

MRQSA Board
Transition Summary for
ISO 20252:2019 to ISO 20252:2026

1. Purpose and copyright note

This document summarises the principal differences between ISO 20252:2019 and ISO 20252:2026 for certification auditors and organisations preparing to update management systems, documented procedures, project controls and evidence packs. It is a paraphrased transition aid and does not reproduce requirements from either standard. Users should consult the ISO 20252:2026 standard for the full details:

ISO 20252: 2026: <https://www.iso.org/standard/88881.html>

BS ISO 20252: 2026: <https://standardsdevelopment.bsigroup.com/projects/2025-00085>

MRS has arranged for members to receive a 25% discount on copies of BS ISO 20252. To order please contact company.partners@mrs.org.uk.

2. Executive summary of the main changes

The 2026 edition is a technical revision of the 2019 edition. The most significant change is the explicit integration of automation, Artificial Intelligence (AI) and related technologies across the core framework and several annexes. The 2026 edition also separates sampling from panel development by creating a new Annex G, strengthens sample-quality and fraud-prevention controls, expands expectations for legal and information-security governance, and gives greater emphasis to traceability, participant protection, data minimisation, synthetic data, secure transfer and demonstrable oversight.

3. High-level structural changes

Area	2019 edition	2026 edition	Transition significance
Overall structure	Core clause plus Annexes A to F.	Core clause plus Annexes A to G.	Organisations must revisit their SoA and internal audit scope to include the new annex structure and additional requirements in clause 4 for internal audits where relevant.
Panel requirements	Panel requirements were mainly contained within Annex A on sampling.	Panel development and life cycle management are separated into Annex G, and the definition of access panels has been expanded	Panel providers, sample buyers and auditors need separate evidence trails for sampling and panel management. The SoA needs to cover all relevant panel types.
Digital observation	Annex D covered digital observation and incorporated concepts from ISO 19731.	Annex D is retitled and updated as digital and online observation. ISO 19731 has been withdrawn as a separate standard.	Controls for online sources, AI-generated content, tracking technologies and device monitoring need review.

Core governance	Legal requirements were a short separate clause.	Legal and business governance requirements are integrated earlier in the core framework.	Auditors should expect a systematic approach to identifying, maintaining awareness of, monitoring and complying with applicable laws and codes.
AI and synthetic data	AI was referenced mainly through automated systems and machine learning terminology.	New core requirements address AI development, deployment, oversight, client disclosure and synthetic data.	Organisations need documented controls for AI use, validation, human oversight, data governance and client authorization.

4. Clause-by-clause comparison of core requirements

2019 clause	2026 clause	Nature of change	Auditor focus	Business action
4.1.1 Statement of applicability	4.1.1 Statement of applicability	The SoA now reflects seven annexes and more explicit distinction between in-house and subcontracted services.	Check that the SoA is current, specific, non-promotional, authorised and aligned with the services actually delivered.	Update the SoA template, declarations, website/client materials and certification scope wording.
4.8 Legal requirements	4.1.2 Legal and other requirements	Legal requirements move into the core framework and are broader, including business governance and sectoral obligations.	Look for a systematic method for identifying, maintaining and communicating applicable legal, regulatory and code requirements.	Create or refresh processes to identify, monitor and communicate legal and regulatory changes.
4.1.2 Confidentiality of research	4.1.3 Confidentiality of research	Privacy, consent withdrawal, data deletion, transparency and consent records are strengthened.	Test evidence for participant notices, withdrawal handling, deletion processes, consent records and special handling of	Review privacy notices, consent capture, withdrawal workflows, data deletion controls and retention exceptions.

