Two Standards One Strategy

Unlocking value with ISO/IEC 27001 & ISO/IEC 42001

BSI - Fran Caballero and Vindhya Kothuri

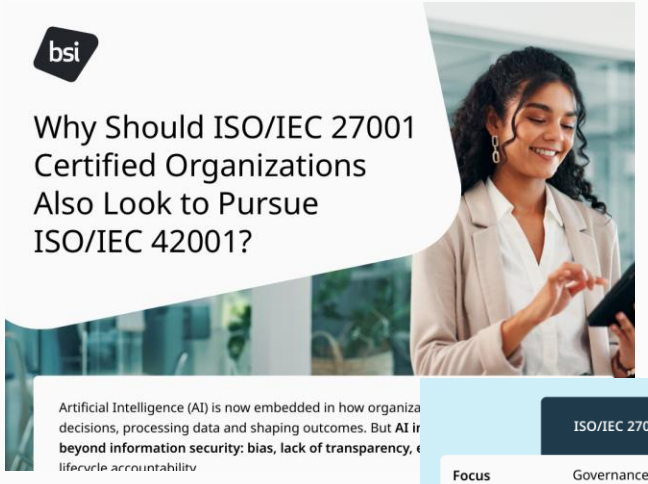
Darktrace – William Booth and Shanita Sojan

14 May 2026

Hello and welcome

- In this webinar we will cover:
  - what ISO/IEC 27001 is and the role it plays in information security management
  - what ISO/IEC 42001 is and how it supports the governance of AI systems
  - how ISO/IEC 27001 and ISO/IEC 42001 compare, differ and overlap
  - how to integrate the two standards within your organization
  - Darktrace's experience of integrating both standards

- Q&A at the end of the webinar – please add your questions to the chat
- You will get a copy of slides and a recording of the webinar
- Opportunity to ask for a follow up from BSI on the feedback form – available immediately after the webinar concludes.



	ISO/IEC 27001	ISO/IEC 42001
Focus	Governance of information security and cyber risks	Governs how AI systems are developed, deployed, and managed and used
Covers	Risk management, cyber resilience and operational excellence in information security	Bias, transparency, societal impact, lifecycle accountability and intended use
Scope	Defines which information assets are in scope and ensures the appropriate level of confidentiality, integrity and availability	Defines which AI systems, components and roles are included

What this means:

A separate scope statement is needed:
Your ISO/IEC 27001 scope does not automatically

Download your free ISO/IEC 27001/42001 infographic

Meet our speakers

Fran Caballero

AI Client Manager

Fran is an AI specialist with 8+ years' experience in machine learning, risk assessment, privacy compliance, and data protection. He audits AI workflows, with expertise in NLU and voice-based devices.

Vindhya Kothuri

AI Client Manager

Vindhya is an AI Client Manager at BSI with 23 years' experience in software development, product management, and AI. Her expertise spans computer vision, IoT, smart cities, BIM, ISO 27001, ISO 42001, and the UK DIATF Trust Framework.

William Booth

Director, Cybersecurity Compliance

William Booth is Director of Cybersecurity Compliance at Darktrace, overseeing ISO 27001 and ISO 27018 certifications. He helped establish Darktrace's Artificial Intelligence Management System, supporting its early ISO 42001:2023 certification.

Shanita Sojan

AI Governance & Cybersecurity Compliance Specialist

Shanita Sojan is a Cybersecurity Compliance professional at Darktrace, working across AI governance and security compliance. She contributes to global AI safety initiatives and is a Global Ambassador for the Global Council for Responsible AI.

Understanding our audience

Where are you in your AI journey?

Which of the following certifications do you currently have?

- ISO/IEC 27001
- ISO/IEC 42001
- Both ISO/IEC 27001 and ISO/IEC 42001
- None of the above

Which area is the biggest priority for your organization?

