

Global ISO Insights — May 2026 (Issue #1)

Practical intelligence for quality, information
security and sustainability leaders



IN THIS ISSUE

- 01 Editor's note & global landscape
- 02 This month's standards updates
- 03 ISO 27001:2022 — where we are now
- 04 CSRD & ESG reporting deep-dive
- 05 Country spotlights
- 06 Industry focus
- 07 Audit tips & common nonconformities
- 08 Standards on the horizon
- 09 Next month

Editor's note



Welcome to Issue #1 of UniCert UK's Global ISO Insights. May 2026 opens with a decisive shift in the certification landscape. The ISO/IEC 27001:2022 transition deadline is now behind us, leaving a mixed picture: most organisations completed on time, but late transitions and a spike in nonconformities—especially around Annex A updates and operational technology—are still working through surveillance cycles. Meanwhile, the ISO 9001 revision has moved into the decisive DIS/FDIS phase, with themes of risk-based thinking, change management and sustainability alignment under close scrutiny by quality leaders who must plan for multi-standard integration.

In sustainability, the CSRD's second wave is pulling suppliers deeper into data requests, with ESRS expectations landing across procurement and finance as much as EHS. Expect tougher assurance demands on Scope 3 and double materiality evidence. Energy remains a board-level concern; high and volatile prices are catalysing renewed interest in ISO 50001 and metering strategies that deliver fast payback.

Two forward-leaning developments stand out. First, adoption of ISO/IEC 42001 (AI management) has moved beyond pilots; early certifications are informing enterprise AI governance playbooks ahead of new regulatory enforcement milestones. Second, sector standards continue to calibrate: ISO 13485 surveillance is intensifying on PMS and software, IATF 16949 is pressing harder on special processes and change control, and aerospace primes are re-baselining supplier oversight in anticipation of the next AS9100 alignment after ISO 9001.

Across this issue we prioritise what senior managers need now: where auditors are finding gaps, what revisions mean in practical terms, and how to synchronise management systems so one improvement cycle serves quality, security and ESG. As always, our analysis is evidence-led and standard-neutral—aimed at helping you make confident, timely decisions.

This month's standards updates



ISO 27001

ISO/IEC 27001:2022 transition—what the post-deadline data shows

With the transition window closed, certification bodies report elevated minor nonconformities concentrated in Annex A control implementation evidence, risk treatment traceability, and monitoring of security metrics. Organisations that treated the update as a document refresh rather than a risk re-baseline saw the heaviest findings. OT environments and SaaS supplier due diligence were recurring weak points. A positive trend: more boards are demanding consolidated risk registers spanning cyber, privacy and resilience, which—when linked to ISMS objectives—are reducing repeat findings at surveillance. Late transitions are still being cleared; most schemes are offering shortened special audits but applying tightened sampling. Expect ongoing scrutiny of threat intelligence processes, cloud shared-responsibility matrices, and control effectiveness measures through to year-end.

ISO 9001

ISO 9001 revision enters critical DIS/FDIS phase

The ISO 9001 revision has moved into the decisive ballot stages, with early feedback highlighting clearer expectations for change management, knowledge management, and more explicit risk/opportunity planning. While no wholesale restructuring is expected under Annex SL, text is tightening around process performance, data-driven improvement and supply-chain assurance. Many organisations are already gap-mapping to avoid a congested transition later. Practical actions now: refresh your quality objectives cascade with measurable leading indicators, verify the currency of process maps and interfaces, and align internal audit programmes to stress-test design and change control. Multi-standard users should watch for alignment impacts on sector schemes (IATF, AS/EN 9100) once the final text lands.

CSRD/ESRS

CSRD 'second wave' hits suppliers: assurance and data quality rise to the top

CSRD reporting for FY2025 is pulling more companies—especially non-EU suppliers to EU-listed entities—into data provision on Scope 3, climate targets, and workforce topics. ESRS expectations are sharpening the focus on traceability, calculation boundaries and governance evidence. Auditors are probing double materiality methodologies and control frameworks around non-financial data. Companies leveraging ISO 14064-1 for GHG quantification and ISO 37301/37001 for governance controls are finding smoother assurance discussions. The immediate pinch-points are supplier data collection cadence, primary data substitution rules, and integration with financial consolidation calendars. Expect stricter external assurance scoping and a push to embed internal controls over sustainability reporting (ICSR) before next filing cycles.

