PACIFIC CERTIFICATIONS

ISO 18788:2015

SECURITY OPERATIONS MANAGEMENT SYSTEM

IMPLEMENTATION GUIDE

Plan	Do	Check	Act
Understand security context, clients, legal duties, human rights risks and operational threats	Implement security operations controls, personnel vetting, communications and response procedures	Monitor operations, incidents, complaints, performance, reviews, internal audits and compliance	Correct gaps, improve controls, update risk treatment and strengthen operational accountability

A practical implementation guide for organizations conducting or contracting private security operations and preparing for ISO 18788:2015 certification, internal implementation, readiness assessment or operational improvement.

Use of this guide: This document is an implementation support resource. It does not replace the official ISO 18788:2015 standard. Organizations should use the official standard for exact requirements and apply this guide as a practical planning, documentation and readiness tool.

HOW TO USE THIS GUIDE

This guide is designed for security company leadership, operations managers, security supervisors, compliance teams, human resources, procurement teams, internal auditors and implementation teams. It follows the management system logic of ISO 18788:2015 and translates the requirements into practical actions, examples of documented information and certification-readiness checks.

Start by confirming the scope of security operations, applicable laws, client requirements, voluntary commitments and human rights considerations. Then build a security operations risk assessment, implement operational controls, verify performance and maintain evidence for assessment.

UNDERSTANDING ISO 18788:2015

ISO 18788:2015 is a management system standard for private security operations. It provides a framework for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the management of security operations.

The standard supports organizations that conduct or contract security operations and related activities. It is particularly relevant where security services may affect clients, communities, employees, contractors, public authorities and other interested parties.

- Professional conduct of security operations
- Accountability to law and respect for human rights
- Consistency with voluntary commitments adopted by the organization
- Risk-based planning of security operations and related support processes
- Control of personnel, subcontractors, operations, incident response and improvement

SOMS FUNDAMENTALS

A Security Operations Management System (SOMS) is the documented and implemented system used to manage private security operations in a controlled, lawful, ethical and accountable manner.

- A clear security operations policy and defined scope
- Defined legal, contractual and human rights obligations
- Leadership accountability and assigned operational authority
- Risk assessment covering threats, vulnerabilities, impacts and safeguards
- Controls for personnel screening, training, supervision, equipment and communications
- Operational planning for deployments, emergency response and incident management
- Monitoring, internal audit, management review, corrective action and continual improvement

Implementation point: The SOMS should describe how security operations are planned, staffed, supervised, performed, monitored and improved. It should not only describe head-office procedures; it must also control field activities, deployment sites and contracted operations.

BENEFITS OF IMPLEMENTATION

ISO 18788 supports better governance, transparency and operational control in security operations. The benefits are strongest when the SOMS is integrated into real deployment practices, contract management and supervision routines.

Benefit area	Practical value
Client confidence	Demonstrates that security operations are managed through a recognized management system.
Legal and human rights compliance	Improves control over lawful conduct, use of force, complaints, escalation and accountability.
Operational consistency	Provides common procedures for deployments, supervision, communications and incident handling.
Risk reduction	Links security threat assessment with controls, contingency planning and performance monitoring.
Subcontractor control	Extends expectations to external providers, partner organizations and contracted personnel.
Improvement	Uses incidents, complaints, audits and reviews to strengthen controls over time.

PDCA MODEL FOR SECURITY OPERATIONS

ISO 18788 can be implemented using the Plan-Do-Check-Act approach. This helps convert strategic policy commitments into controlled operational practice.

PDCA step	Security operations application	Typical evidence
Plan	Define scope, context, legal duties, interested parties, human rights risks and security objectives.	Scope statement, legal register, interested parties register, objectives, risk assessment method
Do	Implement operational controls for personnel, deployments, equipment, communications and incident response.	Deployment instructions, SOPs, screening records, training records, equipment logs, incident records
Check	Evaluate performance through inspections, monitoring, internal audits, client feedback, incident analysis and management review.	Monitoring reports, audit reports, complaints logs, KPI dashboards, review minutes
Act	Correct nonconformities, strengthen controls and update risks, procedures and training.	Corrective actions, lessons learned, revised procedures, updated risk treatment plans

IMPLEMENTATION ROADMAP

A structured project plan helps avoid creating a manual that is disconnected from field operations. The following roadmap can be adapted to the size and complexity of the organization.

