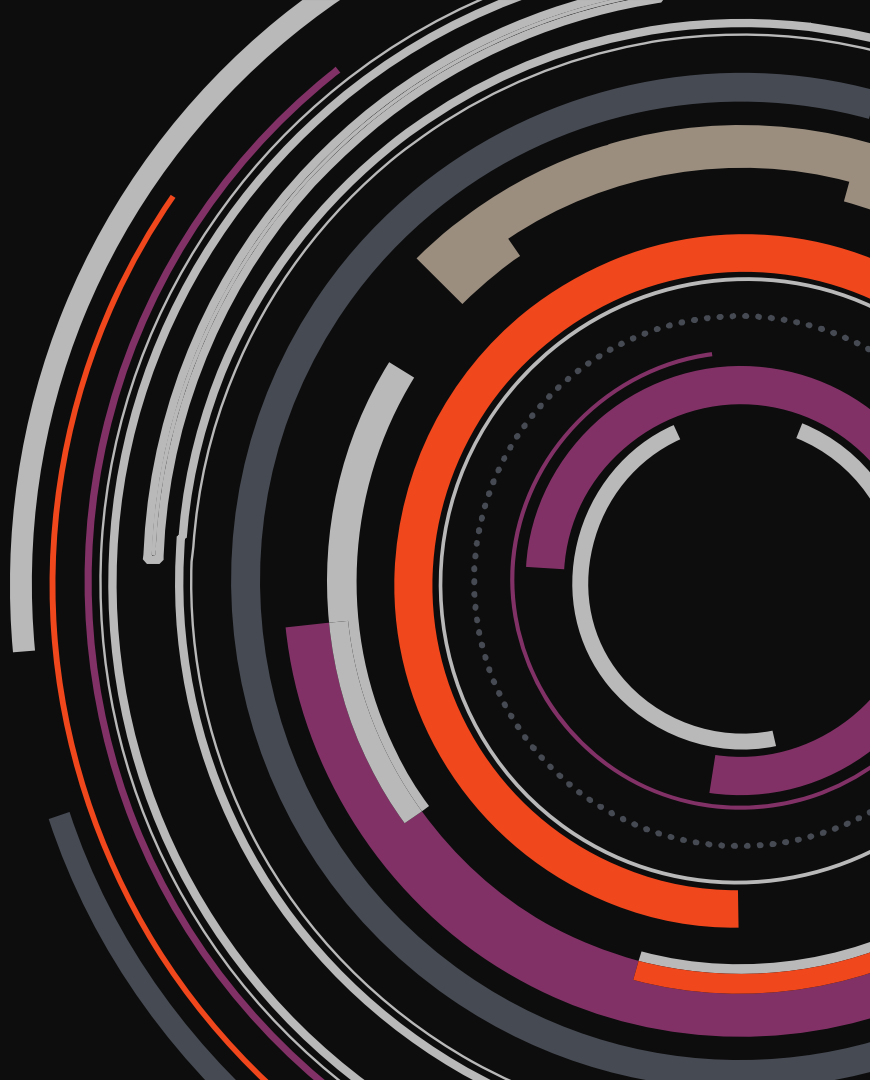
ISO 20252:2026

What is New and What to Do to Prepare for the New Standard

Debrah Harding, FAcSS, FRSA

Managing Director, the Market Research Society (MRS) &

Chair of the ISO Technical Committee, ISO TC 225



Structure of ISO 20252:2026

A core framework for service providers, plus method-specific annexes

Sections 1–2	Scope, and normative references (the standard has none)
Section 3	Terms and definitions used throughout the standard
Section 4	Core framework for every service provider: scope and Statements of Applicability (SoA), legal duties, participant protection, records, AI, personnel responsibilities, information security, subcontracting, project documentation, client relationship management, internal audit and senior management review
Annexes A to G	Method-specific requirements: A:Sampling, B:Fieldwork, C:Physical observation, D:Digital and online observation, E:Self-completion, F:Data management and processing, G:Panel development and life cycle management

Statement of Applicability

Clause 4.1.1: what a service provider attests to, and what an auditor tests

Purpose	The service provider's declaration of the services, and the annexes A to G, to which it attests conformity
Core rule	Clause 4 applies to every service provider and must be supported by at least one annex; no attestation is possible without one
Scope claims	Any claim must clearly state which annexes are in scope; align website, client materials and certificate wording
Maintenance	Responsibility covers in-house and subcontracted work; keep the SoA approved, current and covered by internal audit

The main changes

1

AI and automation

Explicit controls for AI use and synthetic data across the core framework and relevant annexes

2

Sampling and panels

Stronger sample-quality controls

New Annex G separates panel development and life cycle management from sampling

3

Governance and evidence

Greater emphasis on legal obligations, participant protection, information security and traceable oversight

Alignment with other relevant standards such as ISO 27001 and ISO 9001

Governance and security

Legal duties, accountability and information security need demonstrable controls



Legal duties	Clause 4.1.2: identify, monitor and communicate applicable laws, regulations and codes
Accountability	Clause 4.2: document responsibilities, competence and training for AI, subcontracting and security
Information security	Clause 4.3: refresh risk assessments, data classifications, access controls and incident handling
Secure handling	Maintain secure data-handling procedures and evidence of mandatory training

Privacy and records

Clauses 4.1.3 and 4.1.4 strengthen participant and data controls.



