PFGsec

PRACTICAL RESOURCE · AUGUST 2026

GRC & COMPLIANCE

ISO 27001 Readiness Checklist

Actionable checklist for implementation and audit preparation.

Use this working checklist to assess whether the Information Security Management System is defined, operating and supported by evidence before certification activities begin.

PFGsec Consulting Services Ltd.

PFG ISO CK 001 · Version 1.0

Seven readiness areas

Clauses 4 to 10, Annex A implementation, evidence and certification preparation.

00 CHECKLIST GUIDE

Use evidence, not confidence, to determine readiness

Complete the checklist with control owners and retain the evidence used to support every readiness decision. Record gaps in the action tracker and retest before the certification audit.

Status definitions

Ready

Requirement is implemented, operating and supported by current evidence.

Partial

Design exists but implementation, coverage or evidence is incomplete.

Gap

Requirement is absent, ineffective or not supported by reliable evidence.

Not applicable

Use only with a documented and defensible rationale.

Suggested readiness threshold. All mandatory management system requirements should be Ready. Material Annex A controls should be operating and evidenced. Gaps should have approved owners, due dates and risk treatment.

Organization profile

ORGANIZATION

ASSESSMENT DATE

ISMS SCOPE

ASSESSMENT LEAD

TARGET CERTIFICATION DATE

CERTIFICATION BODY

Readiness scorecard

No.	Readiness area	R	P	G
01	Organization context and ISMS scope	☐	☐	☐
02	Leadership, policy and governance	☐	☐	☐
03	Planning, risk assessment and treatment	☐	☐	☐
04	Support and documented information	☐	☐	☐
05	Operational controls and Annex A implementation	☐	☐	☐
06	Performance evaluation and assurance	☐	☐	☐
07	Improvement and certification readiness	☐	☐	☐

SCORING RULE

Do not average away a critical gap. A single unresolved scope, risk, internal audit, management review or corrective action failure may prevent readiness.

EVIDENCE QUALITY TEST

Evidence should be current, attributable, complete, protected and representative of normal operation.

01 ORGANIZATION CONTEXT AND ISMS SCOPE

Organization context and ISMS scope

Confirm that the management system is anchored to business context, interested parties and a defensible scope.

PAGE RESULT
R P G

Ref.	Readiness checkpoint	Minimum evidence	R P G NA
4.1	**Internal and external issues affecting information security are identified and reviewed.**	Current context analysis covering business model, technology, regulation, threat exposure, suppliers and strategic change.	R P G NA
4.1 Amd	**The organization has determined whether climate change is relevant to the ISMS context.**	Documented relevance decision and any resulting risks, obligations or continuity considerations.	R P G NA
4.2	**Interested parties and their information security requirements are identified.**	Register of customers, regulators, employees, suppliers, shareholders and other relevant parties with applicable requirements.	R P G NA
4.2 Amd	**Relevant interested parties that may have climate related requirements are considered.**	Evidence that contractual, regulatory, customer or resilience expectations were considered where applicable.	R P G NA
4.3	**The ISMS scope is defined with clear organizational and technical boundaries.**	Approved scope statement covering entities, locations, processes, services, systems, information and exclusions.	R P G NA
4.3	**Interfaces and dependencies between in scope and out of scope activities are understood.**	Boundary diagram, service map, dependency register and supplier interfaces.	R P G NA
4.3	**Scope exclusions are justified and do not undermine the intended outcomes of the ISMS.**	Documented rationale with management approval and risk consideration.	R P G NA
4.4	**Core ISMS processes and their interactions are defined.**	ISMS process map showing governance, risk, control operation, assurance, incident response and improvement.	R P G NA
4.4	**Information security obligations are traceable to controls and owners.**	Obligations register mapped to policies, controls, evidence and accountable owners.	R P G NA
4.4	**The scope and context are reviewed after material business or technology change.**	Review cadence, change triggers and recent review records.	R P G NA

Key gaps and evidence requested

02 LEADERSHIP, POLICY AND GOVERNANCE

Leadership, policy and governance

Verify that leadership actively directs the ISMS, assigns authority and resolves material risk decisions.