			children or vulnerable persons.	
4.1.3 Documentation and records management	4.1.4 Documentation and records management	Greater emphasis on data minimisation, storage location, transfers, authenticity, integrity, traceability and secure disposal.	Verify that records are sufficient to replicate projects and are controlled throughout their lifecycle.	Map project records, retention rules, storage locations, transfer routes, destruction controls and version control.
No equivalent dedicated clause	4.1.5 Development and use of AI and related technologies	New controls for AI development, deployment, client disclosure, model provenance, validation, human oversight and synthetic data.	Review AI inventory, risk assessment, approvals, client consent, validation evidence, oversight records and deliverable disclosures.	Introduce an AI governance procedure, model documented information about AI models, client approval triggers, validation method and disclosure wording.
4.2 Personnel and infrastructure responsibilities	4.2 Personnel and infrastructure responsibilities	Terminology shifts towards organisational obligations, accountability, infrastructure, assets and technology governance.	Confirm that responsibilities are documented, understood and include AI, subcontracting and information security.	Update documented roles and responsibilities, competence matrices, training plans and accountability assignments.
4.3 Information security	4.3 Information security	Information security is aligned more closely to risk assessment, classification, incident reporting and secure data handling.	Seek evidence of risk assessments, classification, access controls, incident assessment and mandatory training.	Refresh information-security procedures, incident logs, access rules, classifications and annual training content.
4.5 Planning, delivery and reporting	4.5 Planning, delivery and reporting	Expanded requirements for design suitability, limitations,	Sample proposals, project files and reports to test whether	Update proposal templates, project records,

		data storage, data destruction, synthetic data validation, participant engagement and drop-out.	new disclosures and design records are present.	instrument change logs, testing records and reporting templates.
4.6 Management review	4.6 Senior management review and improvement	Senior management accountability is clearer; risk controls and follow-up audit of actions are more explicit.	Check management review minutes for risk, legal, privacy, security, complaints, nonconformity and action closure evidence.	Revise management review agenda and action-tracking process.
4.7 Internal audits	4.7 Internal audits	Internal audit expectations are broader, including SoA, subcontracting, legal obligations, information security, operational change and three-year coverage.	Verify annual scheduling, competence of auditors, independence, project sampling and full-cycle coverage.	Rebuild the audit programme to cover all applicable clauses and annexes over the certification cycle.

5. Annex-by-annex transition implications

5.1 Annex A: Sampling

Annex A is narrowed and strengthened. The 2019 edition combined sampling and access-panel requirements; the 2026 edition retains sampling in Annex A and moves panel development and lifecycle management into Annex G. The sampling annex now recognises a wider range of sample sources, including managed networks, aggregators, affiliate networks, marketplaces and sample exchanges. It also introduces stronger transparency expectations around sample source composition, source blending, sample quality metrics, participant outcomes, secure end links, fraud indicators, hidden questions, bot detection, URL tamper detection, IP and geo-location checks, hashed redirects and click-farm identification. There are two new tables which specify sample provider and sample user transparency requirements. These requirements are specified by the type of sample sources i.e., offline samples sources, panel aggregators and managed networks, and other online sample sources such as sample exchanges.

5.2 Annex B: Fieldwork

Annex B remains broadly the same but adds emphasis on data privacy, data security and legal instructions in fieldworker briefings. The 2026 edition separates fieldworker documentation into a clearer requirement and updates language around personnel,

competence and observation. For auditors, the transition issue is less about wholesale redesign and more about ensuring fieldwork recruitment, briefing, training, validation and complaints records explicitly address current privacy, security and legal obligations.

5.3 Annex C: Physical observation

Annex C is updated mainly to align terminology and reporting with the revised core framework. The key new practical point is that reporting should identify whether AI or related technologies have been applied in sampling, observation or analysis. Businesses should update physical observation briefing and reporting templates so that legal, privacy and AI-use disclosures are routinely captured.

5.4 Annex D: Digital and online observation

Annex D is updated from digital observation to digital and online observation. It retains the focus on passive and online data collection while adding explicit attention to AI-generated content, AI use in sampling, observation or analysis, and stronger alignment with legal and privacy requirements. The 2026 edition also updates terminology around drop-out, online IDs, device IDs and consent withdrawal. Auditors should examine whether providers can demonstrate how online sources are selected, cleaned, validated, anonymised and reported without causing adverse consequences for individuals.

5.5 Annex E: Self completion

Annex E strengthens validation of self-completion responses, especially for panels, multiple-source samples and online environments. The 2026 edition expands the list of potential fraud and inattention indicators to include hidden questions, bot-generated answers, bot detection, IP and geo-location checks, URL tamper detection, hashed redirects and click-farm indicators. Businesses should update online-survey quality-control procedures and ensure client-facing documentation explains how identity, response quality and exclusions are handled.

5.6 Annex F: Data management and processing

Annex F is substantially affected by AI, automation and synthetic data. Documentation of data cleaning and weighting now needs to address synthetic data where used. Automated or AI-assisted logic checks, coding, validation and analysis must be subject to defined accuracy expectations, controls, human oversight and corrective action where results do not meet the required standard. Coding validation may be performed by people or suitable technologies, but independence, competence, documented process and remediation remain central audit themes.

