Pacific Certifications

Trusted Global ISO Certification Body

ISO 18788:2015 Audit Checklist

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 audit checklist 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 Audit Checklist

- Use the checklist to plan an internal assessment or readiness review for ISO 18788:2015.
- Collect objective evidence through interviews, document review, site observation, and sampling of operational records.
- Mark each item as Conforming, Partially Conforming, Nonconforming, or Not Applicable.
- Record evidence clearly and link findings to corrective actions where gaps are identified.
- Ensure the review covers both management system requirements and field-level private security operations.

Status	Use When
C - Conforming	Requirement is implemented and supported by adequate evidence.
PC - Partially Conforming	Requirement is partly implemented but needs improvement or stronger evidence.
NC - Nonconforming	Requirement is not adequately addressed or practice is inconsistent.
N/A - Not Applicable	Requirement does not apply and the reason is documented.

Clause-Wise Audit Checklist

Clause	Audit Question	Evidence to Review	Status	Notes / Findings
4	Has the organization defined internal and external issues affecting private security operations?	Context analysis, risk profile, country/site risk information, stakeholder analysis	☐ C ☐ PC ☐ NC ☐ N/A	
4	Are relevant interested parties and their requirements determined, including clients, personnel, regulators, communities, and subcontractors?	Interested-party register, contracts, legal register, communication records	☐ C ☐ PC ☐ NC ☐ N/A	
4	Is the scope of the management system defined and aligned with actual security services, sites, and operational activities?	Scope statement, service list, location list, exclusions and justification	☐ C ☐ PC ☐ NC ☐ N/A	
5	Has leadership established a policy appropriate to private security operations, legal obligations, human rights, and client requirements?	Policy, communication records, leadership review minutes	☐ C ☐ PC ☐ NC ☐ N/A	
5	Are roles, responsibilities, authorities, and reporting lines clearly assigned for security operations?	Organization chart, job descriptions, appointment letters, post responsibilities	☐ C ☐ PC ☐ NC ☐ N/A	
6	Are risks and opportunities identified and planned, including operational, legal, human rights, and security risks?	Risk assessment, treatment plan, objectives, change plans	☐ C ☐ PC ☐ NC ☐ N/A	
6	Are measurable objectives established and monitored for relevant functions and operational levels?	Objectives, KPI dashboard, action plans, review records	☐ C ☐ PC ☐ NC ☐ N/A	
7	Are resources, infrastructure, equipment, communication systems, and support arrangements adequate for operations?	Resource plans, equipment records, maintenance logs, communication protocols	☐ C ☐ PC ☐ NC ☐ N/A	
7	Are personnel competent, trained, licensed where required, and aware of the code of conduct and operational requirements?	Training records, licenses, competence matrix, induction records	☐ C ☐ PC ☐ NC ☐ N/A	
7	Is documented information controlled, available at point of use, and protected from unintended use?	Document control procedure, document register, revision records, field copies	☐ C ☐ PC ☐ NC ☐ N/A	

Clause	Audit Question	Evidence to Review	Status	Notes / Findings
8	Are security operations planned and controlled according to risk, client requirements, law, and site conditions?	Operational plans, post orders, patrol logs, control room records	☐ C ☐ PC ☐ NC ☐ N/A	
8	Are subcontracted or outsourced security activities controlled through due diligence and performance monitoring?	Supplier evaluations, contracts, onboarding records, performance reports	☐ C ☐ PC ☐ NC ☐ N/A	
8	Are procedures available for incident response, escalation, reporting, investigation, and corrective action?	Incident procedure, incident logs, investigation files, lessons learned	☐ C ☐ PC ☐ NC ☐ N/A	
8	Are controls established for use of force, detention, weapons, equipment, and sensitive operations where applicable?	Use-of-force policy, weapons authorization, equipment issue logs, training records	☐ C ☐ PC ☐ NC ☐ N/A	
9	Does the organization monitor and evaluate operational performance, compliance, incidents, complaints, and objectives?	KPI records, compliance checks, inspection reports, complaints register	☐ C ☐ PC ☐ NC ☐ N/A	
9	Are internal assessments planned and performed by competent personnel with reported results?	Internal assessment program, checklists, reports, corrective actions	☐ C ☐ PC ☐ NC ☐ N/A	
9	Does management review the system for suitability, adequacy, effectiveness, risks, resources, and improvement needs?	Management review agenda, minutes, action log	☐ C ☐ PC ☐ NC ☐ N/A	
10	Are nonconformities, incidents, complaints, and weaknesses corrected with root cause review and corrective action?	NC reports, CAPA records, incident investigation, verification of effectiveness	☐ C ☐ PC ☐ NC ☐ N/A	
10	Is continual improvement supported through lessons learned, analysis, leadership review, and operational feedback?	Improvement log, lessons learned, review actions, trend analysis	☐ C ☐ PC ☐ NC ☐ N/A	

