

RESEARCH BRIEFING · AUSTRALIA

ISO Standards in Australia

Certification, Compliance and Checklists

A practical guide to the Australian certification system covering ISO 9001, 14001, 45001, 27001 and related management-system standards used across industries.

Includes the JAS-ANZ accreditation model, Stage 1 / Stage 2 audit process, ongoing surveillance, industry mapping, and clause-level compliance checklists.

SEPTEMBER 2026

Contents

1. Purpose, scope and how to use this report
2. How ISO certification works in Australia
3. The generic path to certification and remaining certified
4. Time, cost and common failure points
5. Which standard for which industry
6. ISO 9001 — Quality management
7. ISO 14001 — Environmental management (including the 2026 edition)
8. ISO 45001 — Occupational health and safety
9. ISO/IEC 27001 — Information security
10. Other widely used ISO management-system standards
11. Sector schemes that sit on top of ISO 9001
12. Laboratory competence: ISO/IEC 17025 and NATA (accreditation, not certification)
13. Integrated management systems (IMS / “triple cert”)
14. Master compliance checklists
15. 12-month surveillance calendar
16. Australian legal overlays the auditor will expect you to know
17. Sources and verification points

Important. ISO does not certify organisations. In Australia, a JAS-ANZ-accredited certification body audits you against the standard and issues the certificate. JAS-ANZ accredits the certifier; it does not certify your business. Always confirm the certifier’s current scope on the JAS-ANZ public register before you sign a contract.

1. Purpose, scope and how to use this report

This report explains how International Organization for Standardization (ISO) management-system standards are used in Australia, what is required to become certified, and what is required to remain certified. It is written for owners, quality / WHS / environment / information-security managers, and organisations bidding into government or prime-contractor supply chains.

It covers the four standards most frequently specified in Australian tenders — ISO 9001 (quality), ISO 14001 (environment), ISO 45001 (occupational health and safety) and ISO/IEC 27001 (information security) — and then the next tier of standards that matter in particular industries: ISO 22000 and HACCP (food), ISO 13485 (medical devices), ISO 50001 (energy), ISO 22301 (business continuity), ISO/IEC 20000-1 (IT service management), ISO 37001 (anti-bribery), ISO 55001 (asset management), ISO 28000 (security in the supply chain), ISO/IEC 42001 (AI management), plus sector overlays such as IATF 16949 and AS9100. It also explains the separate Australian laboratory pathway under ISO/IEC 17025 through NATA.

What this report is not

- It is not a substitute for purchasing the official standard from Standards Australia / Intertek Inform or ISO. Certification audits are conducted against the copyrighted text.
- It is not legal advice. Certification does not replace Work Health and Safety Acts, environmental licences, the Privacy Act 1988, APRA CPS 234, TGA rules or food-safety law.
- It is not a quote. Audit days and consulting fees vary with headcount, sites, risk and scope.
- It does not endorse any certification body or consultant.

Versions current at September 2026

Standard	Usual certification edition	Australian designation	Notes
ISO 9001	ISO 9001:2015 (Amd 1:2024 climate)	AS/NZS ISO 9001:2016	A 2026 revision has been in the ISO pipeline through 2026. Confirm the edition named on your certificate and in any tender.
ISO 14001	ISO 14001:2026 (published 15 Apr 2026)	AS/NZS ISO 14001 (adopted editions)	Three-year transition from ISO 14001:2015; 2015 certificates must move to 2026 by about May 2029.
ISO 45001	ISO 45001:2018 (Amd 1:2024 climate)	AS/NZS ISO 45001:2018	AS/NZS 4801 withdrawn (2023). OHSAS 18001 certificates are invalid.
ISO/IEC 27001	ISO/IEC 27001:2022	AS ISO/IEC 27001:2022 (where adopted)	Annex A now has 93 controls in four themes. 2013 certificates are expired.
ISO 22000	ISO 22000:2018	AS ISO 22000:2019 (typical adoption)	Often paired with HACCP or a GFSI scheme (FSSC 22000, SQF, BRCGS).
ISO 13485	ISO 13485:2016	AS ISO 13485	Used with TGA conformity assessment; not a TGA licence by itself.
ISO 50001	ISO 50001:2018	AS/NZS ISO 50001	Energy performance, EnPIs, energy review.
ISO 22301	ISO 22301:2019	AS ISO 22301	BIA, RTO/RPO, exercise programme.
ISO/IEC 20000-1	ISO/IEC 20000-1:2018	AS ISO/IEC 20000.1	IT service management.
ISO/IEC 17025	ISO/IEC 17025:2017	AS ISO/IEC 17025	NATA accreditation of laboratories — not JAS-ANZ management-system certification.

Table 1. Editions commonly referenced in Australian certification and procurement as at September 2026.

2. How ISO certification works in Australia

2.1 The four-layer trust chain

ISO is a Geneva-based standards body. It writes standards. It does not visit your site and it does not issue certificates. What Australian buyers, agencies and primes usually mean by “ISO certified” is: an independent certification body (CB) has audited your management system against a named ISO (or AS/NZS ISO) standard and issued a certificate, and that CB is itself accredited by the Joint Accreditation System of Australia and New Zealand (JAS-ANZ) under ISO/IEC 17021.

Layer	Who	What they do
1. Standard writer	ISO (and IEC for some IT/security standards)	Publishes the requirements document (e.g. ISO 9001:2015).
2. National adoption	Standards Australia / Standards New Zealand	Often adopts the ISO text as AS/NZS ISO xxxx. Content is typically identical; tenders may use either designation.
3. Accreditation body	JAS-ANZ	Accredits CBs against ISO/IEC 17021 for named standards and industry scopes. JAS-ANZ is an IAF MLA signatory, so accredited certificates are recognised internationally.
4. Certification body	e.g. Intertek SAI Global, BSI, SGS, DNV, Bureau Veritas, Global-Mark, QMS, LRQA, TÜV SÜD and others	Audits your organisation (Stage 1 + Stage 2), issues the certificate, then runs annual surveillance and 3-year recertification.
Your organisation	The certified client	Owns the management system. Consultants can help build it; they cannot issue the certificate and should not also be the certifier.

Table 2. Who does what in the Australian ISO system.

2.2 ISO versus AS/NZS ISO

For the main management-system standards the Australian/New Zealand adoption is textually the same as the ISO original. A certificate to ISO 9001:2015 issued by a JAS-ANZ-accredited CB is treated as meeting a tender that says “AS/NZS ISO 9001”. The same applies to 14001 and 45001. Always read the tender: some schemes specify “certified to AS/NZS ISO xxxx by a JAS-ANZ accredited body” and will reject a cheap unaccredited or offshore certificate even if it carries an ISO logo.

