ISO 42001 - Key Takeaways from 9 Video Transcripts

THE BIGGEST INSIGHT: You Need ISO 42001 ✅

Why: It's the ONLY AI certification standard
Who else has it: Microsoft, Google, Amazon, Anthropic
What Microsoft does: Requires vendors in SSPA program to get it
Your decision: Yes, get it

TIMELINE REALITY

Implementation: 6 months
Certification: +6 months
Total: 12 months to certified

Effort by team: - Leadership: 1-2 hours total - GRC/Risk: 1-2 weeks (most work) - Engineering: 1 day + evidence gathering - Legal: Half day

Bottom line: Manageable if organized.

KEY DIFFERENCE: AI Impact Assessment

This is the new thing that doesn't exist in ISO 27001:

Risk Assessment: What could go wrong with AI?
Impact Assessment: How could AI harm people?

Real example: Lending company found bias in credit scoring → built transparency tools + bias detection

Both required by ISO 42001.

THE HARDEST PART

NOT paperwork ❌

IS engineering integration ✅

Why? - Context dependent (ChatGPT vs custom LLM vs orchestration) - No universal best practices yet - Requires AI expertise, not just compliance

Reality: This is where actual work happens.

SCOPE STRATEGY

You can scope very narrow: - Example: 500 employees, 6 people on AI phone system - Scope: Just that phone system application - Saves: Time and money on certification

Four roles affect audit days: - Developer - Provider - User
- Multiple

No discounts: Only additions allowed (unlike MD5 which allows 30% reductions)

CERTIFICATION MECHANICS

Stage 1: Design review (1-2 days, 20-25 artifacts)
Stage 2: Full audit (30-45 days later, 75-100 artifacts)
Surveillance: Year 2-3, ~1/3 of controls
Recertification: Year 4, start over

Remote audits: Work fine, just like ISO 27001

Auditor shortage: Real problem right now - zero applicants after 2 months of marketing
Hybrid approach: Technical experts + ISO Auditors working together

---

PRIVACY & CONSENT REALITY

PII in AI context: - Not just medical data - Includes ALL browsing behavior - What you search = PII when combined with identity

Consent: 99% mandatory (made so for legal defense)
May not be fair: But that's the reality
Privacy workaround: Take data without identifying individuals (enough data points = can still identify)

BIAS vs ETHICS

Different concepts: - **Bias**: Always bad (favoring someone unfairly) - **Ethics**: Contextual (may be correct for certain scenario)

Examples: - Medical AI only recommending one medicine = bias - Cultural adaptation for region = ethics

Both need management: But understanding difference matters

MARKET EXPLOSION COMING

Prediction: Will surpass ISO 27001 growth "very quickly"
Currently: Fastest growing AI certification globally
ANAB: Already got 4 applications, expecting 20-25 by end of 2024
New players: AI companies want to become certification bodies
All industries: Healthcare, finance, automotive, aerospace, marketing, call centers

Your opportunity: Get ahead of the curve.

AI WILL IMPACT CERT PROCESS

Already happening: One AB in Asia using AI to write audit reports
Within 2-3 years: Common
Workgroups started: IAF and ITIC looking at AI use in certification

Uses: - Writing non-conformities (more consistent) - Developing audit plans - Assisting in process

Reality: AI auditing AI governance is coming.

CANADIAN PILOT

When: Last summer
Who: Banking institution
Results: Fed back to workgroup, influenced DISC → FDIS changes

Lesson: Real-world audits happening and improving the standard

---

TRAINING & COMPETENCY

Required: - Information security experience - Two years AI experience - Three-day training course - Lead Auditor: 3 audits (chicken/egg problem!)

Available training: Very limited right now
Timeline: 6-12 months before Exemplar Global and IEA add programs
Sources: Universities, industry contracts, AB/CB websites

Reality: Everyone playing catch-up because standard published early.

BOTTOM LINE FOR KAIZEN

1. **Buy ISO 42001**: Just that one ($280 CAD)
2. **Timeline**: 6 months implementation + 6 months certification
3. **Focus**: Engineering integration is hardest part
4. **Scope**: Can be narrow to save money
5. **Unique piece**: AI Impact Assessment (not just risk)
6. **Market**: Exploding - get ahead
7. **Privacy**: More complex than it appears
8. **Cert process**: Remote works, auditor shortage real
9. **AI audits AI**: Coming within 2-3 years

Most valuable documents: Your workflows, checklist, and insights doc
Best practical advice: Scope to single application to save money
Biggest unique concept: AI Impact Assessment vs Risk Assessment

---

Sources: Risk 360, Structure Tutorial, Standards Australia, Certified Info Sec, Ministry of Security (2x), Interser, LRQA, Perry Johnson Registrars
Total transcribed: 2,948 lines from 9 expert sources