ISO 42001

ISO/IEC 42001 adoption gathers pace amid AI governance deadlines

Enterprises are moving from AI principles to operational controls, using ISO/IEC 42001 as a governance backbone for model lifecycle management, risk assessments and human oversight. Early certifications show auditors focusing on data governance, model change control, bias and robustness testing, and incident handling. Organisations integrating

42001 with ISO/IEC 27001 and 27701 are reducing duplication in access controls, supplier management and logs. Practical lessons: define model inventory scope early, set clear go/no-go gates, and link AI risk acceptance to business owners. Regulators' emerging enforcement timelines are accelerating board attention; having a management system in place is proving a credible readiness signal for both compliance and customer assurances.

ISO 50001

Energy costs sustain momentum for ISO 50001 and metering-first strategies

Persistently high and volatile energy prices continue to strengthen the business case for ISO 50001. The fastest paybacks are coming from metering granularity, automated M&V, and load-shifting rather than capex-heavy retrofits. Certification bodies report stronger objective-setting and more sophisticated EnPIs where energy reviews are refreshed quarterly, not annually. Common pitfalls remain: weak operational control over compressed air and HVAC, outdated significant energy use (SEU) analyses, and lack of cross-functional ownership between facilities, production and finance. Integration with carbon reporting (ISO 14064-1) is rising, enabling consistent baselines for CSRD disclosures and internal carbon pricing. Expect more top-management scrutiny of performance verification as contracts and hedges roll off.

ISO 22000

Food safety systems recalibrate around prevention and culture

Food businesses are adjusting their ISO 22000-based systems in response to heightened market expectations on allergen controls, supplier verification and food safety culture. GFSI scheme owners are tightening guidance on validation evidence and environmental monitoring. Auditors report more findings in prerequisite programme (PRP) maintenance and traceability during rapid product changeovers. Organisations that link HACCP reassessments to real-time complaint and recall data are seeing fewer major nonconformities. Cross-linking food defence and fraud controls to procurement performance reviews is also becoming a differentiator. With complex, multi-country supply chains, remote supplier audits remain common—but expect deeper on-site verification at high-risk suppliers as travel patterns normalise.

ISO 27001:2022 — where we are now



The 2022 transition is behind us — what changed in practice.

Six months after the ISO/IEC 27001:2022 transition deadline, the pattern of post-transition findings is clear. The strongest programmes treated the update as an opportunity to re-baseline risk and strengthen control ownership; the weakest focused on document renumbering with minimal operational change. Three themes dominate audits:

1) Annex A control clarity and evidence. Auditors are asking for sharper linkages between risk treatment plans and the updated control set, especially where cloud, OT and SaaS predominate. Control A.5 (organisational controls) is driving questions about governance charters and decision rights. In A.8 (technological controls), evidence of configuration baselines, hardening standards and patch cadence is under closer review, particularly for managed services. A.5.23/24 (threat intelligence and information security for use of cloud services) are frequent gaps: many policies exist, but systematic intake of threat intel and shared-responsibility matrices with providers are incomplete.

2) Metrics and effectiveness. More certification bodies are challenging whether ISMS objectives have measurable leading indicators and whether monitoring actually informs management decisions. Dashboards that simply restate incident counts are being downgraded; evidence of trend analysis, hypothesis-driven corrective actions and ownership by business risk owners earns credit. Linkage to business continuity (ISO 22301) and privacy (ISO/IEC 27701) strengthens the narrative where dependencies are explicit.

3) Supplier assurance and lifecycle. Findings often trace to weak supplier onboarding, change notification and exit criteria. For SaaS and MSPs, auditors look for contractual hooks, independent assurance mapping (e.g., SOC 2, ISO 27017/27018), and periodic technical validation beyond paperwork.