Step	Implementation activity	Output
1	Confirm scope, sites, services, client categories and deployment locations.	Approved SOMS scope
2	Identify applicable laws, contract duties, human rights expectations and voluntary commitments.	Legal and obligations register
3	Define policy, roles, responsibilities and reporting lines.	SOMS policy, organogram and responsibility matrix
4	Conduct security operations risk assessment and human rights impact review.	Risk and threat register
5	Document operational procedures for planning, deployment, supervision and incident response.	SOPs and operating controls
6	Implement personnel vetting, training, equipment and communications controls.	HR, training and asset records
7	Monitor performance, incidents, complaints and compliance.	KPI reports and logs
8	Conduct internal audit, management review and corrective action closure.	Readiness evidence

CLAUSE 4 - CONTEXT OF THE ORGANIZATION

The organization should define the internal and external issues that affect security operations and the SOMS. This includes operational environments, types of services, client expectations, security threats, human rights risks, political or social conditions, public authority requirements and community impact.

- Determine the scope of the SOMS, including security services, locations, departments, functions and outsourced activities.
- Identify interested parties such as clients, employees, subcontractors, regulators, local communities, public authorities, insurers and affected persons.
- Define applicable requirements, including legal, regulatory, contractual, client and voluntary commitments.
- Document how context and interested-party information will be reviewed and updated.

Readiness check: The scope should be operationally precise. It should state what security operations are included, where they are performed, and which support functions are controlled by the SOMS.

CLAUSE 5 - LEADERSHIP

Top management should provide direction and demonstrate commitment to lawful, ethical and professionally managed security operations. Leadership should ensure that the SOMS is not treated as a documentation exercise but as a control system for real operational conduct.

- Approve and communicate a security operations management policy.
- Assign roles, responsibilities and authorities for security operations, compliance, human rights, incident response and client communication.
- Ensure that operational leaders have authority to stop unsafe, unlawful or nonconforming activities.
- Promote accountability, discipline, escalation and transparent reporting.
- Integrate SOMS objectives with business strategy and client commitments.

Leadership element	Expected implementation evidence
Policy	Approved SOMS policy with commitments to professional conduct, applicable law, human rights and continual improvement
Responsibilities	Role descriptions, responsibility matrix, escalation chart and authority levels
Communication	Briefings, supervisor instructions, toolbox talks and management messages
Accountability	Disciplinary rules, incident escalation and management review actions

CLAUSE 6 - PLANNING

Planning should address risks and opportunities that may affect security operations and SOMS outcomes. This includes operational threats, client requirements, human rights risks, legal compliance risks and the potential impact of security actions on people and communities.

- Define a method for identifying and evaluating security operations risks.
- Identify risks related to personnel, clients, deployment locations, weapons or equipment, communications, transport, subcontractors and information.
- Plan treatment actions and assign owners, due dates and effectiveness checks.
- Set measurable objectives for operational performance, legal compliance, training, incident reduction, response times, client satisfaction and corrective action closure.

Climate action consideration: Amendment 1:2024 requires organizations to consider whether climate change is a relevant issue for the management system. For security operations, this may include extreme weather, site accessibility, emergency response capability, workforce safety, community tensions and continuity of deployed services.

CLAUSE 7 - SUPPORT

Support processes provide the resources, competence, awareness, communication and documented information required to run controlled security operations.

Support area	Implementation guidance
Resources	Provide personnel, equipment, PPE, vehicles, communications tools, IT systems and facilities appropriate to security operations.
Competence	Define competence criteria for guards, supervisors, control room personnel, investigators, drivers, management and support teams.
Awareness	Ensure personnel understand the policy, code of conduct, human rights duties, escalation rules, incident reporting and consequences of noncompliance.
Communication	Define internal, client, regulator, emergency and public communication arrangements.
Documented information	Control procedures, forms, deployment instructions, records, revisions, approvals, retention and secure access.

CLAUSE 8 - OPERATION

Operational control is the core of ISO 18788 implementation. The organization should plan, implement and control the processes needed to meet client requirements while maintaining lawful and accountable conduct.

- Plan deployments based on contract requirements, site risks, staffing needs and supervision arrangements.
- Control selection, vetting, induction, training and assignment of personnel.
- Maintain procedures for use of force, weapons, equipment, searching, detention support, emergency support and incident response where applicable.
- Control subcontracted services and partner organizations.
- Protect client information, operational data and security-sensitive records.
- Maintain logs for attendance, patrols, handover, incidents, equipment issue, vehicle use and communications.

Operational evidence is essential. The Stage 2 assessment should be able to trace a security contract from risk review and planning through deployment, supervision, incident handling, client reporting and improvement.