2.3 Why JAS-ANZ accreditation is the practical requirement

Unaccredited certificates exist. They are rarely accepted for NSW Government, Victorian DTP, Queensland PQC, Austroads National Prequalification, Federal Safety Commissioner pathways, or major private primes. Before engaging a CB:

- Search the JAS-ANZ Register of Accredited Bodies (register.jasanz.org) for the legal name of the CB.
- Confirm the CB is accredited for the exact standard (9001, 14001, 45001, 27001, etc.).
- Confirm the CB’s accredited scope covers your industry (often expressed as NACE / ANZSIC activity codes — construction is a frequent example).
- Confirm the certificate will carry the JAS-ANZ accreditation symbol and a number you can verify.
- Ask whether combined (integrated) audits are available if you want more than one standard.

2.4 Certification is voluntary — market and law still bite

Holding an ISO certificate is almost never a statutory obligation in its own right. The legal duties sit in other instruments: model WHS laws and state WHS Acts, environmental protection licences, the Privacy Act and Australian Privacy Principles, APRA CPS 234 for prudentially regulated entities and their material service providers, TGA rules for medical devices, food standards and state food Acts, and contract law. Certification is the market’s preferred evidence that you have a systematic way of meeting those duties. In construction, infrastructure, defence, IT-for-government and many corporate panels it functions as a de facto licence to bid.

3. The generic path to certification and remaining certified

Almost every management-system standard uses the same lifecycle. The clauses differ; the project plan does not. Most CBs will not schedule Stage 2 until the system has been operating long enough to generate evidence — commonly at least one full internal-audit cycle and one management review, often framed as three months of live operation for first-time certifications.

3.1 Implementation sequence

Step	What happens	Evidence the auditor later wants
1. Decide the standard(s) and scope	Name sites, products/services, exclusions and justification. Scope that is too wide is expensive; scope that is too narrow fails tenders.	Written scope statement.
2. Secure leadership	Budget, a management representative or system owner, and a policy signed by top management.	Policy, org chart, resource plan.
3. Buy the standard	Purchase the official text. Do not implement from blogs.	Controlled copy of the standard.
4. Gap analysis	Map current practice to every shall-statement. Score gaps.	Gap report and action plan.
5. Context, interested parties, risks	Clause 4 and 6 work. Legal register. Risk/opportunity process.	Context paper, stakeholder matrix, risk register, legal register.
6. Design the system	Processes, responsibilities, documented information needed for control — not a shelf of generic manuals.	Process map, procedures where needed, forms, registers.
7. Implement and train	Run the system on real work. Competence and awareness records.	Training matrix, toolbox talks, induction records.
8. Operate and collect records	Nonconformities, incidents, customer complaints, monitoring data, supplier evaluations.	Live records, not empty templates.
9. Internal audit	Cover the whole system over the cycle. Auditors must be independent of the work they audit.	Audit programme, plans, reports, NCR close-out.
10. Management review	Top management reviews performance, resources, risks, audit results, improvement.	Agenda, minutes, actions with owners and dates.
11. Choose a JAS-ANZ CB	Quote by audit days (IAF MD5 methodology). Check impartiality — the CB cannot have designed your system.	Contract, audit programme.
12. Stage 1 audit	Readiness / documented-information review. Findings must be closed or accepted before Stage 2.	Stage 1 report.
13. Stage 2 audit	Implementation and effectiveness on site (or hybrid). Major nonconformities block the certificate until closed.	Stage 2 report, certificate.
14. Surveillance	Typically annual (sometimes 6-monthly for high risk). Sample of processes and sites.	Surveillance reports.
15. Recertification	Full system audit in year 3, before expiry.	New 3-year certificate.

Table 3. End-to-end certification lifecycle used by Australian CBs.

3.2 Audit findings language

- Major nonconformity — absence of a required process, or a failure that raises doubt the system can achieve its intended outcomes. Must be corrected and verified before certification is granted or restored.
- Minor nonconformity — isolated lapse. Corrective action plan is usually required; close-out is checked at the next visit or by desktop review.
- Opportunity for improvement / observation — not a failure. Ignoring a cluster of OFIs is how minors become majors next year.

3.3 Remaining compliant after the plaque goes on the wall

The certificate is valid for three years only if surveillance is passed. The system must keep running. Typical conditions of certification include: notify the CB of significant changes (ownership, sites, scope, major incidents, loss of key process); do not misuse the logo; pay surveillance fees; close findings in the agreed time. Certificates can be suspended or withdrawn. If you change CB, a transfer audit under IAF rules is used — you do not start from zero if the outgoing certificate is in good standing.

4. Time, cost and common failure points

Published ranges from Australian consultants and CBs for a small-to-medium single-site first certification typically sit in the following bands. These are planning figures, not quotes. Multi-site sampling, high-risk sectors, and ISO 27001 (because of risk assessment and control evidence) push costs up.

Cost element	Typical SME planning range (AUD)	What drives it
Official standard(s)	A few hundred dollars each	Must buy licensed copies.
Internal time	Often the largest cost	Process owners, training, record-keeping.
Consultant / system build (optional)	About \$7,000–\$25,000+ for one standard on a simple SME; more for 27001 or multi-site	Maturity of existing processes; how much is templated vs tailored.
Certification body (Stage 1 + 2)	Often several thousand to low tens of thousands	IAF mandatory audit days by employee numbers and risk; travel; integrated discounts.
Whole first-year package (build + certify), one standard, SME	Commonly quoted around \$12,000–\$25,000 all-in for simple 9001/45001/14001	Does not include your staff time.
Annual surveillance	Roughly 1/3 of the initial audit effort	Plus close-out of findings.
Year-3 recertification	Closer to a full system audit	Plan 6–9 months before expiry.

Table 4. Indicative cost architecture. Obtain current quotes; IAF MD5 and CB day-rates change.

Calendar time for a first certification is commonly 3–6 months for a well-run SME that already has basic procedures; 6–12 months is more realistic if culture, multi-site control or 27001 risk work is immature. Government tenders that “require ISO by the closing date” are the usual reason projects fail: Stage 2 cannot be pulled forward if there is no operating evidence.