PAGE RESULT
R P G

Ref.	Readiness checkpoint	Minimum evidence	R P G NA
5.1	**Top management demonstrates accountability for the effectiveness of the ISMS.**	Executive sponsorship, governance minutes, decisions, funding and evidence of oversight.	R P G NA
5.1	**Information security objectives and requirements are integrated into business processes.**	Business planning, project, procurement, change and operational processes include security requirements.	R P G NA
5.1	**Management supports risk based decisions and removes barriers to implementation.**	Approved risk treatments, accepted residual risks, funded actions and escalated decisions.	R P G NA
5.1	**The importance of effective information security is communicated.**	Leadership communications, awareness activities and management expectations.	R P G NA
5.2	**An information security policy is approved, appropriate and available.**	Current approved policy aligned to organizational purpose, strategic direction and applicable obligations.	R P G NA
5.2	**The policy commits to meeting applicable requirements and continual improvement.**	Explicit commitments within the policy and supporting governance practices.	R P G NA
5.2	**The policy is communicated and available to relevant interested parties.**	Publication record, employee acknowledgement and external availability where appropriate.	R P G NA
5.3	**ISMS roles, responsibilities and authorities are assigned.**	Role descriptions, RACI, committee terms of reference and named control owners.	R P G NA
5.3	**Conflicts of interest and separation of duties are considered in role design.**	Role review, approval workflow and compensating controls for unavoidable conflicts.	R P G NA
5.3	**Information security performance and material issues are reported to management.**	Defined reporting cadence, dashboard, escalation criteria and recent reports.	R P G NA

Key gaps and evidence requested

03 PLANNING, RISK ASSESSMENT AND TREATMENT

Planning, risk assessment and treatment

Confirm that risk drives priorities, selected controls and the Statement of Applicability.

PAGE RESULT
R P G

Ref.	Readiness checkpoint	Minimum evidence	R P G NA
6.1.1	**Risks and opportunities affecting the intended outcomes of the ISMS are identified.**	Planning record linking context, objectives, risks, opportunities and actions.	R P G NA
6.1.2	**A repeatable information security risk assessment method is defined.**	Approved methodology covering criteria, likelihood, consequence, risk levels and acceptance rules.	R P G NA
6.1.2	**Risk criteria are consistent and support comparable results.**	Defined scales, thresholds, examples and calibration guidance.	R P G NA
6.1.2	**Risk owners are assigned and participate in assessment and acceptance decisions.**	Current risk register with named owners, approvals and review dates.	R P G NA
6.1.2	**Assessments identify risks to confidentiality, integrity and availability.**	Risk scenarios linked to information, services, threats, vulnerabilities and business consequences.	R P G NA
6.1.3	**Risk treatment options are selected and documented.**	Treatment plan showing avoid, modify, share or retain decisions with accountable owners.	R P G NA
6.1.3	**Necessary controls are determined from risk and obligations, not Annex A alone.**	Control selection rationale linked to risks, laws, contracts and business requirements.	R P G NA
6.1.3	**Selected controls are compared with Annex A to confirm no necessary control was omitted.**	Annex A comparison review and documented conclusions.	R P G NA
6.1.3	**The Statement of Applicability is current and complete.**	Control inclusion, implementation status, justification and exclusion rationale for all Annex A controls.	R P G NA
6.1.3	**Risk treatment plans and residual risks are approved by risk owners.**	Signed approvals, due dates, resources and accepted residual risk.	R P G NA
6.2	**Measurable information security objectives are established.**	Objectives with measures, targets, owners, resources, due dates and evaluation method.	R P G NA
6.3	**Changes to the ISMS are planned and controlled.**	Change assessment considering purpose, consequences, resources, responsibilities and integrity of the ISMS.	R P G NA

Key gaps and evidence requested

04 SUPPORT AND DOCUMENTED INFORMATION

Support and documented information

Check that people, competence, communication and controlled information can sustain the ISMS.