What to do now: run a focused internal audit on Annex A mapping, test a sample of high-risk suppliers end-to-end, and revalidate your risk acceptance criteria against current threat and business impact. Tighten evidence chains—link risks to controls to metrics to management review decisions. Finally, schedule scenario-based tests that exercise detection, response and recovery with third parties in the loop; surveillance cycles in 2026 will increasingly expect this maturity.

ESG & CSRD reporting deep-dive



The CSRD's second reporting wave—covering many additional groups reporting on FY2025 data in 2026—is elevating the bar on governance, traceability and assurance-readiness. Three converging currents define best practice.

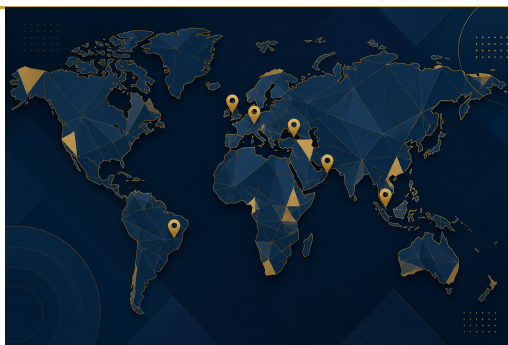
1) ESRS integration with internal controls. Assurance providers are scrutinising how double materiality determinations were performed and governed. Leading filers treat materiality as an auditable process: documented criteria, stakeholder engagement evidence, decision logs, and board approval. Controls over sustainability reporting (ICSR) are being embedded into existing SOX-like frameworks, with clear owners, reconciliations and change management procedures.

2) Data architecture and carbon quantification. Companies using ISO 14064-1 to structure organisational boundaries, base year selection and calculation methodologies are finding fewer challenges from assurance teams, especially where estimates and primary data substitution rules are disclosed clearly. Alignment with the ISSB's IFRS S2 is improving comparability, and many are building a single data model for greenhouse gases, energy (ISO 50001 EnPIs) and financial metrics to support audit trails.

3) Value chain depth and cadence. The most acute pain point remains Scope 3 supplier data. Successful programmes converge procurement, finance and sustainability to enforce data contracts, calendar discipline and escalation paths. Supplier enablement (templates, emission factors, and methodological guardrails) is now a must-have, not a nice-to-have. Expect more limited assurance mandates to expand towards reasonable assurance over selected metrics.

Practical steps for 2026: lock your consolidation calendar with the finance function; publish data dictionaries and calculation handbooks; and rehearse auditor walkthroughs for high-risk topics such as climate targets, transition plans and capex alignment. Where ISSB and ESRS differ, document rationale and ensure consistent signposting across filings. Finally, prepare for deeper scrutiny of scenario analysis, carbon credit usage and internal carbon pricing assumptions.

Country spotlights



United Kingdom	UKAS-accredited certifications remain robust across ISO 9001, 14001, 27001 and 50001, with strong demand from financial services, technology and critical infrastructure. CSRD spillover is material for UK multinationals with EU listings; TPT climate transition-plan guidance is shaping disclosures. The ICO's focus on cyber incidents is nudging tighter 27001 control evidence. Energy price volatility sustains ISO 50001 uptake, particularly among manufacturers. Early adopters are piloting ISO/IEC 42001 to operationalise AI governance ahead of regulatory developments. Auditors report increasing integration of governance, risk and compliance tooling with management system evidence trails.
Germany	DAKKS-backed certifications continue to grow, with automotive, machinery and chemicals driving IATF 16949, ISO 9001 and 50001 demand. CSRD readiness is advanced; many groups are harmonising ESRS with existing Umwelt- and Arbeitsrecht controls. BAFA expectations on supply-chain due diligence intersect with ISO 14001/45001 audits. Energy-intensive Mittelstand firms are deepening EnPIs and sub-metering under ISO 50001. Information security remains strong in industrial OT contexts, with auditors probing patch governance and network segmentation. Medical device clusters focus on ISO 13485 and ISO 14971 alignment to MDR surveillance.
Turkey	The Turkish Standards Institution (TSE) and TURKAK accreditation support steady growth in ISO 9001, 14001 and 22000, especially among food exporters and textiles. Currency and energy cost pressures are pushing manufacturers toward ISO 50001 for operational savings. EU market access remains a driver; suppliers are responding to CSRD data requests and CBAM-related expectations with stronger carbon accounting (ISO 14064-1). KVKK data protection enforcement continues to stimulate ISO 27001 interest, notably among fintech and outsourcing providers. Earthquake resilience has renewed attention on business continuity integration with management systems.
United Arab Emirates	MOIAT and the Emirates International Accreditation Centre (EIAC) underpin rapid adoption of ISO 27001, 22301 and 50001 across government-linked entities, energy and logistics. Free zones (DIFC, ADGM) are catalysing governance and data protection programmes that intersect with 27001/27701. With ambitious net-zero and efficiency targets, facilities management and district cooling operators are scaling ISO 50001. Interest in ISO/IEC 42001 is growing in financial services and smart city programmes as AI deployments expand. Food importers and processors maintain ISO 22000 as a market baseline, with added focus on supply-chain verification.