Frequent reasons Stage 2 fails or is deferred

- The documented system does not match what people actually do (the “two-system” problem).
- Scope is vague, or exclusions are not justified.
- No legal/other-requirements register, or it is a generic download that misses state licences.
- Internal audits are a tick-box of the manual, not of live work; the internal auditor audited their own process.
- Management review is a toolbox talk with no inputs (audit results, objectives, incidents, customer data) and no outputs (decisions, resources).
- Objectives are slogans (“be the best”) rather than measurable targets with owners and timeframes.
- For 45001: consultation is a poster; workers cannot describe how they influence hazard controls.
- For 14001: significant aspects were never reviewed when the process changed; emergency drills are missing.
- For 27001: Statement of Applicability lists all 93 controls as “applicable” with identical justifications; Annex A is treated as a shopping list rather than a risk-treatment output.
- Certificate shopping with a non-JAS-ANZ body to hit a tender date — the certificate is then rejected by the buyer.

5. Which standard for which industry

No industry is required by ISO itself to hold any certificate. The table below reflects how Australian procurement and regulation actually behave. Always read the specific tender, prequalification deed or regulator guideline.

Industry / buyer	Usually expected	Often added	Notes
General professional services, manufacturing, logistics	ISO 9001	14001 or 45001 if sites or plant are material	Default “ISO” in many RFTs means 9001.
Civil construction & infrastructure (state prequal, Austroads, FSC-related work)	9001 + 45001	14001 above value/risk thresholds; Federal Safety Commissioner WHS accreditation is separate from ISO	Documented systems may suffice below ~\$1m; certified systems commonly required from ~\$1m–\$10m+ depending on scheme.
Mining, oil & gas, heavy industrial	45001 + 14001 + 9001	50001, 55001, 29001, 22301	Principal contractor prequal is the driver.
Facilities management	9001 + 45001 + 14001	41001 (FM), 50001	Triple cert is common on government FM panels.
IT, SaaS, digital government, fintech suppliers	27001 (+ often 9001)	20000-1, 22301, 42001 (AI)	APRA CPS 234 and Privacy Act overlay 27001. Peppol / eInvoicing providers face a 27001 mandate path through 2027.
Defence supply chain	9001 + 45001	27001, 28000, DISP membership	Security clearance and DISP are separate regimes.
Food manufacture, processing, export	HACCP and/or ISO 22000 or a GFSI scheme (SQF, BRCGS, FSSC 22000)	9001	State food Acts and FSANZ Code remain the law.
Medical devices	ISO 13485 + ARTG inclusion / TGA conformity assessment	9001 (weaker substitute), 14971 risk management	13485 is not itself a TGA certificate.
Healthcare, aged care, NDIS providers	Sector quality standards (NDIS Practice Standards, Aged Care Quality Standards)	9001, 45001	Use a CB also approved as an NDIS quality auditor where relevant.
Automotive supply	IATF 16949 (built on 9001)	14001, 45001	Customer-mandated.
Aerospace / aviation supply	AS9100 (built on 9001)	14001, 45001	OASIS database / IAQG rules apply.
Laboratories, calibration, inspection	NATA ISO/IEC 17025 or 17020 accreditation	9001 if the parent company wants a corporate QMS	Do not advertise NATA as “ISO certified”.
Energy-intensive sites, net-zero programmes	14001 and/or 50001	14064 GHG verification (different process)	Climate-change context is now explicit in HLS amendments.

Table 5. Practical Australian market mapping — not a legal mandate list.

6. ISO 9001 — Quality management systems

ISO 9001 is the most requested management-system certificate in Australian government and private procurement. It is a quality management system (QMS) standard: consistent products and services, controlled processes, competent people, and evidence that you improve when things go wrong. It does not prescribe how to make your product. The current dominant certification edition remains ISO 9001:2015 (including the 2024 climate-change amendment to clauses 4.1 and 4.2). A 2026 revision has been progressing through ISO during 2026 — treat the edition printed on the certificate and named in the RFT as controlling.

6.1 Seven quality management principles

Auditors do not score the principles as a separate checklist, but they explain why the clauses exist: customer focus; leadership; engagement of people; process approach; improvement; evidence-based decision making; relationship management.

6.2 Clause map (auditable clauses 4–10)

Clause	Title	What “good” looks like in an Australian audit
4.1–4.2	Context and interested parties	A living analysis of markets, regulation, capacity and parties (customers, regulators, staff, suppliers). Climate change must be considered as an external issue and, if relevant to parties, as a need/expectation.
4.3–4.4	Scope and QMS processes	Scope names sites and services. Process map shows interactions, owners, inputs/outputs, criteria and risks. Exclusions (usually only 8.3 design) are justified.
5	Leadership	Policy is known, not laminated and forgotten. Top management can discuss objectives, risks and customer performance without reading a script.
6.1–6.2	Risks, opportunities, objectives	Risks tied to processes (not a generic SWOT slide). Objectives are SMART, deployed to relevant functions, with plans.
6.3	Planning of changes	Changes to the QMS are planned — software cutovers, new sites, new product lines.
7.1–7.5	Support	People, infrastructure, process environment, monitoring resources (calibration), organisational knowledge, competence, awareness, communication, controlled documented information.
8.1–8.2	Operation and customer requirements	Orders/tenders are reviewed before commitment. Changes to requirements are controlled.
8.3	Design and development	Only if you design. Inputs, controls, outputs, reviews, verification, validation, change control.
8.4	Externally provided processes	Supplier evaluation, incoming control, outsourced process control — a frequent tender weak spot.
8.5–8.7	Production/service, identification, NCR product	Work instructions where needed, identification and traceability if required, preserved product, control of nonconforming outputs.
9	Performance evaluation	Process KPIs, customer satisfaction, analysis, internal audit programme, management review with the full 9.3 agenda.
10	Improvement	Nonconformity and corrective action that finds root cause; continual improvement that is more than “we had a meeting”.

Table 6. ISO 9001 clause intent.

6.3 Documented information — what is actually mandatory

ISO 9001:2015 killed the compulsory quality manual and the six named procedures of the 2008 edition. You must maintain (keep current) documented information for: the scope (4.3); information needed to support process operation (4.4 / 8.1); the quality policy (5.2); and quality objectives (6.2). You must retain (keep as evidence) records including competence (7.2); calibration/verification of monitoring resources (7.1.5); review of product/service requirements (8.2.3); design records if 8.3 applies; supplier evaluation (8.4); release of product/service (8.6); nonconforming outputs (8.7); monitoring results (9.1); internal audits (9.2); management review (9.3); and nonconformity/corrective action (10.2). Everything else is required only if you need it to control the process.