Operational Security Checklist

Area	Audit Question	Evidence to Review	Status	Notes / Findir
Security risk management	Are threat, vulnerability, impact, and residual risk considerations documented and updated for each relevant operation?	Site risk assessments, threat briefings, control plans	☐ C ☐ PC ☐ NC ☐ N/A	
Human rights	Are human rights risks identified and addressed in policies, training, operations, and grievance mechanisms?	Human rights assessment, code of conduct, training records, grievance log	☐ C ☐ PC ☐ NC ☐ N/A	
Personnel screening	Are screening, selection, licensing, and suitability checks performed lawfully and consistently?	Screening procedure, hiring records, licenses, verification evidence	☐ C ☐ PC ☐ NC ☐ N/A	
Training and awareness	Do security personnel understand post duties, emergency actions, communication protocols, and conduct expectations?	Training matrix, assessment results, interview notes	☐ C ☐ PC ☐ NC ☐ N/A	
Deployment control	Are guards deployed according to approved rosters, site instructions, and competence needs?	Rosters, duty logs, handover records, supervision reports	☐ C ☐ PC ☐ NC ☐ N/A	
Communication	Are communication channels maintained for routine reporting, escalation, emergencies, and client coordination?	Radio/phone logs, escalation matrix, communication tests	☐ C ☐ PC ☐ NC ☐ N/A	
Patrol and access control	Are patrols, visitor controls, access points, and site inspections performed as planned?	Patrol logs, visitor registers, access records, CCTV/control room logs	☐ C ☐ PC ☐ NC ☐ N/A	
Incident management	Are incidents reported promptly, investigated, analyzed, and closed with appropriate corrective action?	Incident reports, investigation files, action closure evidence	☐ C ☐ PC ☐ NC ☐ N/A	
Complaints and grievances	Are complaints from clients, personnel, communities, or other parties recorded and resolved?	Complaint register, grievance records, response evidence	☐ C ☐ PC ☐ NC ☐ N/A	
Emergency preparedness	Are emergency plans, drills, coordination with authorities, and response resources maintained?	Emergency plans, drill records, contact lists, after-action reports	☐ C ☐ PC ☐ NC ☐ N/A	

Area	Audit Question	Evidence to Review	Status	Notes / Findir
Equipment control	Is operational equipment issued, maintained, inspected, and returned under control?	Issue registers, inspection records, maintenance logs	☐ C ☐ PC ☐ NC ☐ N/A	
Weapons control, if applicable	Are weapons authorization, storage, issuance, training, legal compliance, and incident reporting controlled?	Weapons register, authorization records, training evidence, storage inspections	☐ C ☐ PC ☐ NC ☐ N/A	
Subcontractor control	Are subcontracted personnel and suppliers evaluated, briefed, supervised, and monitored?	Supplier evaluations, contracts, site records, performance review	☐ C ☐ PC ☐ NC ☐ N/A	
Data and information	Are sensitive operational records protected against unauthorized access, loss, or misuse?	Access permissions, secure storage, retention rules, incident records	☐ C ☐ PC ☐ NC ☐ N/A	
Climate and operating conditions	Are climate-related risks considered where they affect worker safety, travel, access, equipment, or emergency response?	Risk reviews, site plans, contingency measures, heat/weather controls	☐ C ☐ PC ☐ NC ☐ N/A	

Audit Summary and Action Log

Finding / Issue	Clause / Area	Risk Level	Corrective Action	Owner	Target Date	Closure Evidence
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				
		☐ High ☐ Medium ☐ Low				

Prepared by	Role	Date	Reviewed by	Date