ N/A		☐ High ☐ Medium ☐ Low	
9	**Performance evaluation**	Check monitoring, measurement, analysis, evaluation, internal assessment, management review, reporting, and security performance data.	☐ Fully ☐ Partial ☐ Not Implemented ☐ N/A		☐ High ☐ Medium ☐ Low	
10	**Improvement**	Assess nonconformity handling, corrective action, lessons learned, complaints, incident investigations, and continual improvement.	☐ Fully ☐ Partial ☐ Not Implemented ☐ N/A		☐ High ☐ Medium ☐ Low	
A1	**Climate action consideration**	Consider climate-related issues where they affect security operations, operational resilience, worker safety, travel, site risks, or interested-party requirements.	☐ Fully ☐ Partial ☐ Not Implemented ☐ N/A		☐ High ☐ Medium ☐ Low	

Private Security Operations Gap Analysis

Operational Area	Evaluation Focus	Current Practice	Evidence Reviewed	Gap / Risk	Action Required
Governance and accountability	Defined command structure, authorization levels, compliance obligations, client interfaces, and accountability for security operations.				
Risk assessment and treatment	Threat, vulnerability, impact, human rights, legal, operational, and country/site risk assessment with appropriate controls.				
Human rights and code of conduct	Screening, training, conduct rules, grievance channels, use-of-force restrictions, and respect for vulnerable groups.				
Operational planning and control	Deployment plans, post orders, supervision, communications, patrol procedures, access control, and escalation protocols.				
Personnel competence and vetting	Role competence, background checks where lawful, licenses, refresher training, and records for security personnel.				
Subcontractor and supply chain control	Due diligence, contractual requirements, performance monitoring, and control of subcontracted security services.				
Incident and emergency management	Incident reporting, response plans, investigation, evidence retention, corrective action, and emergency coordination.				
Weapons, equipment, and force controls	Authorization, storage, maintenance, issue/return records, legal compliance, and proportionality controls where applicable.				
Client and interested-party communication	Communication protocols with clients, authorities, communities, employees, and other relevant interested parties.				
Performance and improvement	KPIs, inspections, supervisory checks, lessons learned, internal assessments, management reviews, and improvements.				

Documented Information and Evidence Log

Document / Record	Purpose	Available?	Adequate?	Comments / Action
Scope and applicability statement	Defines covered security operations, locations, clients, exclusions, and outsourced activities.	☐ Yes ☐ No	☐ Yes ☐ No ☐ Partial	
Security operations policy	States commitments to legal compliance, human rights, responsible security operations, and continual improvement.	☐ Yes ☐ No	☐ Yes ☐ No ☐ Partial	
Legal and other requirements register	Tracks licenses, labor laws, weapons rules, data protection, contract duties, and client requirements.	☐ Yes ☐ No	☐ Yes ☐ No ☐ Partial	
Security risk assessment and treatment plan	Identifies threats, vulnerabilities, impacts, controls, residual risks, and approvals.	☐ Yes ☐ No	☐ Yes ☐ No ☐ Partial	
Code of conduct and human rights controls	Defines acceptable behavior, reporting channels, grievance handling, and conduct expectations.	☐ Yes ☐ No	☐ Yes ☐ No ☐ Partial	
Operational procedures / post orders	Defines site instructions, patrols, access control, escalation, communication, and reporting.	☐ Yes ☐ No	☐ Yes ☐ No ☐ Partial	
Competence, screening, and training records	Shows personnel competence, licensing, refresher training, and awareness of procedures.	☐ Yes ☐ No	☐ Yes ☐ No ☐ Partial	
Incident reports and investigation records	Captures incidents, response actions, root cause, corrective action, and lessons learned.	☐ Yes ☐ No	☐ Yes ☐ No ☐ Partial	
Management review records	Shows leadership review of system performance, risks, incidents, objectives, and improvement needs.	☐ Yes ☐ No	☐ Yes ☐ No ☐ Partial	

Gap Analysis Summary

Summary Item	Result / Notes
Major readiness gaps	
High-risk operational areas	
Documents requiring revision	
Training or competence gaps	
Recommended next actions	