6.4 Australian overlays

- Consumer law and Australian Consumer Law guarantees sit outside the standard but appear as “legal requirements” in clause 8.2 / 8.5.
- Measurement traceability for calibrated equipment should run to NATA-accredited labs or equivalent where accuracy matters.
- Government prequalification often wants the certificate plus a quality plan for the specific contract — the certificate alone is not the quality plan.

7. ISO 14001 — Environmental management systems

ISO 14001 specifies an environmental management system (EMS). It does not set emission limits. It requires you to know your environmental aspects and impacts, comply with legal and other requirements, set objectives, control operations and emergencies, and improve environmental performance. ISO 14001:2026 was published on 15 April 2026 and replaces ISO 14001:2015 (which had already absorbed a 2024 climate-change amendment). The transition period is

three years: 2015 certificates need to move to the 2026 edition by about May 2029. Changes are widely described as moderate: clearer risk-and-opportunity language, a broader set of environmental conditions in context analysis (climate, pollution, biodiversity, natural-resource availability), alignment with ISO’s Harmonized Structure, and a substantially expanded Annex A guidance. Organisations already competent against 2015 should not need a rebuild.

7.1 Clause intent

Clause	Title	Australian audit focus
4	Context, parties, scope	Include climate and other environmental conditions. Neighbours, EPA / state regulator, Traditional Owners, councils and lenders are typical interested parties.
5	Leadership and policy	Policy commits to protection of the environment (including prevention of pollution), fulfilment of compliance obligations, and improvement.
6.1.2	Environmental aspects	Lifecycle perspective — not only what happens on your site. Criteria for significance. Update when processes, materials or suppliers change.
6.1.3	Compliance obligations	A legal register that names actual instruments: EPBC Act where relevant, state EP Acts, licences, trade-waste agreements, waste classifications, PFAS or contaminated-land duties, NGER if a controlling corporation, planning consents.
6.2	Objectives	Tied to significant aspects and compliance risk — not generic “reduce paper”.
7	Support	Competence for environmentally critical roles (e.g. spill response, licensed waste). Communication including complaints.
8.1	Operational control	Work instructions, contractor control, design and procurement influence on lifecycle impacts.
8.2	Emergency preparedness	Spill, firewater, flood, hazardous-chemical release. Tests/drills and post-drill learning.
9.1.2	Evaluation of compliance	A planned process to check licence conditions — not an assumption that “we have a licence so we comply”.
9.2–9.3 / 10	Audit, review, improvement	Same HLS machinery as 9001, with environmental performance data as the input.

Table 7. ISO 14001 clause intent in the Australian regulatory setting.

7.2 Mandatory documented information (14001:2026 — substantially the same list as 2015)

- Maintain: scope (4.3); environmental policy (5.2); risks/opportunities and processes needed (6.1.1 / 6.1.4); criteria for significant aspects (6.1.2); compliance obligations (6.1.3); environmental objectives (6.2); operational control information as needed (8.1); emergency preparedness and response (8.2).
- Retain: competence (7.2); communications evidence (7.4); monitoring and measurement results (9.1.1); compliance-evaluation evidence (9.1.2); internal audits (9.2); management review (9.3); nonconformity and corrective action (10.2); plus evidence that operational controls and emergency tests occurred.

7.3 Certification does not replace the EPA

An ISO 14001 certificate is not an environment protection licence, planning permit, or EPBC approval. Auditors will look for the licence and for monitoring data that the licence requires. If you are in non-compliance with a licence condition, a mature EMS records it as a nonconformity and treats it; hiding it is both a legal and an audit problem.

8. ISO 45001 — Occupational health and safety

ISO 45001:2018 (with the 2024 climate amendment to context clauses) is the current OH&S management-system standard. It superseded OHSAS 18001 and, in Australia and New Zealand, AS/NZS 4801:2001 — which Standards Australia withdrew in 2023. New certifications against 4801 are not available. ISO 45001 does not replace the model Work Health and Safety Act (adopted in all jurisdictions except Victoria, which has the Occupational Health and Safety Act 2004) or the regulations and codes of practice under those Acts. It is a systematic way of discharging the primary duty of care and due-diligence duties of officers.

8.1 What is distinctive about 45001

- Workers are interested parties by definition. Clause 5.4 requires both consultation (seeking views before a decision) and participation (involving workers in decision-making), with emphasis on non-managerial workers.
- Hazard identification is proactive and ongoing — not a one-off SWMS library created for a tender.
- The hierarchy of control is expected in operational planning (eliminate, substitute, engineer, administer, PPE).
- Outsourcing, procurement and contractors (8.1.4) are in scope — a major issue on Australian construction and labour-hire sites.
- There is an explicit process to evaluate compliance with legal and other requirements (9.1.2), analogous to 14001.
- The standard covers work-related ill health (psychosocial hazards, occupational disease) as well as injury. Safe Work Australia’s model Code of Practice on managing psychosocial hazards is now part of the “legal and other requirements” conversation in most jurisdictions.

8.2 Clause map

Clause	Title	Australian audit focus
4	Context, workers and other parties, scope	Include labour-hire, subcontractors, visitors. Do not write remote or labour-hire workers out of scope without a robust argument.
5.1–5.3	Leadership, policy, roles	Officers’ due diligence under WHS law is the cultural test. Policy commits to safe and healthy workplaces, legal fulfilment, consultation/participation, improvement.
5.4	Consultation and participation	HSRs, committees, pre-starts that actually change controls. Remove barriers (language, fear of reprisal, unpaid time).
6.1.2	Hazard identification and risk	Routine and non-routine, emergency, human factors, design of work, change, past incidents, psychosocial. Risk methodology used consistently.
6.1.3	Legal and other requirements	WHS Act + regs + codes; workers’ compensation; heavy-vehicle NRS if applicable; electrical licensing; high-risk work licences; mine safety law where relevant; federal FSC scheme conditions if accredited.
6.2	OH&S objectives	Leading and lagging indicators. “Zero harm” with no plan is not an objective.
7	Support	Competence for high-risk work. Awareness of hazards and reporting rights. Documented information control.
8.1	Operational planning and control	SWMS / SOPs for high-risk construction work as defined in WHS Regulations. Management of change. Hierarchy of controls.
8.1.4	Procurement, contractors, outsourcing	Induction, licences, supervision, overlapping duties on shared sites (s. 16 model WHS Act).
8.2	Emergency preparedness	First aid, fire, rescue, remote work, psychosocial crisis. Drills.
9–10	Evaluation and improvement	Incident investigation that is not blame-only; legal-compliance evaluations; health monitoring where required; management review that includes worker participation outcomes.