Participant protection

Review notices, consent records, withdrawal handling and deletion workflows

Retain specific protections for children and vulnerable participants

Traceable records

Apply data minimisation and document storage locations, transfers and retention exceptions

Maintain authentic, traceable records sufficient to replicate projects, with version control and secure disposal

AI governance

New clause 4.1.5 makes AI oversight explicit



Inventory

Record tools, models, provenance, deployment locations and the data processed

Validation and oversight

Define risk assessment, approvals, validation criteria and expert human oversight

Client disclosure

Set client approval triggers and explain AI use in deliverables where required

Synthetic data

For synthetic data, document methodology, sources, validation, bias mitigation and labelling

AI usage

Clause 4.1.5.3: ten requirements for AI use in research projects



Accountability

Allocate responsibility to a nominated individual or committee, with regular human oversight across the AI life cycle

Data handling

Specify data types and protection levels, inform parties of external processing; no client data without express agreement

Participants

Inform participants when they interact with AI, such as personas or chatbots

Proposals

Describe the AI type, research stage, model provenance, deployment location and data governance

Reporting

Record and tell clients if AI generated insights; document model version, validation and accuracy in deliverables

Monitoring

Run security, privacy and quality checks through the life cycle; review output regularly and after major changes

Client management and project documentation

Clause 4.5 expands expectations across client management, planning, delivery and reporting



1

Research design

Record design suitability, limitations, participant engagement and drop-out

2

Proposal disclosures

Update proposals and specifications for AI, synthetic data and sample-quality disclosures

3

Data lifecycle

Document data storage, retention and destruction arrangements

4

Project evidence

Keep instrument change logs, testing evidence and reports that explain validation methods and relevant limitations

Audit and oversight

Clauses 4.6 and 4.7 make management accountability and audit coverage clearer



Management review

Senior management reviews should cover risk, legal duties, privacy, security, complaints and nonconformities

Corrective action

Track corrective actions to closure and retain follow-up audit evidence

Annual audits

Schedule internal audits annually, with competent, independent auditors and project sampling

Full-cycle coverage

Cover every applicable clause and annex across the three-year certification cycle, including subcontracting and operational change

Sample quality

Annexes A and E strengthen transparency and response validation



Sample provider and user transparency

Annex A recognises managed networks, aggregators, affiliate networks, marketplaces and sample exchanges and the requirements for each varies – two new tables

Transparency

Document sample composition, source blending, quality metrics and participant outcomes

Fraud prevention

Strengthen checks for fraud, bots, duplication, inattention and click-farm activity

Secure checks

Review secure end links, URL tampering, hashed redirects, IP and geo-location checks. Explain identity checks and exclusions to clients

Annexes B, C and D: Fieldwork and observation

1

B: Fieldwork

Broadly unchanged - make privacy, security and legal duties explicit in briefings, training, validation and complaints records

2

C: Physical observation

Align briefing and reporting with the revised core requirements - identify AI use in sampling, observation or analysis

3

D: Digital and online

Broadened from digital observation to digital and online observation

New controls for AI-generated content, tracking technologies and device monitoring

Data processing

Annex F brings AI, automation and synthetic data into processing controls



Methods and accuracy

Document synthetic data in cleaning and weighting methods where used

Define accuracy expectations for automated logic checks, coding, validation and analysis

Oversight and validation

Maintain human oversight and corrective action when results fall short

Coding validation may use people or suitable technologies

Independence, competence and documented remediation remain essential

New Annex G

Panel development and life cycle management form a separate Annex



1

Recruitment

Cover recruitment, membership agreements, identity verification and profile maintenance

2

Panel operations

Review panel capacity, incentives, support, opt-out and participation-frequency controls

3

Panel coverage and transparency

Specifies transparency requirements plus sample blending and managing fraud

4

Applicability

All panel types covered including continuously reporting panels (e.g. media measurement) for the first time

3

YEARS

A three-year transition period

In the UK three years to migrate from the 2019 edition to the 2026 edition – a similar approach being undertaken in other markets such as the US and Australia

Preparing for transition

1

Map the gaps

Remap the SoA and procedures, decide where Annex G applies

Build an AI register and record transition gaps

2

Update the controls

Review participant information, project templates and sample - quality procedures