5.7 Annex G: Panel development and life cycle management

Annex G is new in the 2026 edition. It takes panel-related material that was previously embedded in Annex A and expands it into a dedicated framework for panel development, recruitment, profile data, membership agreements, identity verification, panel capacity, maintenance, incentives, opt-out, support, participation frequency and panel quality control. There are two tables which specify panel provider and project transparency requirements. These requirements are specified by the type of panels i.e., continuously reporting panels, panel aggregators and managed networks, and other online sample sources such as sample exchanges. This is the first time that the standard has included requirements for continuously reporting panels.

Organisations operating panels, using panel providers or relying on aggregators and managed networks should treat Annex G as a major transition workstream.

6. Transitional Period

A transitional period of three years will be in place for organisations to migrate from the old 2019 version of the ISO 20252 standard to the new 2026 edition.

7. Key transition themes for auditors

- **Scope and SoA:** Confirm whether the certification scope has been remapped from Annexes A to F to Annexes A to G and whether subcontracted services are accurately represented.
- **AI governance:** Test whether AI use is authorised, documented, communicated to clients where required, validated and subject to human oversight.
- **Legal and privacy controls:** Look for a systematic process for identifying legal obligations and embedding them in proposals, participant communications, project delivery and reporting.
- **Sample quality:** Verify that fraud, inattention, duplication, bot activity, source blending and sample-source limitations are actively controlled and evidenced.
- **Panel lifecycle management:** Where panels are included in scope, audit recruitment, profile maintenance, identity verification, incentives, support, opt-out and participation-frequency controls against Annex G.
- **Reporting transparency:** Confirm that client reports and deliverables disclose limitations, AI use, validation methods, sample quality impacts and restrictions on identifiable raw data where applicable.

8. Transition actions for organisations

1. Map the current 2019 SoA and procedures to the 2026 clause and annex structure.
2. Decide whether Annex G applies directly, through subcontracted services, or through reliance on panel suppliers.
3. Create an AI and related technologies register covering tools, models, deployment locations, data processed, oversight, validation and client approval requirements.
4. Review proposal, quotation and project specification templates to include AI, synthetic data, data storage, retention, destruction and sample-quality disclosures.
5. Update participant-facing information to reflect consent, withdrawal, deletion, privacy, tracking technologies, device IDs, online IDs and routing or automation where applicable.
6. Strengthen sample and response-quality procedures to include current fraud and bot-detection controls.
7. Revise fieldwork, observation, self-completion and data-processing procedures to incorporate legal, privacy, information-security and AI-related requirements.
8. Update internal audit schedules so all applicable 2026 clauses and annexes are covered across the certification cycle.
9. Train relevant personnel, auditors, project managers and subcontractor managers on the 2026 changes.
10. Run a transition gap assessment and retain evidence of decisions, corrective actions and management review approval.

9. Practical readiness checklist

Checkpoint	Evidence to prepare	Status
SoA updated to 2026 annex structure	Approved SoA, scope mapping, client-facing declaration.	Not started / In progress / Complete
Legal and governance process refreshed	Legal register or equivalent, owner, review cadence, communication records.	Not started / In progress / Complete
AI governance implemented	Document information about AI models, approval records, validation evidence, oversight logs, client permissions.	Not started / In progress / Complete

Synthetic data controls available	Methodology, source documentation, validation criteria, bias mitigation and labelling approach.	Not started / In progress / Complete
Sample quality procedures strengthened	Fraud controls, bot detection, de-duplication records, secure end-link evidence, sample-source documentation.	Not started / In progress / Complete
Panel lifecycle controls mapped	Annex G gap assessment, recruitment records, profile update evidence, support logs, opt-out records.	Not started / In progress / Complete
Project documentation updated	Proposal templates, project specifications, change logs, instrument testing records, reporting templates.	Not started / In progress / Complete
Information security controls reviewed	Risk assessments, classifications, access controls, incident records, secure transfer checks.	Not started / In progress / Complete
Internal audit programme revised	Annual audit schedule, three-year coverage plan, auditor competence records, project audit sampling plan.	Not started / In progress / Complete
Management review completed	Senior management review minutes, action plan, closure evidence and follow-up audit records.	Not started / In progress / Complete