Table 8. ISO 45001 clause intent against Australian WHS practice.

8.3 Relationship to other Australian safety credentials

- Federal Safety Commissioner (Office of the Federal Safety Commissioner) WHS accreditation is a separate scheme for certain Commonwealth-funded building work. ISO 45001 helps but does not replace OFSC accreditation.
- State contractor prequalification (e.g. NSW, VIC, QLD) often lists certified 45001 as the WHSMS pathway above specified contract values.
- ISO 45001 is evidence of a system. It is not a defence if an officer cannot show due diligence in a prosecution. Keep the two conversations connected.

9. ISO/IEC 27001 — Information security management

ISO/IEC 27001:2022 specifies an information security management system (ISMS). Certification means a CB has confirmed that you systematically identify information assets and risks, treat those risks, and operate controls. The 2022 edition is the only valid certification edition (the 2013 edition's transition window closed). Annex A now lists 93 controls in four themes — Organisational (37), People (8), Physical (14) and Technological (34) — rather than 114 controls in 14 domains. Eleven controls are new relative to 2013 (including threat intelligence, cloud services, ICT readiness for business continuity, configuration management, data masking, data leakage prevention).

9.1 Clauses 4–10 versus Annex A

This distinction fails more 27001 projects than any other. Clauses 4–10 are mandatory management-system requirements. You cannot “not apply” leadership, risk assessment or internal audit. Annex A is a reference control set. You select controls from risk treatment (and from legal/contractual need), compare them with Annex A so you have not forgotten a necessary control, and document the result in the Statement of Applicability (SoA). You do not implement all 93 controls unless risk and obligation say so. You do not skip the SoA.

9.2 Mandatory ISMS documented information

Document / record	Clause	Why auditors treat it as non-negotiable
ISMS scope	4.3	Boundaries: locations, functions, assets, interfaces with suppliers. Cloud and outsourced SOC must be in or justified out.
Information security policy	5.2	Top-management direction.
Risk assessment methodology and results	6.1.2, 8.2	Repeatable method; current assessment.
Risk treatment plan	6.1.3, 8.3	Actions, owners, dates, residual risk acceptance.
Statement of Applicability	6.1.3 d	Every Annex A control listed; inclusion justification; implementation status; exclusion justification.
Information security objectives	6.2	Measurable, planned.
Competence / awareness evidence	7.2, 7.3	Role-based, including privileged users.
Operational planning / control evidence	8.1	The ISMS runs daily, not only at audit.
Monitoring and measurement results	9.1	Control effectiveness, not only policy existence.
Internal audit programme and results	9.2	Independent of the work audited; covers clauses and selected controls.
Management review results	9.3	Full agenda including changes in threats and residual risk.
Nonconformity and corrective action	10.2	Incidents and audit findings closed with root cause.

Table 9. Core ISO/IEC 27001:2022 documented information.

In practice auditors also expect an information-asset inventory, a supplier/cloud register, an incident-response process, access-control rules, change and backup evidence, and policies that match the applicable Annex A themes. Those artefacts usually fall out of risk treatment rather than from a second hidden mandatory list.

9.3 Statement of Applicability — four required elements

- The necessary controls you determined from risk treatment (and the comparison with Annex A).
- Justification for including each of those controls.
- Whether each necessary control is implemented.
- Justification for excluding any Annex A control.

9.4 Australian legal and sector overlays

- Privacy Act 1988 and Australian Privacy Principles — personal information is an information asset; notifiable data breaches are incidents.

- APRA CPS 234 Information Security — binding for ADIs, insurers and super funds and material for their service providers. 27001 is the usual way suppliers demonstrate a system; it is not an APRA approval.
- Security of Critical Infrastructure Act 2018 (SOCI) and Risk Management Program rules — for responsible entities in defined critical-asset classes.
- Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM) / Essential Eight — for Commonwealth entities and many suppliers. Map Annex A to Essential Eight rather than running two unrelated programmes.
- Consumer Data Right, APRA CPS 230 Operational Risk, and incoming Peppol / eInvoicing security expectations (ISO/IEC 27001 becoming mandatory for relevant service providers on a staged path through 2027).
- State health and education privacy statutes when those sectors are in scope.

10. Other widely used ISO management-system standards

Each of the following uses the same Harmonized Structure (clauses 4–10), the same Stage 1 / Stage 2 model, and the same JAS-ANZ accreditation logic unless noted. What changes is the subject-matter core in clause 6 and 8.

10.1 ISO 22000:2018 — Food safety management

Combines a management system with HACCP principles (Codex). You identify food-safety hazards, select control measures, classify them as operational PRPs or CCPs, monitor, correct, verify, validate and trace one step forward and one step back. In Australia this sits beside the Food Standards Code, state food Acts, export controls, and often a GFSI-benchmarked scheme demanded by retailers (SQF, BRCGS, FSSC 22000). ISO 22000 alone may not satisfy a supermarket specification.

- Need: food-safety policy and objectives, PRPs, hazard analysis, hazard-control plan, traceability, emergency/recall, verification, internal audit, management review.
- Typical users: manufacturers, packers, ingredient suppliers, some logistics operators.

10.2 ISO 13485:2016 — Medical devices quality management

A QMS standard written for regulatory purposes. It is stricter than ISO 9001 on documentation, design controls (where applicable), risk management (normally ISO 14971), sterile barrier and process validation, identification/traceability, and post-market feedback including advisory notices and vigilance. The TGA does not always name ISO 13485 as a statutory certificate, but a 13485-aligned QMS is the normal way to support conformity assessment and ARTG inclusion. A 13485 certificate from a CB is not a TGA manufacturing licence.

10.3 ISO 50001:2018 — Energy management

Requires an energy review, energy baseline, Energy Performance Indicators (EnPIs), energy objectives and action plans, operational control of significant energy uses, design and procurement that consider energy performance, and demonstration of improvement in energy performance — not merely of the management system. Relevant to manufacturers, data centres, universities, hospitals and any organisation with NGER or corporate net-zero reporting that wants operational discipline rather than only carbon accounting.

10.4 ISO 22301:2019 — Business continuity

Requires business impact analysis (BIA), risk assessment of disruption, continuity strategies, documented business continuity plans, incident response structure, and an exercise programme that tests recovery time and recovery point objectives. Often paired with 27001 (ICT readiness) and with SOCI obligations for critical infrastructure.