Train personnel and subcontractor managers

3

Demonstrate readiness

Refresh the audit programme - test implementation and close gaps

Retain management approval and corrective-action evidence

Company actions: scope

Companies transitioning to the 2026 standard: define scope and accountability

01	**Scope mapping**	Map services and procedures to the 2026 clauses and Annexes A to G Existing certificate holders should map from their 2019 SoA
02	**Annex G**	Decide whether Annex G applies directly, through subcontracting or through reliance on panel suppliers - include all relevant panel types
03	**Approved SoA**	Approve an accurate SoA and align declarations, website or client materials and certification-scope wording
04	**Legal duties**	Refresh the process for identifying legal duties, record the owner, review cadence and how changes reach relevant staff
05	**People and skills**	Update roles, competence matrices and training for personnel, project managers, auditors and subcontractor managers Retain the gap assessment and decisions

Readiness evidence

A transition pack should link each control to an owner and evidence



Scope and governance

Scope and governance: approved SoA, legal register, responsibilities and review records

AI and synthetic data

AI and synthetic data: model records, permissions, validation and oversight logs

Sampling and panels

Sampling and panels: fraud controls, source records and Annex G evidence

Delivery and assurance

Delivery and assurance: updated project files, security records, audit coverage and management action closure

Company actions: controls

Companies transitioning to the 2026 standard: embed controls in daily delivery

Tools and project design

Create an AI register covering tools, models, deployment locations, data processed, oversight, validation and client approval triggers

Update proposals, quotations and project specifications for AI, synthetic data, storage, retention, destruction and sample-quality disclosures

Participants and operations

Revise participant notices and workflows for consent, withdrawal, deletion, tracking technologies, device or online IDs and automation where applicable

Strengthen sample and response-quality procedures and map panel lifecycle controls and retain supplier, source and exclusion evidence

Update fieldwork, observation and processing procedures for legal, privacy, security and AI duties and define secure transfers and corrective action for failed validation

Company evidence pack

Companies transitioning to the 2026 standard: track readiness and retain proof

Governance	Governance: approved SoA and scope map, legal register or equivalent, owners and communication records
AI and synthetic data	AI and synthetic data: model records, approvals, client permissions, validation, oversight, methodology, bias mitigation and labelling
Sample and panel quality	Sample and panel quality: source documentation, fraud and bot controls, de-duplication, secure end links and Annex G lifecycle records
Delivery and security	Delivery and security: revised project templates, change logs, testing, reports, risk assessments, access controls, incidents and transfer checks
Assurance	Assurance: annual internal audit schedule, three-year coverage plan, competence and sampling records, management approval and action-closure evidence

Track each of the source's ten readiness checkpoints as Not started, In progress or Complete.

Route to certification

1

Prepare

Gap-assess your services against ISO 20252:2026

Build and test your management system

2

Be assessed

Choose a certification body and agree scope

Complete the Stage 1 and Stage 2 audits

3

Certify and maintain

Close nonconformities and receive your certificate

Keep it through surveillance, internal audits and review

Certification steps: prepare

Companies seeking certification: build the system before you apply

01	**Gap assessment**	Compare current services, procedures and records with the 2026 core clauses and Annexes A to G
02	**Scope and SoA**	Decide which services to certify and which annexes apply, then approve the Statement of Applicability
03	**Management system**	Document procedures, responsibilities, competence and training, including AI, security and legal duties
04	**Internal checks**	Run an internal audit and a senior management review, and close corrective actions
05	**Choose a body**	Compare certification bodies, check accreditation and scheme approval, then agree a proposal and contract

Certification steps: audit

The certification body assesses your system in stages



Optional pre-audit

Test readiness and get early feedback before the formal audit begins

Stage 1: preparedness review

The auditor reviews scope, documentation and readiness, and plans the main assessment

Stage 2: main assessment

Auditors test implementation across projects, records and people against the standard and your SoA

Findings and decision

Correct any nonconformities with evidence, after which the certification body decides whether to issue the certificate

Certification steps: maintain

Certification runs as a three-year cycle, not a one-off audit



Certificate	Issued after a positive decision; scope wording and declarations must match your approved SoA
Surveillance	Periodic visits by the certification body during the cycle; frequency is set by the certification body
Internal audit	Annual internal audits by competent, independent auditors, covering all applicable clauses and annexes over three years
Management review	Senior management reviews risk, legal duties, privacy, security, complaints and nonconformities, and tracks actions to closure
Change and renewal	Manage operational change, subcontracting and new AI use through the SoA, and plan renewal before the cycle ends

Confirm audit stages, timings and surveillance frequency with your certification body.

Measuring global uptake

ISO Technical Committee TC 225: a country-by-country evidence base on ISO 20252 use and adoption for its Strategic Business Plan



Evidence sources Qualitative research in key markets, existing ESOMAR surveys and its national representative network, and the annual Global Market Research survey of national associations - possible new surveys would fill data gaps

Measures Accredited and non-accredited certification, association-led schemes, client procurement requirements and regional differences in implementation

Evolving needs AI and related technologies, methodologies and sustainability for consideration in future ISO 20252 updates

The outcome A clearer picture of awareness, uptake and potential barriers, with stronger evidence for future revisions

Questions?

Debrah.harding@mrs.org.uk