- Strengthening information security management
- Establishing responsible AI governance
- Integrating AI risk into existing governance frameworks
- Building customer, regulator or stakeholder trust

What best describes your organization’s current AI journey?

- We are experimenting with AI
- We are scaling AI across the business
- We have defined AI strategy but early stages
- We have no AI initiatives yet

The Resilience Architecture

Integrating Security & AI Governance

Harmonizing ISO/IEC 27001 & ISO/IEC 42001

The convergence of Information Security and AI Governance

Building a Trusted and Future-Ready Organization

Supporting business growth, trust, and regulation readiness

Why are you here – Unlocking value

How AI governance fits into your information security program

A practical framework for becoming AI trust-ready

Clear boundaries between governance, compliance, and certification

Poll 1
Who leads AI Governance vs. Information Security in your company?

a) Two separate teams with different priorities

b) The Security team is trying to manage AI risks too

c) A single unified team with a common roadmap

d) We are still deciding who should take the lead

Why this matters now – The cost of inaction

- Rising EU AI Act enforcement and governance scrutiny
- Accelerating customer trust requirements
- Transforming security from a shield into a competitive differentiator

The Foundation & The Framework

ISO/IEC 27001

- Information Security (ISMS).
- Confidentiality, Integrity, Availability.
- Protection of the Data.

ISO/IEC 42001

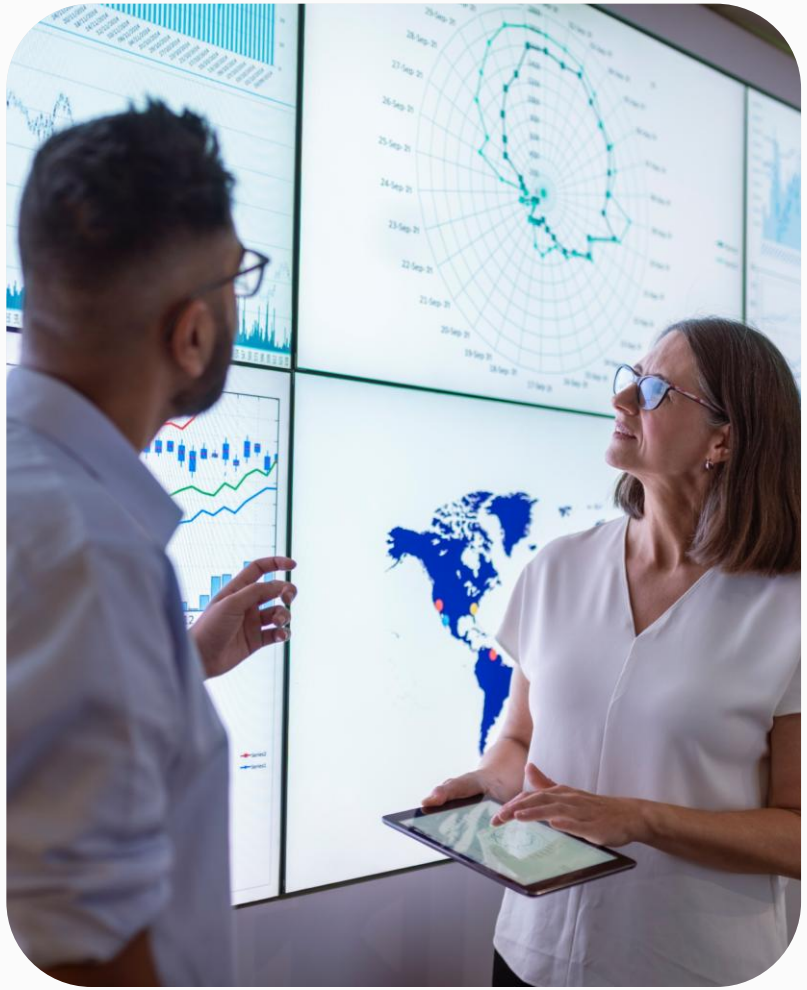
- Artificial Intelligence (AIMS).
- Ethics, Bias, and Transparency.
- Protection of the Decision.