PAGE RESULT
R P G

Ref.	Readiness checkpoint	Minimum evidence	R P G NA
7.1	**Resources required to establish, operate and improve the ISMS are provided.**	Approved budget, staffing, tooling, external support and implementation plan.	R P G NA
7.2	**Required competence is defined for security and control roles.**	Competence matrix, role requirements and development plans.	R P G NA
7.2	**People performing relevant work are competent based on education, training or experience.**	Training records, certifications, experience evidence and competence evaluation.	R P G NA
7.3	**Personnel understand the policy, their contribution and consequences of nonconformance.**	Awareness programme, acknowledgements, testing and role specific briefings.	R P G NA
7.4	**Internal and external communication requirements are defined.**	Communication matrix covering subject, timing, audience, owner, method and approval.	R P G NA
7.5.1	**Documented information required by the standard and the organization is available.**	Controlled document register including mandatory and risk driven information.	R P G NA
7.5.2	**Documents are clearly identified, reviewed and approved before use.**	Naming, version, owner, review date, approval and classification metadata.	R P G NA
7.5.3	**Access, distribution, storage, retention and disposal are controlled.**	Document control procedure, permissions, retention schedule and disposal evidence.	R P G NA
7.5.3	**External documents needed for the ISMS are identified and controlled.**	Register of standards, laws, contracts, supplier documents and authoritative guidance.	R P G NA
7.5.3	**Records remain legible, attributable, retrievable and protected from unauthorized change.**	Evidence repository controls, audit trail, backup and access review.	R P G NA

Key gaps and evidence requested

05 OPERATIONAL CONTROLS AND ANNEX A IMPLEMENTATION

Operational controls and Annex A implementation

PAGE RESULT
R P G

Verify that planned controls operate consistently and produce reliable evidence.

Ref.	Readiness checkpoint	Minimum evidence	R P G NA
8.1	**Operational processes needed to meet security requirements are planned and controlled.**	Operating procedures, control schedules, service workflows and acceptance criteria.	R P G NA
8.1	**Planned changes are controlled and unintended changes are reviewed.**	Change records, risk assessment, testing, approval, rollback and post implementation review.	R P G NA
8.1	**Externally provided processes, products and services are controlled.**	Supplier due diligence, contracts, control requirements, monitoring and exit arrangements.	R P G NA
8.2	**Risk assessments are performed at planned intervals and after significant change.**	Assessment schedule, trigger criteria and completed assessments.	R P G NA
8.3	**Risk treatment plans are implemented and progress is tracked.**	Treatment tracker, implementation evidence, overdue escalation and closure verification.	R P G NA
A.5	**Organizational controls have owners, procedures and evidence.**	Governance, asset, access, supplier, incident, continuity, legal and compliance records.	R P G NA
A.6	**People controls are implemented across the employment lifecycle.**	Screening, terms, awareness, disciplinary process, role change and termination records.	R P G NA
A.7	**Physical controls protect sites, equipment and supporting facilities.**	Access controls, monitoring, environmental protection, equipment security and disposal evidence.	R P G NA
A.8	**Technological controls are implemented and monitored.**	Identity, endpoint, network, logging, vulnerability, configuration, data, cloud and secure development evidence.	R P G NA
SoA	**Every applicable Annex A control has implementation evidence proportionate to risk.**	Control design, owner, operating frequency, evidence source and effectiveness result.	R P G NA
SoA	**Excluded Annex A controls have clear, defensible justification.**	Documented exclusion rationale confirming the control is not necessary for risk treatment or obligations.	R P G NA
Operations	**Exceptions are time bound, approved and monitored.**	Exception register with risk, owner, expiry date, compensating controls and closure evidence.	R P G NA

Key gaps and evidence requested

06 PERFORMANCE EVALUATION AND ASSURANCE

Performance evaluation and assurance

Confirm that management can evaluate performance, audit the ISMS and make evidence based decisions.

PAGE RESULT
R P G

Ref.	Readiness checkpoint	Minimum evidence	R P G NA
9.1	**The organization defines what will be monitored and measured.**	Measurement framework covering controls, objectives, risk, incidents, compliance and improvement.	R P G NA
9.1	**Methods, frequency, responsibilities and evaluation criteria are defined.**	Metric definitions, data sources, cadence, owners, thresholds and analysis method.	R P G NA
9.1	**Results are analyzed, evaluated and retained as evidence.**	Dashboards, trend analysis, decisions, actions and retained source data.	R P G NA
9.2.1	**Internal audits are conducted at planned intervals.**	Approved audit programme covering scope, criteria, methods, responsibilities and schedule.	R P G NA
9.2.1	**Audits evaluate both conformity and effective implementation.**	Audit work papers, samples, interviews, evidence and conclusions.	R P G NA
9.2.2	**Auditors are objective and independent of the activities audited.**	Auditor competence, independence assessment and conflict management.	R P G NA
9.2.2	**Audit findings are reported and corrective actions are tracked.**	Audit report, finding log, owners, due dates, root cause and closure verification.	R P G NA
9.3	**Management reviews the ISMS at planned intervals.**	Agenda, attendance and minutes covering all required review inputs.	R P G NA
9.3	**Management review decisions address improvement, changes and resources.**	Recorded decisions, actions, owners, deadlines and follow through.	R P G NA
9.3	**Changes in context, interested parties, risks and performance inform management review.**	Current inputs including trends, incidents, audit results, objectives, suppliers and opportunities.	R P G NA