HUMAN RIGHTS AND USE OF FORCE CONTROLS

Respect for human rights is a central consideration for security operations. The SOMS should include practical controls to prevent abuse, excessive force, unlawful conduct, discrimination and inappropriate treatment of affected persons.

Control topic	Expected controls
Code of conduct	Rules for professional behaviour, lawful conduct, confidentiality, anti-bribery and respect for affected persons
Use of force	Clear authorization, proportionality, reporting, investigation and review requirements
Weapons and equipment	Authorization, issue and return records, safe storage, competence and compliance with applicable law
Detention or restraint support	Defined limits of authority, escalation, documentation and protection of individuals
Vulnerable persons	Awareness for children, elderly persons, persons with disabilities and other vulnerable groups
Complaints and grievances	Accessible complaint channels and impartial review of allegations

SECURITY RISK ASSESSMENT AND THREAT TREATMENT

A security operations risk assessment should identify threats and vulnerabilities that may affect personnel, clients, assets, communities, information and service continuity.

- Define risk criteria for likelihood, impact, exposure, legal implications and human rights severity.
- Identify threats such as theft, intrusion, violence, civil unrest, insider compromise, information leakage, vehicle attack, kidnap, sabotage and public disorder.
- Assess risks by contract, site, route, task, personnel category or operational context.
- Define controls such as supervision, access control, communications, route planning, emergency response, training and liaison with authorities.
- Review risk assessments after incidents, contract changes, location changes and major environmental or social changes.

Risk register field	Example content
Activity / site	Warehouse guarding, VIP protection, event security, cash escort, mobile patrol
Threat	Unauthorized access, crowd disorder, hostile actor, information leakage, equipment misuse
Impact	Injury, legal breach, client loss, human rights allegation, service interruption
Controls	Screening, supervision, patrol route, communications, PPE, escalation, client briefing
Residual risk	Risk remaining after controls and further treatment actions

PERSONNEL VETTING, COMPETENCE AND AWARENESS

Private security operations depend on reliable and competent personnel. Recruitment, screening, training and ongoing supervision should be controlled through documented processes.

Personnel control	Implementation guidance
Screening and vetting	Verify identity, qualifications, licenses, experience, background checks and legal eligibility as applicable.
Contracts and commitments	Use confidentiality, code of conduct, conflict of interest and disciplinary acknowledgement forms.
Initial training	Cover SOMS policy, client requirements, legal duties, human rights, emergency response, incident reporting and use of force rules.
Role-specific competence	Define additional requirements for supervisors, drivers, weapons handlers, control room staff and close protection teams.
Ongoing evaluation	Use site inspections, supervisor observations, incident reviews and refresher training to maintain competence.

SUPPLIER, SUBCONTRACTOR AND PARTNER CONTROLS

Where security operations are supported by subcontractors, consultants, equipment providers, training bodies or partners, the organization should control their selection, approval, performance and continued suitability.

- Define criteria for supplier and subcontractor approval.
- Ensure subcontracted security personnel meet licensing, competence, screening and code-of-conduct requirements.
- Include legal, human rights, confidentiality and reporting obligations in agreements.
- Monitor performance through inspections, incident reviews, client feedback and compliance checks.
- Maintain approved supplier lists, evaluations, contracts, insurance and corrective action records.

Implementation point: Outsourcing does not remove accountability. The organization should retain control over outsourced processes that affect conformity, legal compliance, human rights and client requirements.

INCIDENT REPORTING, COMPLAINTS AND GRIEVANCE MECHANISMS

Incidents, complaints and grievances provide important evidence of operational control and improvement. The system should encourage accurate reporting and prevent retaliation or suppression of concerns.

Mechanism	What to define	Typical records
Incident reporting	What must be reported, timing, escalation, investigation and client notification.	Incident reports, witness statements, photos, supervisor review
Complaint handling	How clients, employees and affected persons can raise concerns.	Complaint log, acknowledgement, investigation, closure response
Grievance mechanism	Fair and accessible channel for allegations involving misconduct or harm.	Grievance records, investigation notes, corrective actions
Lessons learned	How repeated or serious events lead to system changes.	Trend analysis, revised procedures, training updates

CLAUSE 9 - PERFORMANCE EVALUATION

The organization should evaluate whether the SOMS is implemented and effective. Performance evaluation should cover both head-office controls and field-level operational evidence.

- Monitor objectives, security incidents, complaints, response times, staffing levels, training completion, patrol performance and corrective action closure.
- Conduct internal audits against ISO 18788, legal requirements, client obligations and internal procedures.
- Review operational performance with top management and decide improvement actions.
- Use client feedback, supervisor reports, incident trends and compliance results to evaluate effectiveness.