Understanding the Needs: One or Both?

- ISO 27001 (The Container): Focus on data protection and cyber threats
- ISO 42001 (The Content): Focus on AI decisions, bias, and fairness
- Both are necessary for scaling AI in highly regulated markets

The Power of Integration – One Strategy: Shared DNA

- High-Level Structure (HLS)
- Unified Leadership
- Integrated Risk Management

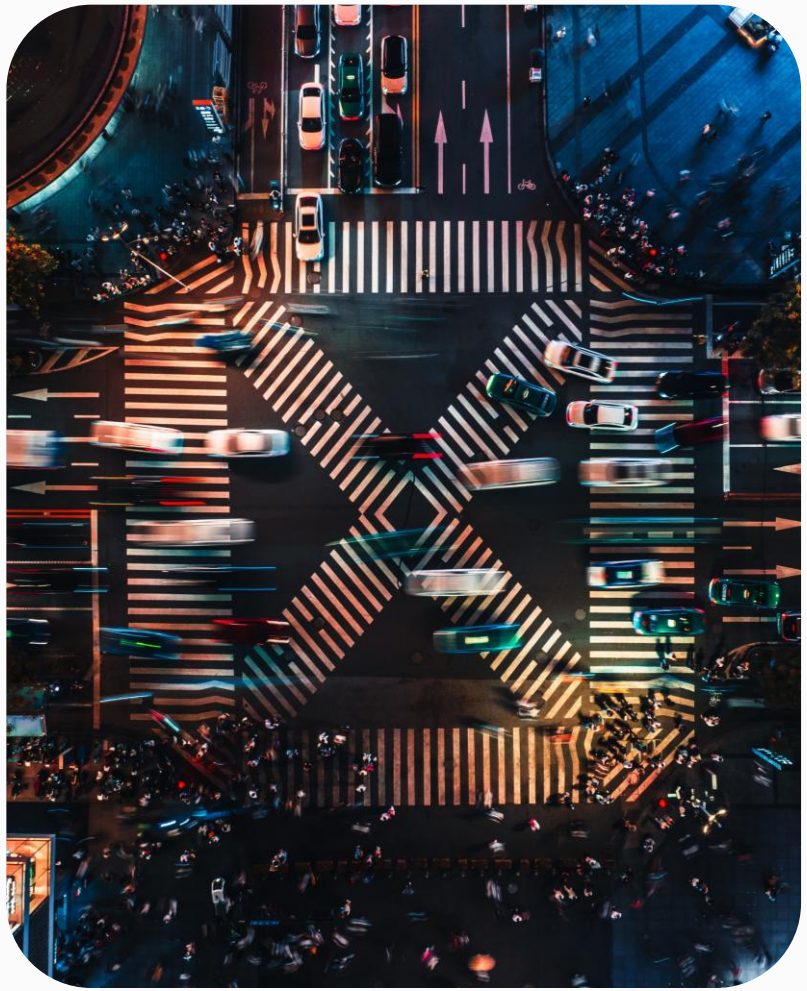


Implementing the Resilience Architecture

- Gap Analysis of current ISO 27001 controls
- Integrated Risk Assessment
- Updating the Statement of Applicability (SoA)

Navigating Strategic Missteps

- Unclear boundaries of AI systems
- Security goals that ignore AI performance/ethics
- Generic policies vs. operational reality