Key gaps and evidence requested

07 IMPROVEMENT AND CERTIFICATION READINESS

Improvement and certification readiness

Close material gaps, prove corrective action effectiveness and prepare a complete audit evidence set.

PAGE RESULT
R P G

Ref.	Readiness checkpoint	Minimum evidence	R P G NA
10.1	**Opportunities to improve the suitability, adequacy and effectiveness of the ISMS are identified.**	Improvement register linked to performance, audits, incidents, changes and management review.	R P G NA
10.2	**Nonconformities are contained and corrected without undue delay.**	Issue record, immediate correction and impact assessment.	R P G NA
10.2	**Root causes are evaluated and actions prevent recurrence.**	Root cause analysis, corrective action plan and cross impact review.	R P G NA
10.2	**Corrective actions are proportionate and their effectiveness is verified.**	Completion evidence, effectiveness test and closure approval.	R P G NA
Stage 1	**The scope, policy, risk method, risk register, treatment plan and SoA are approved.**	Controlled versions available in the audit repository.	R P G NA
Stage 1	**Mandatory processes and documented information are established.**	Document index mapped to clauses and evidence owners.	R P G NA
Stage 1	**The organization has completed internal audit and management review.**	Recent reports, findings, decisions and follow up actions.	R P G NA
Stage 2	**Controls have operated long enough to produce representative evidence.**	Operating samples covering the defined audit period and control frequency.	R P G NA
Stage 2	**Personnel can explain their roles and demonstrate control operation.**	Interview preparation, role briefings and evidence walkthroughs.	R P G NA
Stage 2	**Open findings and exceptions are understood and actively managed.**	Current issue register, risk acceptance, remediation dates and management visibility.	R P G NA
Audit	**A controlled evidence request and response process is ready.**	Evidence coordinator, tracker, secure repository, naming standard and quality review.	R P G NA
Audit	**Certification body scope and audit logistics are confirmed.**	Engagement plan, sites, remote access, sampling, schedule and participant availability.	R P G NA

Key gaps and evidence requested

08 EVIDENCE PACK AND ACTION TRACKER

Convert checklist gaps into controlled actions and a reliable audit evidence pack

Use the evidence index to confirm completeness, then record every unresolved item with an owner, deadline and validation method.

Minimum evidence pack

- [ ] **Approved ISMS scope and context analysis**
- [ ] **Interested parties and obligations register**
- [ ] **Information security policy and objectives**
- [ ] **Risk methodology, register and treatment plan**
- [ ] **Statement of Applicability**
- [ ] **Control ownership and operating procedures**
- [ ] **Competence and awareness records**
- [ ] **Monitoring and measurement results**
- [ ] **Internal audit programme and report**
- [ ] **Management review minutes and decisions**
- [ ] **Corrective action and improvement register**
- [ ] **Representative control evidence for the audit period**

AUDIT PREPARATION RULE

Do not upload evidence without checking that it answers the request, matches the scope, identifies the source and demonstrates the relevant period.

Final readiness decision

- [ ] **Ready for Stage 1**
- [ ] **Ready for Stage 2**
- [ ] **Conditional readiness**
- [ ] **Not ready**

ASSESSMENT LEAD _____ DATE _____

EXECUTIVE SPONSOR _____ DATE _____

RELEASE GATE

Proceed only when scope is stable, mandatory processes are complete, internal audit and management review are closed, and material control evidence is available.

09 READINESS ACTION TRACKER

Assign every unresolved gap to an owner, deadline and validation method

Use this tracker for checklist items marked Partial or Gap. Close actions only after implementation and evidence have been independently checked.

ID	Gap or action	Owner	Due date	Priority	Status
01					
02					
03					
04					
05					
06					
07					
08					
09					
10					
11					
12					

Validation method

Escalation and decisions