Singapore

Under SAC accreditation, Singapore maintains high certification maturity in 9001, 27001 and 22301 across finance, ICT and logistics. PDPC/IMDA governance frameworks are catalysing privacy-security integration and early moves on ISO/IEC 42001 for AI governance. Energy efficiency remains policy-backed; ISO 50001 is seeing uptake in data centres and advanced manufacturing. As a regional hub, companies face CSRD-driven data requests from EU clients; many are aligning ISO 14064-1 reporting with ISSB-aligned disclosures. Food manufacturers and cold-chain operators continue to emphasise ISO 22000 and FSSC 22000 schemes.

India

NABCB accreditation under QCI supports strong growth in ISO 9001 and 27001, led by IT services, pharmaceuticals and engineering. IATF 16949 demand is expanding with EV supply chains and electronics manufacturing. Regulators (MeitY, CERT-In) are intensifying cybersecurity expectations, pushing tighter supplier assurance in 27001 audits. Energy costs and Perform, Achieve and Trade (PAT) mechanisms are spurring ISO 50001 in steel, cement and chemicals. Medical device parks are building ISO 13485 capability to serve global markets. CSRD data requests from EU customers are prompting wider adoption of ISO 14064-1 for carbon accounting.

Industry focus



Medical devices (ISO 13485)

Audits are sharpening around post-market surveillance (PMS), complaint trending and field safety corrective actions, with stronger linkage to risk files under ISO 14971. Software as a Medical Device (SaMD) remains a hotspot: lifecycle documentation, cybersecurity interfaces with ISO/IEC 27001, and validation of cloud-hosted services are frequent findings. EU MDR/IVDR surveillance is tightening change control and clinical evaluation traceability, while US FDA's Quality Management System Regulation (QMSR) alignment with ISO 13485 is streamlining multi-market compliance strategies. Practical priorities: clarify design transfer criteria, strengthen supplier qualification for critical components, and verify UDI processes across ERP/LIMS. Expect deeper sampling of DHR/DMR records and CAPA effectiveness evidence.

Automotive (IATF 16949)

IATF audits continue to focus on core tools discipline (APQP, PPAP, MSA, SPC) and the effectiveness of problem-solving routines that close systemic gaps, not just escape points. Change management is under the microscope, particularly for software-enabled components and EV platforms where engineering changes propagate rapidly through tiered supply chains. Expect more scrutiny of customer-specific requirements (CSRs), special processes (CQI audits), and traceability controls during ramp-ups. Suppliers are strengthening management reviews with production readiness metrics and layered process audits to stabilise launches. Cybersecurity interfaces with UNECE R155/R156 are entering scope via customer requirements and need coordination with 27001 for supplier assurance.

Aerospace (AS9100 series)

With production increases across civil programmes, AS9100 audits are testing the robustness of configuration management, FAI (AS9102) discipline and counterfeit parts prevention (AS5553/6081). The IAQG's enhanced certification scheme (9104-1/9104-2) and OASIS V3 are raising expectations for audit planning, PEAR quality and objective evidence. Supplier surveillance is intensifying on special processes, foreign object debris (FOD) prevention, and human factors. Organisations are strengthening risk-based thinking by linking design/manufacturing risk registers to concession data and escapes. Practical priorities: refresh process FMEAs, verify calibration and tooling control at sub-tiers, and ensure problem-solving is statistically validated before closure.