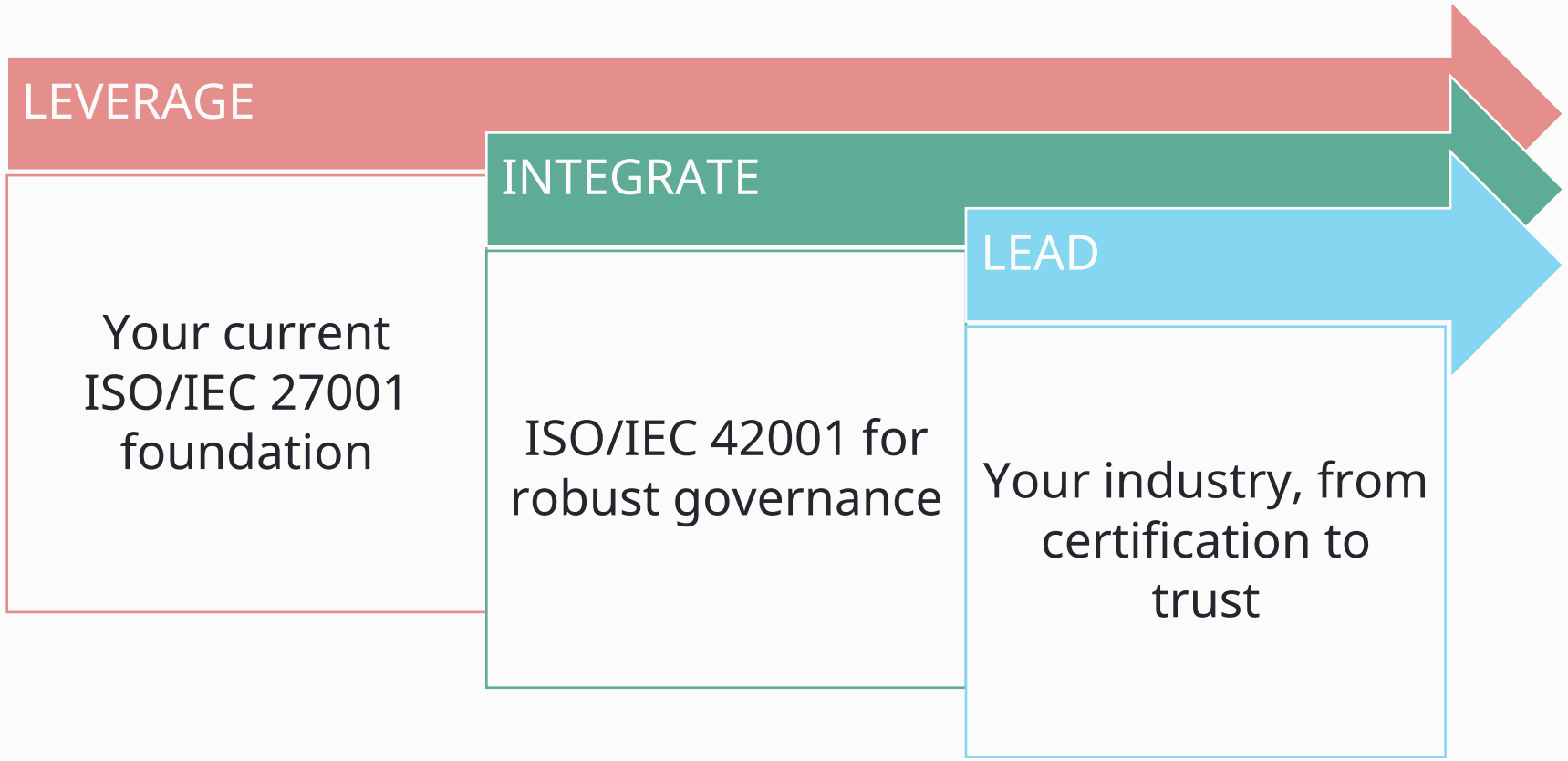
Poll 2

What is your biggest concern regarding integrated implementation?

a) Cost

b) Complexity

Roadmap to a Future-Ready Organization



Poll 3

Does ISO 42001 guarantee legal compliance with the EU AI Act?

