



AI Governance – the role of ISO/IEC 42001

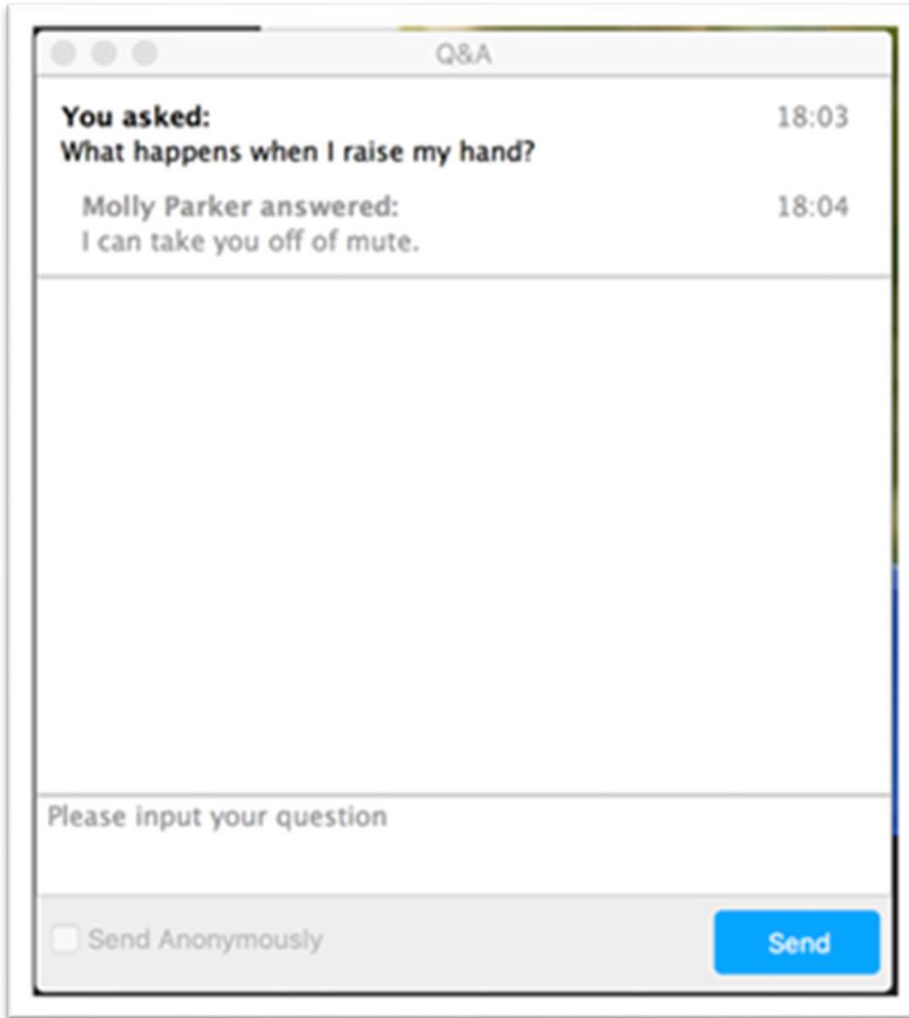
Date: 26 September 2025

Speakers: Esther Mallowah, ICAEW

Pauline Norstrom, Anekanta®AI and Anekanta®Consulting

Dr Sam De Silva, CMS

Ask a question



The screenshot shows a web application window titled "Q&A". It displays a history of questions and answers. The first entry shows a question asked at 18:03 and an answer by Molly Parker at 18:04. Below the history is a large text input area. At the bottom, there is a label "Please input your question", a checkbox labeled "Send Anonymously", and a blue "Send" button.

Text	Time
You asked: What happens when I raise my hand?	18:03
Molly Parker answered: I can take you off of mute.	18:04

Please input your question

☐ Send Anonymously Send

Click on the Q&A button in the bottom toolbar to open the submit question prompt.

Type in your question and click send.

Note. If you wish to ask anonymously tick the send anonymously box shown on the illustration to the left.