10.5 ISO/IEC 20000-1:2018 — IT service management

The certifiable ITSM standard. Service catalogue, SLAs, change, incident, problem, configuration, capacity, continuity and supplier management. Appears in managed-service and government ICT tenders, usually next to 27001 and 9001. Compatible with ITIL practice but is not “ITIL certification”.

10.6 ISO 37001 — Anti-bribery

An anti-bribery management system: bribery risk assessment, financial and non-financial controls, due diligence on third parties, gifts and hospitality rules, speak-up arrangements, investigation and tone from the top. Useful for organisations caught by the Criminal Code foreign-bribery provisions and for infrastructure bidders. Does not confer immunity.

10.7 ISO 55001 — Asset management

For organisations whose value is in long-lived assets (utilities, rails, councils, mining plant). Decision-making across the asset life cycle, SAMP (strategic asset management plan), alignment of asset objectives with organisational objectives. Complements 9001 and 55000 guidance.

10.8 ISO 28000:2022 — Security and resilience in the supply chain

Security management system for the supply chain — people, goods, infrastructure and information in transit and storage. Seen in defence, ports, high-value logistics and some government security tenders.

10.9 ISO/IEC 42001:2023 — Artificial intelligence management

A management-system standard for organisations that develop or use AI. Risk, impact assessment, data quality, transparency and human oversight. JAS-ANZ accreditation for 42001 is appearing among Australian CBs. Expect it first in Commonwealth digital and automated-decision tenders rather than as a general SME requirement.

10.10 ISO 41001 — Facility management

FM management system used by some government facility contractors alongside the 9001/14001/45001 triple.

11. Sector schemes that sit on top of ISO 9001

These are not generic ISO standards in the 9001/14001 sense, but they dominate particular Australian supply chains. They generally require ISO 9001 as a base and add sector shall-statements. Certification is through CBs accredited for that scheme, sometimes with extra oversight (IATF, IAQG).

Scheme	Sector	Relationship to ISO
IATF 16949	Automotive	ISO 9001 plus automotive-specific requirements. Customer and IATF rules on CB selection.
AS9100 / AS9110 / AS9120	Aviation, space and defence	ISO 9001 plus IAQG requirements. OASIS registration.
ISO 29001	Oil and gas supply organisations	Sector quality overlay on 9001.
ISO 22163 (IRIS)	Rail	9001 plus rail-specific QMS.
FSSC 22000 / SQF / BRCGS	Food	GFSI-benchmarked; may use ISO 22000 as a foundation (FSSC) or a different structure.
NDIS Practice Standards	Disability services	Separate scheme; some CBs hold both JAS-ANZ ISO accreditation and NDIS auditor approval.

Table 10. Sector overlays commonly encountered with ISO certificates in Australia.

12. Laboratory competence: ISO/IEC 17025 and NATA

ISO/IEC 17025:2017 is the competence standard for testing and calibration laboratories. In Australia this is an accreditation pathway, not a JAS-ANZ management-system certification pathway. The National Association of Testing Authorities (NATA) is the government-recognised accreditation body. NATA assesses technical competence for a defined scope of tests or calibrations — methods, people, equipment, measurement uncertainty, proficiency testing,

metrological traceability to the National Measurement Institute where applicable.

Do not describe a NATA-accredited lab as “ISO 17025 certified”. Do not assume an ISO 9001 certificate on the parent company proves the lab’s results are competent. Conversely, 17025 accreditation is not a substitute for a corporate 9001 certificate covering sales, design and non-lab processes. Related NATA standards include ISO 15189 (medical labs), ISO/IEC 17020 (inspection bodies) and ISO/IEC 17043 (proficiency-testing providers).

13. Integrated management systems (IMS)

ISO 9001, 14001, 45001, 27001, 22000, 22301, 50001 and 20000-1 share the Harmonized Structure (formerly Annex SL): the same clause numbers for context, leadership, planning, support, operation, performance evaluation and improvement. An integrated management system uses one context analysis, one leadership process, one internal-audit programme, one management review and one corrective-action process, with discipline-specific modules plugged into clauses 6 and 8 (aspects, hazards, information-security risk, HACCP, energy review, BIA).

“Triple certification” in Australian construction and FM almost always means 9001 + 14001 + 45001 on one certificate or a set of aligned certificates after a combined audit. Benefits: fewer duplicate procedures, fewer audit days (CBs discount combined time under IAF rules), one set of objectives cascading through quality, environment and safety. Risks: a major nonconformity in one discipline can complicate the whole certificate if they are tightly coupled; internal auditors need multi-discipline competence; a bloated IMS manual that nobody owns.

Practical design rule. Integrate the management machinery (clauses 4, 5, 7.5, 9.2, 9.3, 10). Keep the technical risk engines separate and expert-owned: WHS hazard register, environmental aspects register, ISMS risk register / SoA, HACCP plan, energy review. Do not force one risk matrix to serve all four unless it genuinely can.

14. Master compliance checklists

Use these as implementation and internal-audit prompts. They paraphrase shall-intent; they are not the standard. Tick only when you can show a record or a demonstrable practice, not when a template exists.

14.1 Universal checklist — every HLS management system

■	Clause / item	What to have in place
■	4.1 Context	Internal and external issues documented and reviewed; climate change considered where the 2024 HLS amendment applies.
■	4.2 Interested parties	Parties and their relevant needs/expectations identified; legal needs flagged.
■	4.3 Scope	Scope statement names products/services, sites, boundaries and justified exclusions.
■	4.4 System processes	Processes, interactions, owners, criteria, resources and risks determined; documented information sufficient to run and to prove they ran.
■	5.1 Leadership	Top management can explain the system, policy, objectives and performance without a consultant present.
■	5.2 Policy	Policy appropriate to the organisation, includes required commitments, available as documented information, communicated, available to parties as appropriate.
■	5.3 Roles	Responsibilities and authorities assigned and communicated; a person with authority to report on system performance to top management.
■	6.1 Risk and opportunity	Process exists; actions planned and taken; effectiveness reviewed. Not a one-page SWOT left in 2022.
■	6.2 Objectives	Measurable objectives at relevant levels; plans with actions, resources, owners, due dates, evaluation method.
■	6.3 Change	Changes to the management system planned.
■	7.1 Resources	People, infrastructure, environment for the operation of processes.