a) Yes

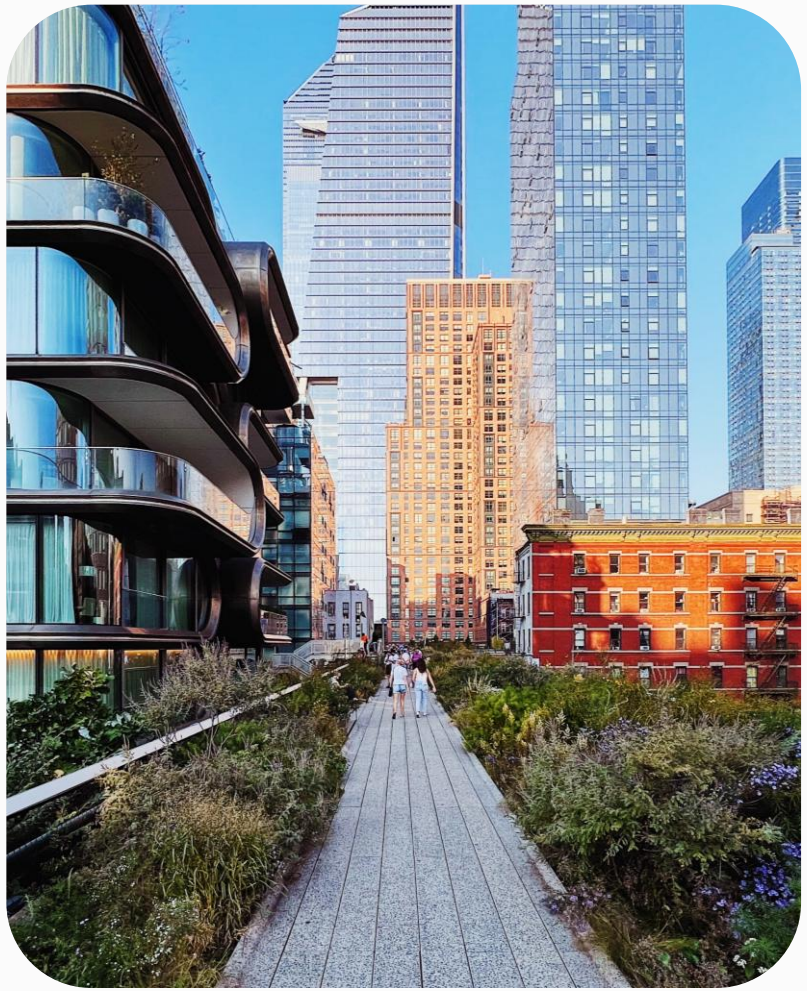
b) No

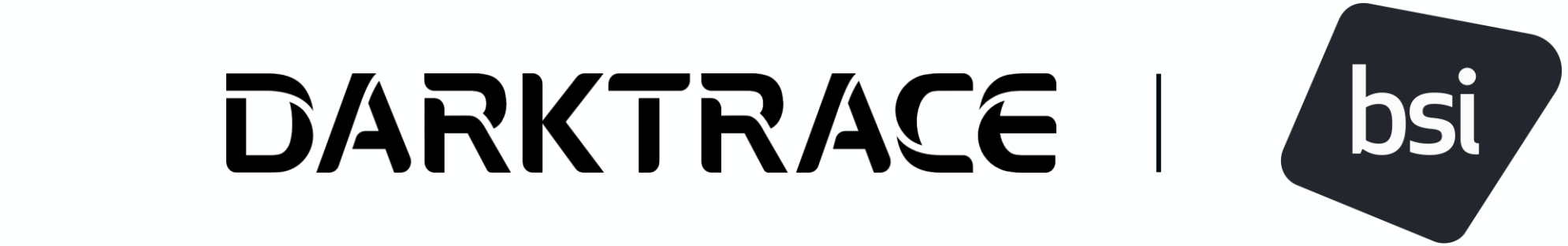
The Reality Check of the EU AI Act

- ISO/IEC 42001: voluntary organizational governance
- EU AI Act: mandatory Product Safety & Market Law
- AIMS provides the Quality (Art. 17) and Risk (Art. 9) Infrastructure