Performance indicator	Example measure
Training completion	Percentage of assigned staff trained before deployment
Incident reporting timeliness	Percentage of incidents reported within defined time
Client complaints	Number, severity and closure time of complaints
Patrol conformity	Completed patrols versus planned patrols
Corrective action closure	Actions closed on time and verified effective
Compliance	Licensing, legal and contract requirements maintained

CLAUSE 10 - IMPROVEMENT

Improvement should be driven by incidents, audit findings, complaints, management review outputs, changes in risk, client feedback and operational lessons learned.

- Define how nonconformities are reported and controlled.
- Investigate causes of incidents and failures rather than only correcting symptoms.
- Take corrective action proportionate to operational risk and human rights impact.
- Verify whether actions are effective.
- Update risk assessments, procedures, training and controls when necessary.
- Maintain evidence of continual improvement over time.

Readiness check: A mature SOMS can show how a field incident or complaint was logged, investigated, corrected, reviewed by management and converted into improved operational controls.

DOCUMENTED INFORMATION TOOLKIT

The following documents and records are commonly useful when implementing ISO 18788. The exact structure should be scaled to the organization and should reflect actual operations.

Document / record	Purpose
SOMS scope and policy	Defines boundaries and leadership commitments
Context and interested parties register	Captures internal/external issues and stakeholder requirements
Legal and contractual obligations register	Tracks applicable law, licenses, permits and client requirements
Security operations risk assessment	Identifies threats, risks, controls and residual risk
Human rights risk assessment	Identifies risks of harm or abuse and related safeguards
Operational procedures and post orders	Controls daily field activities and supervisor expectations
Personnel screening and competence records	Shows staff suitability, training and role authorization
Incident, complaint and grievance logs	Maintains accountability and evidence of response
Internal audit and management review records	Demonstrates evaluation and governance
Corrective action register	Tracks root cause, action, responsibility and closure

CERTIFICATION READINESS CHECKLIST

Use the checklist below before scheduling certification assessment activity.

- Scope is approved and accurately reflects security operations.
- Policy is approved, communicated and understood.
- Roles, responsibilities and escalation lines are defined.
- Applicable legal, regulatory and contractual requirements are identified.
- Security operations risk assessment is completed and current.
- Human rights risks and controls are addressed.
- Personnel vetting, competence and training records are available.
- Operational SOPs, post orders and deployment instructions are implemented.
- Incident, complaint and grievance mechanisms are active.
- Subcontractors and suppliers are evaluated and controlled.
- Internal audit has covered all applicable SOMS processes.
- Management review has been completed with actions recorded.
- Corrective actions are tracked, closed and verified for effectiveness.

90-DAY IMPLEMENTATION PLANNER

Period	Focus	Key deliverables
Days 1-15	Project launch and scope	Implementation plan, SOMS scope, responsibilities and communication plan
Days 16-30	Context and obligations	Interested parties register, legal/contractual obligations register, policy draft
Days 31-45	Risk and human rights review	Security risk assessment, human rights risk review and treatment plan
Days 46-60	Operational controls	SOPs, post orders, incident process, complaint process and supplier controls
Days 61-75	Training and implementation	Training records, staff briefings, deployment evidence and operational logs
Days 76-85	Internal audit	Internal audit plan, findings, corrective actions and readiness review
Days 86-90	Management review and closure	Management review minutes, action closure and Stage 1 readiness pack

FREQUENTLY ASKED QUESTIONS

1. Is ISO 18788 only for armed security companies?

No. ISO 18788 can apply to organizations conducting or contracting private security operations and related activities. The controls should be scaled to the nature, risk and legal context of the services performed.

2. Can ISO 18788 be integrated with ISO 9001?

Yes. Many organizations integrate client requirements, document control, corrective action and performance evaluation with their quality management system, while adding specific security operations and human rights controls required for ISO 18788.

3. What is the most important preparation for Stage 2?

The organization should show implemented evidence from actual operations, including contract review, site risk assessment, deployment controls, training, supervision, incident reporting and improvement records.

4. Does the standard require human rights consideration?

Yes. The SOMS should demonstrate accountability to law and respect for human rights in security operations, including conduct, reporting, investigation and grievance controls.

5. What records are most commonly requested during assessment?

Typical records include legal registers, risk assessments, training and vetting records, post orders, incident logs, complaint records, subcontractor evaluations, internal audit reports, management review minutes and corrective actions.

End of guide