Today's presenters



Pauline Norstrom
CEO
Anekanta®AI and
Anekanta®Consulting



Dr Sam De Silva
Partner and Global Co-Head
Commercial Practice Group
CMS



Esther Mallowah
Head of Tech Policy
ICAEW

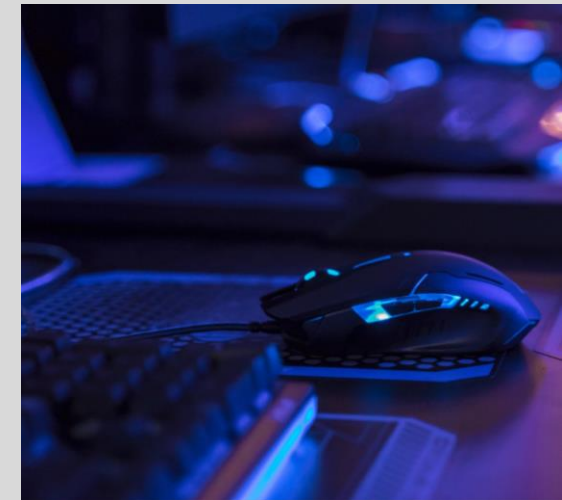
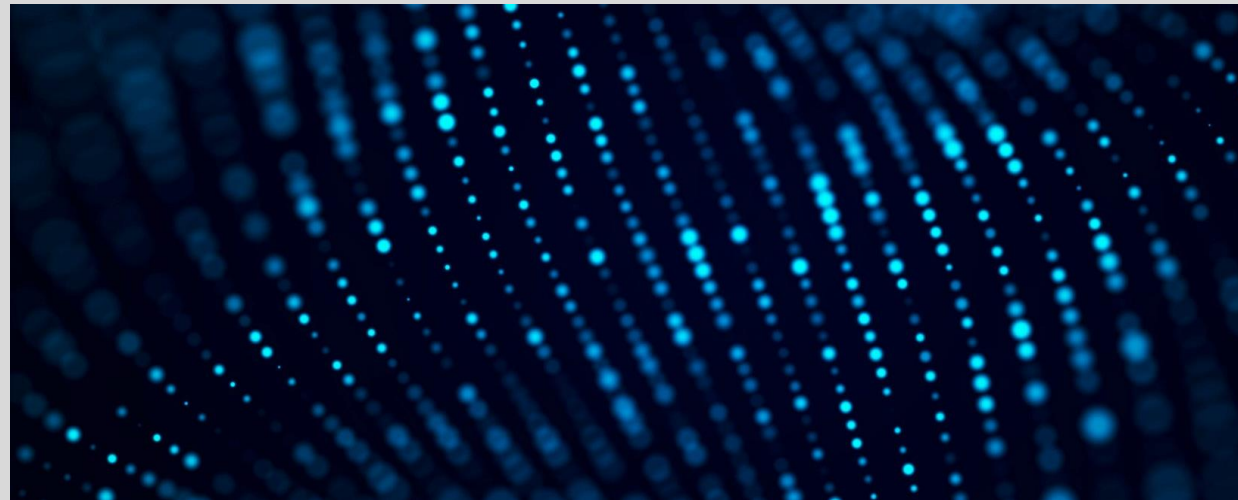
Poll: How familiar are you with ISO/IEC 42001?

- Very familiar – have significant experience working with the standard
- Somewhat familiar – have some experience working with the standard
- Basic – have had limited involvement with the standard
- None – what is ISO/IEC 42001?