Driving Growth, Trust, and Regulatory Readiness

- Faster time-to-market for AI products
- Competitive edge: 'Certified Trustworthy'
- Best-in-class preparation for future laws




DARKTRACE
bsi

DARKTRACE

ISO 42001: Our Journey

Presented by:

William Booth

Director, Cybersecurity Compliance

Shanita Sojan

Team Lead, Cybersecurity Compliance

Darktrace at a Glance

2013

Founded

10,000

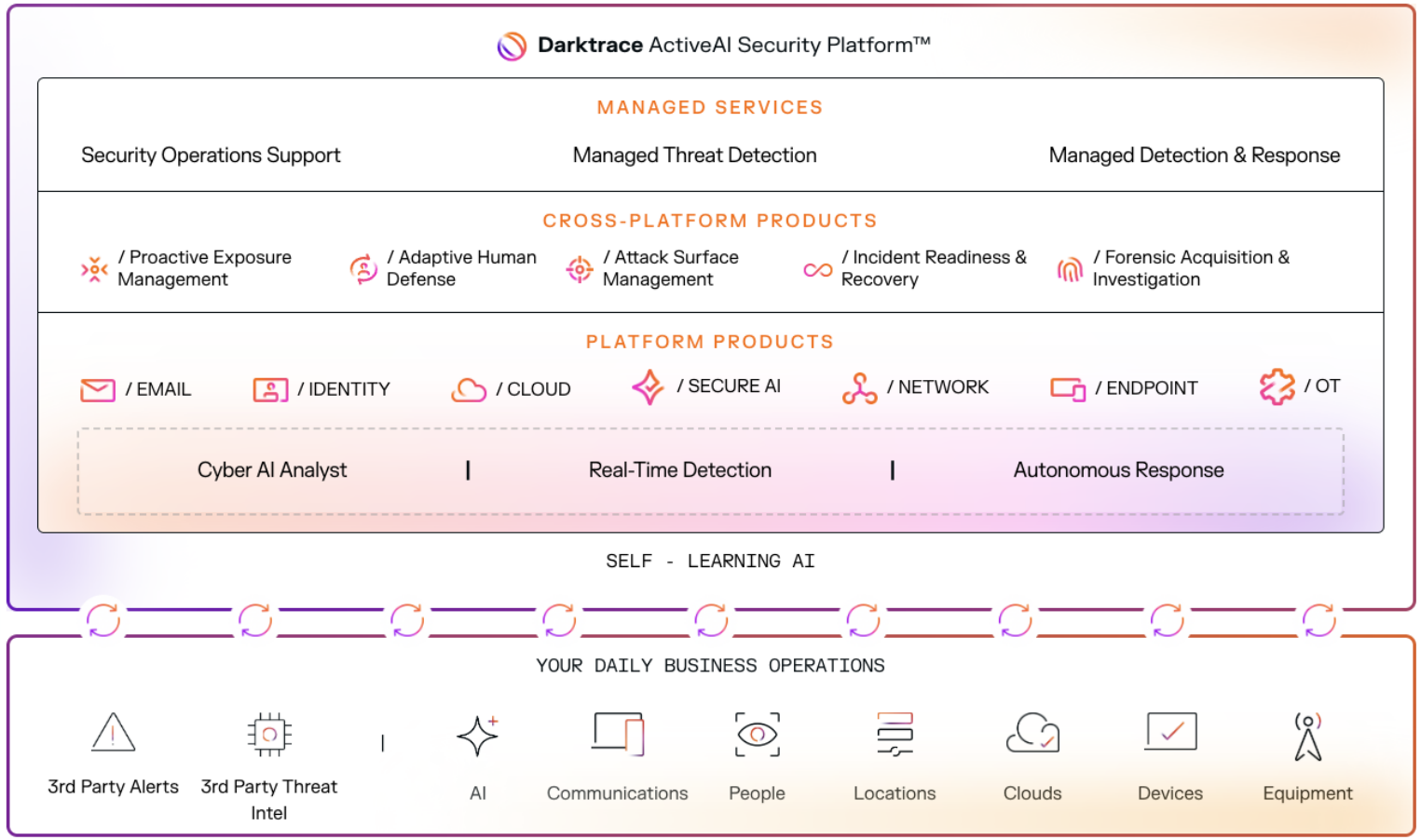
Customers

110

Countries

2,300+

Employees



Our Compliance Journey

Mar 2017 // **ISO 27001**

Darktrace achieves ISO 27001 certification

Sep 2021 // **ISO 27018**

Darktrace achieves ISO 27018 certification

Dec 2024 // **ISO 42001**

Darktrace pursues ISO 42001 (June) Stage 1 Audit passed

May 2025 // **ISO 42001**

Darktrace achieves ISO 42001 certification

Darktrace Certified Frameworks

ISO/IEC 42001:2023 (AI Management System) - ISO/IEC 27001:2022 (Information Security Management System)

ISO/IEC 27018:2019 (Protection of PII data in public cloud) - Cyber Essentials (UK Government baseline certification)

Why We Chose to Be an Early Adopter

Customer Trust

Enterprise and government customers need independent evidence – not just our word – that our AI systems are governed responsibly.

Regulatory readiness

EU AI Act obligations were approaching. We wanted to establish our Responsible AI program before being required to – not scramble afterwards.

Product Credibility

ISO 42001 scope covers production and provision of our AI systems directly. Certification strengthens the credibility of our products in market.

Setting the benchmark

As an AI cybersecurity company, we wanted to demonstrate what good AI governance looks like and help define it for the sector.

What ISO 42001 Governs at Darktrace

Data Provenance

How is the data underpinning our AI models sourced, assessed for bias and documented? Who owns it and what are our obligations?

AI lifecycle

How are Darktrace's AI models designed, validated and deployed from R&D through production and eventual retirement?

Impact Assessment