■	Clause / item	What to have in place
■	7.2 Competence	Competence determined, obtained, evaluated; evidence retained.
■	7.3 Awareness	People aware of policy, their contribution, implications of nonconformance (and, for 45001, incidents and hazards).
■	7.4 Communication	What, when, with whom, how, who — internal and external as required by the discipline.
■	7.5 Documented information	Creation, update, control, protection, retention and disposal. External documents (standards, licences, customer specs) controlled.
■	8 Operation	Controls implemented as planned; outsourced processes controlled.
■	9.1 Monitoring	What is monitored, methods, when, when analysed; results retained; performance against objectives.
■	9.2 Internal audit	Programme based on importance, changes and previous results; auditors independent; results reported; findings closed.
■	9.3 Management review	Scheduled; full input list from the standard; outputs include decisions, improvement, resource needs; records retained.
■	10.1 Improvement	Opportunities identified and acted on.
■	10.2 Nonconformity / CA	React, control, correct, deal with consequences, evaluate need for action to eliminate cause, implement, review effectiveness, update risks, retain records. No “retrain the operator” as the only cause every time.
■	Certificate conditions	Scope still true; CB notified of significant change; logos used per rules; surveillance booked before anniversary.

Checklist A. Common Harmonized Structure requirements.

14.2 ISO 9001 extras

■	Clause / item	What to have in place
■	7.1.5 Monitoring resources	Where measurement validity is critical: calibrated/verified equipment, traceability, safeguards against adjustment, status identified.
■	7.1.6 Organisational knowledge	Knowledge necessary for process operation determined, maintained, made available; consider changing needs.
■	8.2 Requirements	Customer and legal requirements determined; organisation able to meet them; review before commit; changes controlled; records of review.
■	8.3 Design (if in scope)	Planning, inputs, controls (review/verification/validation), outputs, change control; records at each step.
■	8.4 External providers	Criteria for evaluation, selection, monitoring and re-evaluation; type and extent of control; information communicated to the provider.
■	8.5 Production / service	Controlled conditions; identification and traceability if required; property belonging to customers or external providers; preservation; post-delivery activities; change control.
■	8.6 Release	Planned verification completed; evidence of conformity; traceable authority for release.
■	8.7 Nonconforming outputs	Identified and controlled; correction, segregation, return, concession; records of nonconformity, actions, concessions, authority.
■	9.1.2 Customer satisfaction	Method to monitor perception; results analysed.
■	9.1.3 Analysis	Analysis of conformity, customer satisfaction, process performance, provider performance, risks/opportunities, improvement needs.

Checklist B. ISO 9001-specific prompts.

14.3 ISO 14001 extras

■	Clause / item	What to have in place
■	6.1.2 Aspects	Activities, products, services in scope; lifecycle perspective; abnormal and emergency conditions; criteria for significance; documented aspects and significant aspects.

■	Clause / item	What to have in place
■	6.1.3 Compliance obligations	Determined and accessible; how they apply to the organisation documented.
■	6.1.4 Planning action	Actions for significant aspects, compliance obligations, risks and opportunities; integration into EMS and business processes.
■	8.1 Operational control	Controls for significant aspects including leased plant, contractors and design/procurement influence.
■	8.2 Emergencies	Identify potential emergency situations; plan response; prevent or mitigate impacts; test periodically; review after tests and actual events; provide relevant information to parties.
■	9.1.1 Environment monitoring	What, methods, criteria, calibration of monitoring equipment; documented information on results.
■	9.1.2 Compliance evaluation	Frequency planned; results retained; knowledge of compliance status.
■	2026 transition	If still on 2015: gap against 14001:2026 (broader environmental conditions, clarified risk language, Harmonized Structure wording); transition audit booked before May 2029.

Checklist C. ISO 14001-specific prompts.

14.4 ISO 45001 extras

■	Clause / item	What to have in place
■	5.4 Consultation	Process for consultation and participation at all levels; time, training and resources; information access; barriers removed; non-managerial workers consulted on the list in 5.4 (policy, roles, legal fulfilment, objectives, contractor controls, monitoring needs, audits, improvement).
■	6.1.2 Hazards	Ongoing, proactive identification: routine/non-routine, incidents, emergencies, people (including contractors and visitors), work areas, equipment, human factors, design, change, past incidents, social factors including workload and bullying/harassment.
■	6.1.2.2 OH&S risks	Assessment methodology; opportunities to improve OH&S performance also identified.
■	6.1.3 Legal OH&S	Access to up-to-date legal and other requirements; determination of how they apply.
■	8.1.2 Hierarchy	Eliminate – substitute – engineering – administration – PPE applied in planning.
■	8.1.3 Management of change	Temporary and permanent changes: new products, processes, plant, people, legal change.
■	8.1.4 Contractors / outsource / procurement	OH&S criteria in procurement; coordination with contractors; controls on outsourced functions.
■	8.2 OH&S emergencies	Planned response; first-aid and test drills; communication to workers, contractors, visitors, emergency services.
■	9.1.1 OH&S monitoring	Includes operational controls, competency, legal compliance inputs, progress on objectives, health surveillance where required.
■	Incident process	Reporting culture; investigation; corrective action; communication of lessons; statistical review at management review.

Checklist D. ISO 45001-specific prompts.

14.5 ISO/IEC 27001 extras

■	Clause / item	What to have in place
■	6.1.2 Risk assessment	Defined risk criteria (impact, likelihood, acceptance); identifies risks to confidentiality, integrity, availability of information in scope; repeatable and current.
■	6.1.3 Treatment + SoA	Treatment options chosen; controls determined; compared with Annex A; SoA complete for all 93 controls; residual risk accepted by authority.
■	Asset inventory	Information and supporting assets known; owners assigned (almost always expected even if not named as a separate shall).
■	A.5 Organisational controls	Policies, roles, segregation of duties, threat intelligence, supplier relationships, incident management, continuity, compliance — as applicable per SoA.

■	Clause / item	What to have in place
■	A.6 People controls	Screening, terms of employment, awareness, disciplinary process, remote working, event reporting — as applicable.
■	A.7 Physical controls	Perimeters, entry, desks and screens, equipment siting, clear desk, supporting utilities, off-site assets — as applicable.
■	A.8 Technological controls	Identity, access, privilege, cryptography, network security, secure development, logging, malware, backup, vulnerability, cloud, data leakage, masking, configuration — as applicable.
■	8.2 / 8.3 Operate	Risk assessment and treatment performed at planned intervals and on significant change.
■	Incidents	Detection, response, evidence, communication, legal notification (Notifiable Data Breaches) tested.
■	Suppliers / cloud	Contracts, assurance (SOC 2 / shared SoA), off-boarding, residency — aligned to risk.

Checklist E. ISO/IEC 27001:2022-specific prompts.