ISO management system standards

What accountants need to know

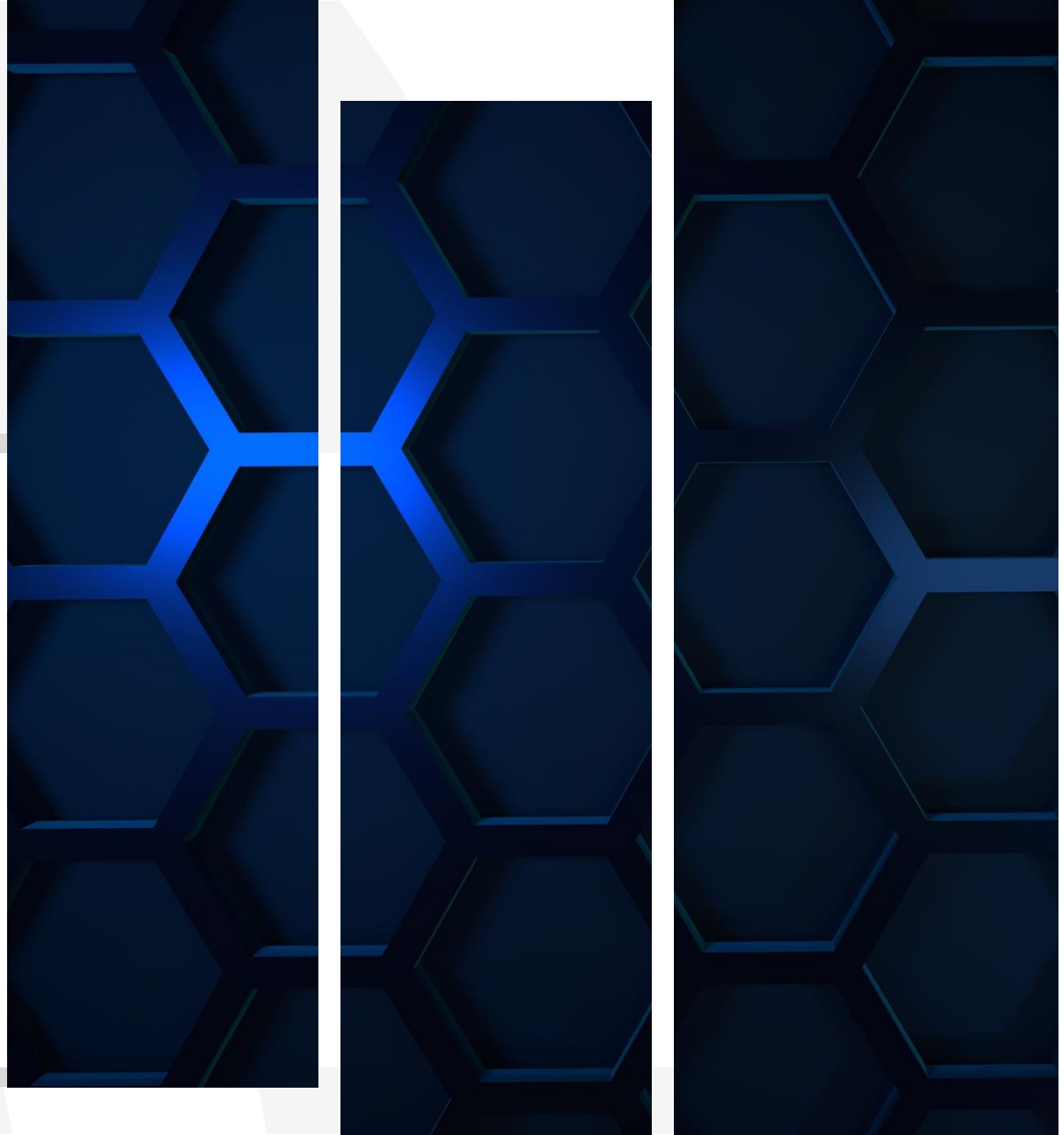
- Annex SL = shared 10-clause structure → easy integration of ISO 22301, ISO 37001, ISO 9001, etc
- Management system standards focus on the “how”; they are certifiable and give external assurance
- Technical standards focus on the “what”; generally not certifiable (e.g. ISO 14064 for GHG reporting)
- Integrated systems reduce duplication, clarify accountability and streamline audits for regulators and investors.
- Key benefit is a common, auditable language for risk management, compliance, and value creation



ISO/IEC 42001

The new global AI management system standard

- First certifiable framework dedicated to **responsible AI** across the entire enterprise
- Mirrors Annex SL + Plan-Do-Check-Act cycle → aligns with existing ISO management systems
- Core requirements:
 - AI management policy and governance roles
 - full inventory of AI use cases
 - risk assessments (ethical, legal, operational, financial)
 - controls for transparency, stakeholder engagement and incident response
- Treats AI as a business-wide capability, not isolated pilots
- Certification can reassure boards, regulators, investors and clients that AI is well-governed