What are the effects of our AI decisions on customers and wider society? Assessed before deployment, reviewed on every significant change.

Third-Party AI Risks

How do we govern AI Suppliers used within the organisation as well as the third-party AI models, datasets, open-source licensing embedded in our products?

GenAI Guardrails

Controls governing internal AI usage for productivity, AI agent deployments – data boundaries, human oversight requirements and AI concern reporting.

Ongoing Monitoring

Management reviews of our AIMS, concern reporting and performance evaluation of AI systems, surveillance audits, internal audits and corrective action cycles.

How ISO 27001 & ISO 42001 Work Together

ISO/IEC 27001 + ISO 27018

Protecting our information and customer data

- How we build, sell and operate our cybersecurity products securely?
- How we handle and protect confidential customer data and PII?
- Access control, encryption and incident response across our platform
- Security assurance our 10,000+ customers rely on for procurement

Shared Foundation

- Risk- based management approach
- Shared policies, procedures and documentation
- Internal Audit
- Continuous improvement

ISO/IEC 42001

Trustworthy and safe AI deployment

- How our AI models are designed, trained and validated for cybersecurity
- Data provenance and bias assessment for AI powering our detections
- Third-party LLM and model supplier risks.
- AI impact assessment before deploying changes to our AI systems.

Why Certifying Now Puts You Ahead of the Regulation

Proactive Compliance Readiness

Demonstrates proactive AI governance before regulations become mandatory (Aligns to EU AI act and NIST AI RMF)

Procurement advantage

Enterprise and government customers are already filtering vendors by AI questionnaires. Certification removes friction from high-value deals.

Lower Future Compliance Costs

Reduce future compliance costs and last-minute remediation efforts.

Competitive Market Advantage

Creates a competitive advantage by proving responsible and trustworthy AI practices ahead of competitors.