14.6 First-certification readiness gate (all standards)

■	Clause / item	What to have in place
■	Standard purchased	Licensed copy of the current edition under control.
■	CB selected	JAS-ANZ register checked for standard + industry scope; impartiality confirmed.
■	Scope frozen	Matches the application form the CB will print on the certificate.
■	System operated	Enough live records (commonly ≥3 months) to sample.
■	Internal audit done	Full system covered, findings closed or plan accepted.
■	Management review done	Minutes exist; actions assigned.
■	Legal register current	State-specific instruments, not a generic internet list.
■	Staff briefed	People in sampled roles can describe their process without the manual in hand.
■	Stage 1 closed	Stage 1 findings addressed before Stage 2.
■	Logistics	Sites accessible; SME available; contractors on site if they are in scope.

Checklist F. Ready for Stage 2?

15. Twelve-month surveillance calendar

After certification, treat the certificate anniversary as a project. The following cadence keeps most SMEs audit-ready. Scale frequency up for high-risk sites, 27001 threat change, or multi-site sampling plans.

When	Activity	Owner
Weekly / monthly (ops)	Process KPIs, incident/NCR/complaint intake, backup and access reviews (27001), pre-starts and plant checks (45001), waste/emission checks where licensed (14001).	Process owners
Monthly	Open-action review (audit findings, incidents, objectives). Supplier issues. Change log.	System owner
Quarterly	Internal audits on a rolling programme so the whole system is covered in 12 months. Legal-register scan (new regs, licence renewals). Risk-register refresh if context changed.	Internal auditor + system owner
At least annually	Full management review. Policy and objective refresh. Competence review. Emergency drill (14001/45001). ISMS risk assessment (27001). Compliance evaluation (14001/45001). Aspects review (14001). Hazard review (45001).	Top management
Before surveillance (8–12 weeks)	Close overdue actions. Confirm scope and sites. Send CB any significant-change notice. Refresh sampled records.	

When	Activity	Owner
Surveillance visit	Treat as a mini Stage 2. Do not “prepare a folder” that is not the live system.	
Year 3, minus 6–9 months	Recertification planning. Consider adding a standard or integrating. Check edition transitions (e.g. 14001:2026).	
Anytime	Notify CB of ownership change, new site, scope change, serious incident, or loss of a process that was in scope.	

Table 11. Ongoing compliance calendar.

16. Australian legal overlays the auditor will expect you to know

ISO clauses 6.1.3 / 9.1.2 (and 9001’s requirement to meet applicable statutory requirements for products and services) push auditors to sample your legal register. The list below is a starting map, not exhaustive. Legal obligations differ by state and by licence.

Theme	Typical instruments	ISO standard that samples them
Work health and safety	Model WHS Act / state WHS or OHS Acts; WHS Regulations; codes of practice; workers’ compensation; high-risk work licensing; Heavy Vehicle National Law; mine safety statutes	45001 (primary), 9001 operationally
Environment	EPBC Act; state EP Acts and regulations; environment protection licences; waste and transport licences; contaminated land; water and trade waste; NGER Act; planning consents	14001 (primary), 50001 energy
Privacy and cyber	Privacy Act 1988 / APPs; Notifiable Data Breaches; state health privacy; SOCI Act; PSPF/ISM for government work; APRA CPS 234 / CPS 230	27001 (primary), 22301
Consumer and product	Australian Consumer Law; sector product safety; electrical equipment; building products	9001, 13485
Therapeutic goods	Therapeutic Goods Act; ARTG; TGA conformity assessment; essential principles	13485
Food	Food Standards Code; state food Acts; export control; country-of-origin labelling	22000 / HACCP
Corruption and crime	Criminal Code (foreign bribery); state integrity bodies; Modern Slavery Act reporting for large entities	37001, 9001 supplier control
Employment	Fair Work Act; awards; labour-hire licensing in some states	9001, 45001 (contractor control)

Table 12. Legal overlay map — confirm against current consolidated law in your jurisdictions.

17. Sources and verification points

Standards and accreditation rules change. Before you spend money or bid a tender, verify against primary sources.

- ISO — [iso.org](https://www.iso.org) — official catalogue and news (e.g. ISO 14001:2026 publication, 15 April 2026).
- Standards Australia / Intertek Inform — purchase AS/NZS ISO adoptions in AUD.
- JAS-ANZ — [jasanz.org](https://www.jasanz.org) and register.jasanz.org — accredited bodies, scopes, schemes (9001, 14001, 45001, 27001, 22000, 42001 and others).
- IAF — [iaf.nu](https://www.iaf.nu) — Multilateral Recognition Arrangement and mandatory documents (MD5 audit time, MD1 multi-site, MD11 integrated audits, MD26 transition).
- NATA — [nata.com.au](https://www.nata.com.au) — laboratory, inspection and related accreditation; distinction between accreditation and certification.
- Safe Work Australia — model WHS laws, codes, psychosocial guidance.
- State WHS regulators — SafeWork NSW, WorkSafe VIC, WHSQ, etc.
- State EPAs and the DCCEE / NGER Clean Energy Regulator — environmental and climate reporting.

- OAIC — Privacy Act and Notifiable Data Breaches.
- APRA — CPS 234 and CPS 230.
- TGA — medical device QMS and conformity assessment guidance.
- FSANZ and state food regulators — Food Standards Code.
- Office of the Federal Safety Commissioner — building-industry WHS accreditation (separate from ISO 45001).
- Austroads and state road-agency prequalification documents — construction QMS/WHSMS/EMS thresholds.

Document status. Prepared September 2026 as a planning and training aid. Edition numbers, transition deadlines (especially ISO 14001:2026 and any ISO 9001:2026 rules), JAS-ANZ scopes and state legal instruments should be re-checked on the date you rely on them. This report does not reproduce ISO copyrighted text.

Quick reference — who to call for what

Need	Go to
Buy the standard	Standards Australia / Intertek Inform or ISO webstore
Confirm a certificate is genuine	The issuing CB’s public certificate search, then JAS-ANZ register for the CB itself
Find an accredited certifier	register.jasanz.org filtered by standard and country
Laboratory competence	NATA, not a 9001 CB
WHS legal duty	Your state regulator and Safe Work Australia — not the ISO 45001 certificate
Privacy incident	OAIC NDB scheme — not only the 27001 incident procedure
Medical device supply	TGA — not only the 13485 plaque

Table 13. Primary contacts.

End of report. Use Checklists A–F as working papers: copy them into your internal-audit pack, add owners and due dates, and treat an unticked row as a gap until evidence exists.