Applying ISO/IEC 42001 in practice

Opportunities and limits

- Governance: objective criteria for internal audit and external assurance
- Risk reduction: early detection of bias, data-quality issues and compliance gaps
- Commercial edge: certification differentiates firms in tenders and due-diligence processes
- Example – automated expense approvals: map AI workflow, audit fairness, set escalation paths, document decisions
- Leverages existing ISO systems, minimising extra overhead for multi-standard organisations
- Caveats: process-oriented (quality of outputs not guaranteed), certification is a snapshot in time, and costs may outweigh benefits for limited AI use
- Recommendation: blend ISO/IEC 42001 with technical controls, robust contracts and professional judgement to embed a culture of continual improvement

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

CMS is an international organisation of independent law firms ("CMS Member Firms"). CMS LTF Limited (CMS LTF) is a company limited by guarantee incorporated in England & Wales (no. 15367752) whose registered office is at Cannon Place, 78 Cannon Street, London EC4N 6AF United Kingdom. CMS LTF coordinates the CMS Member Firms. CMS LTF provides no client services. Such services are solely provided by CMS LTF's CMS Member Firms in their respective jurisdictions. CMS LTF and each of its CMS Member Firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS LTF and each CMS Member Firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the CMS Member Firms or their offices; details can be found under "legal information" in the footer of cms.law.

CMS Locations

Aberdeen, Abu Dhabi, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bengaluru, Bergen, Berlin, Bogotá, Bratislava, Brisbane, Bristol, Brussels, Bucharest, Budapest, Casablanca, Chennai, Cologne, Dubai, Dublin, Duesseldorf, Ebene, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Gothenburg, Gurugram, Hamburg, Hong Kong, Hyderabad, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Maputo, Mexico City, Milan, Mombasa, Monaco, Mumbai, Munich, Muscat, Nairobi, New Delhi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, São Paulo, Sarajevo, Shanghai, Sheffield, Silicon Valley, Singapore, Skopje, Sofia, Stavanger, Stockholm, Strasbourg, Stuttgart, Sydney, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

Further information can be found at **cms.law**

UK - 713577250.1



Dr Sam De Silva

Partner & Global Co-Head Commercial Practice Group

E sam.desilva@cms-cmno.com

T +44 20 7524 6223

ISO 42001 - How to get started

1

PLAN

Define Scope & Policy (Clauses 4-6)

Define the AIMS context, boundaries, and interested parties; approve the AI policy; set risk assessment criteria; establish objectives, KPIs, and an implementation roadmap

2

DO

Implement Controls (Clauses 7-8)

Implement planned processes and controls: roles & responsibilities, competence & training, documented information; AI lifecycle controls (data, models, validation, change); supplier/third-party management; maintain auditable records.

3

CHECK

Monitor and Measure (Clause 9)

Monitor and measure KPIs; log incidents and nonconformities; conduct internal audits; hold management reviews; maintain an evidence trail linked to objectives and risks.

4

ACT

Corrective Action (Clause 10)

Execute corrective actions; update the risk treatment plan; improve controls; refresh objectives/KPIs; communicate outcomes and reinforce awareness

Common Pitfalls

Treating ISO/IEC 42001 as a certificate rather than an operating system for AI.

AIMS scope too narrow or vague; AI risks omitted.

Missing audit evidence and records for assessments and reviews.

Unmanaged supplier/third-party AI risks (lifecycle and contractual controls).

AI risk management not integrated with business strategy, leading to low awareness.

Lessons Learned

Top-level leadership commitment with budgeted objectives is critical for AI policy effectiveness.

Clear scope definition and criteria avoid costly audit challenges.

Evidence-based KPIs and named artefact owners make audits mechanical.

Integration via Annex SL with ISO 27001/9001 improves efficiency and consistency.

Scheduled continual improvement (e.g., quarterly) sustains resilience, trust, and a living framework.

Remember sector/use case specific AI standards may be applicable. Risk controls may include standards for data quality, transparency, bias, software development lifecycle etc.

Annual Cyber Lecture

**Ransomware and the evolution of the
cyber threat - from data protection to
resilience**

**6 October 2025
18:00 – 20:30 BST
Chartered Accountants' Hall**



Starting your NED career early: is being a Trustee the right path?

Everything you need to know about a trusteeship as the first step on your route to being an NED.

**29 October 2025
12:00 – 13:00 GMT
Zoom webinar**





[icaew.com](https://www.icaew.com)