Three Myths – Quickly Busted

Myth 1

“It’s just ISO 27001 for AI”

Reality

ISO 27001 protects information. ISO 42001 governs AI systems themselves – data provenance, impact assessment, model risks. They address entirely different risks and are both needed.

Myth 2

“It’s only for AI labs and model builders”

Reality

Any organization developing, deploying, or using AI in its products or decision is in scope. If AI influences outcomes for your customers, ISO 42001 is relevant.

Myth 3

“It’s a documentation exercise”

Reality

BSI sampled Darktrace’s AI systems over 13.5 days of assessment. Controls must be operational and evidenced – not just written. This is substantive, rigorous governance.

What Certification Actually Delivered

Greater Control Over AI Systems

ISO 42001 gave us structured oversight of our AI systems – clear ownership, documented risk treatment and defined accountability across the full AI lifecycle.

Industry Best Practices Embedded

Data provenance, impact assessment, third-party AI supplier risk and GenAI guardrails are now systematic, auditable and continuously improving.

Overall Security Program Strengthened

Achieving ISO 42001 alongside our existing frameworks raised the bar across our entire security program – more rigorous, more consistent, more defensible.

Customer Trust – Real Commercial Impact

Two enterprise customers moved directly into trialing without lengthy RFI processes – citing ISO 42001 certification as the basis for their confidence in Darktrace's AI products.

DARKTRACE

Thank You

Any questions for our speakers?

Fran Caballero

AI Client Manager

Vindhya Kothuri

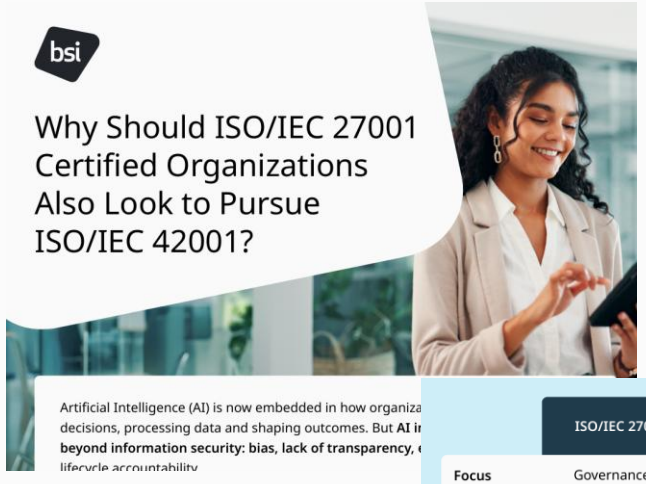
AI Client Manager

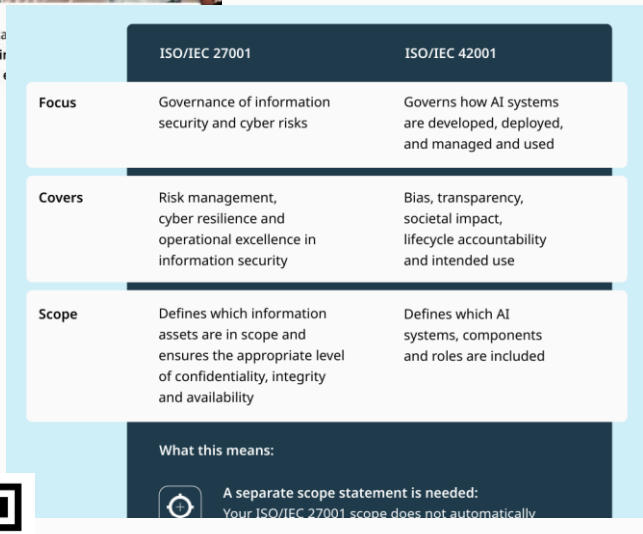
William Booth

Director, Cybersecurity Compliance

Shanita Sojan

AI Governance & Cybersecurity Compliance Specialist





Download your free ISO/IEC 27001/42001 infographic

Thank you

bsigroup.com/ai