Audit tips & common nonconformities



01. Close the loop on Annex A mapping (27001)

Maintain a live register linking risks to controls to metrics to management decisions. Sample a few high-risk scenarios and walk the thread end-to-end with evidence. Auditors will reward clarity and penalise disconnected artefacts.

02. Stress-test change control (9001/IATF/AS)

Pick three recent engineering or process changes and audit their ripple effects: risk review, validation, training, document control and supplier notification. Look for unintended consequences on capability, scrap and warranty.

03. Metering before retrofits (50001)

Before capex, verify sub-metering and data quality on significant energy uses. Use short M&V cycles to quantify savings potential and set EnPIs. Weak data undermines both investment cases and audit confidence.

04. Materiality as a controlled process (CSRD/ESRS)

Treat double materiality like an auditable workflow: criteria, stakeholders, evidence, decisions and approvals. Lock the calendar to financial close and document estimation methods and controls for any modelled data.

05. Supplier assurance beyond paperwork

For critical SaaS/MSP or special process suppliers, run periodic technical validations (e.g., configuration reviews, witness audits) and map third-party attestations to your requirements. Define exit criteria up front.

06. Food safety culture with evidence (22000)

Demonstrate culture through leading indicators: near-miss trends, hygiene observation scores, corrective action timeliness and management Gemba notes. Tie results to training content updates and resource allocation.

Standards on the horizon



ISO 9001—Revision (DIS/FDIS) — DIS under ballot; FDIS targeted for later in 2026 (subject to committee timelines)

The revision maintains Annex SL structure with clearer expectations on risk-based thinking, change management and performance evaluation. Organisations should begin structured gap assessments, prioritising objective cascades, process interfaces and data-driven improvement. Sector schemes (IATF 16949, AS/EN 9100) are expected to follow with alignment updates after publication; early planning will smooth multi-standard transitions.

AS9100 series—Alignment after ISO 9001 revision — Planned update by IAQG post-ISO 9001 publication

The aerospace quality management standards are expected to align once ISO 9001 is finalised. IAQG working groups are analysing potential impacts on risk-based thinking, configuration management interfaces and supplier oversight. Organisations should monitor OASIS communications and prepare for transition planning that coordinates with 9104-1/2 scheme requirements.

ISO 13485—Next revision initiative — Revision project under discussion to improve alignment with EU MDR/IVDR and US FDA QMSR

A future revision is being scoped to address terminology harmonisation, software lifecycle expectations and post-market surveillance linkages to risk management. While timelines are still being set, design and supplier controls are likely to see clarified requirements. Manufacturers should maintain robust technical documentation and change control to ease any forthcoming transition.

ISO 14064-1—Alignment and guidance work within TC207 — Ongoing committee activity exploring enhancements and guidance harmonisation

Work continues within ISO/TC 207 on improving consistency with market practices and interoperability with frameworks such as the GHG Protocol and emerging ISSB requirements. Organisations can future-proof by documenting boundaries, base years and estimation methods transparently, and by aligning internal controls over GHG data with financial reporting disciplines.

Coming next month

June's issue will unpack the ISO 9001 ballot feedback and what it signals for clause-by-clause transition planning. We will also examine how early ISO/IEC 42001 certifications are structuring AI model inventories and risk acceptance, and compare audit evidence expectations across ISO 14064-1, ESRS and ISSB. Finally, we will look at energy contracting strategies that complement ISO 50001, and run a sector round-up on supplier quality performance in aerospace and automotive ramp-ups. Send us your toughest audit questions—we will tackle them with practical checklists.

About UniCert

UniCert is a UK-headquartered accredited certification body delivering ISO certification, inspection, training, ESG sustainability assurance and supply-chain audit services to organisations worldwide. Our auditors operate across Europe, the Middle East, Asia and the Americas under recognised IAF MLA accreditation arrangements.

Need a quote, gap analysis or audit reminder?

Visit www.unicertification.co.uk or email info@unicertification.co.uk

This newsletter is produced for informational purposes only and reflects publicly available information at the time of writing. It does not constitute legal, regulatory or audit advice.