WEBINAR RECORDED

PECB

Are We Letting AI Run Wild? ISO/IEC 42001 and ISO/IEC 27001 Reality Check

APRIL 30 | 03:00 PM CEST

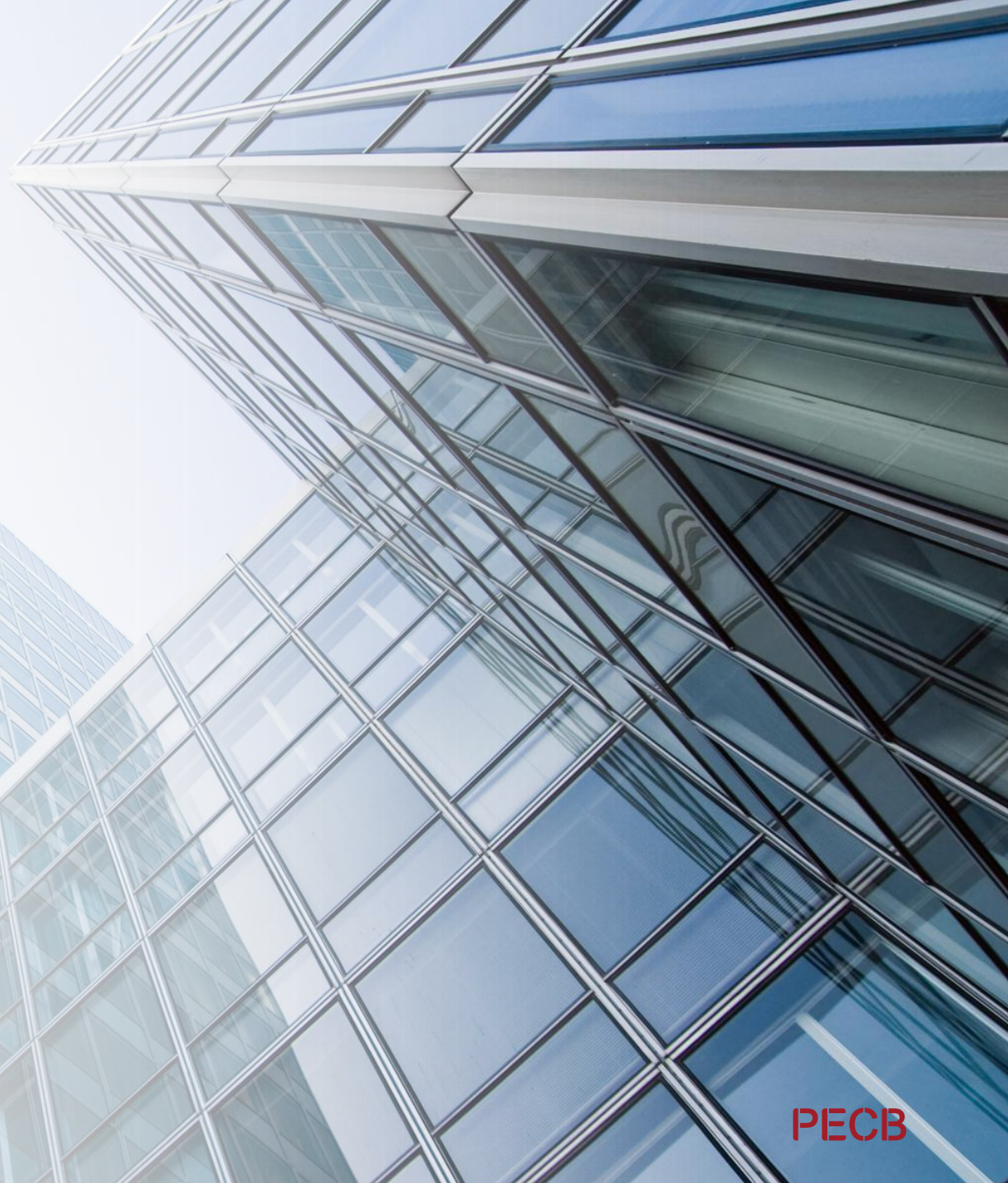
Driton Bejtullahu

CEO at Be Consulted

#GlobalLeadingVoices

Agenda

- AI Risks & Security Gaps
- ISO/IEC 27001 vs ISO/IEC 42001
- Governance & Control Gaps in AI
- Regulatory & Stakeholder Expectations
- Practical Alignment & Implementation
- Q&A



PECB

AI Risks & Security Gaps

Think about your current security setup—where might AI introduce risks you haven't yet considered?

Stakeholder	Typical Responsibilities	Key Risks / Concerns
AI Provider (AI platform provider, AI product/service provider)	Deliver AI platforms and services securely and reliably- Ensure availability, performance, and compliance with standards- Provide transparency in features and limitations	**Service outages, Security breaches, Misuse of platform, Vendor lock-in risks**
AI Producer (AI developer)	Design, build, and test AI models- Document model design, training data, and evaluation- Ensure accuracy, robustness, and ethical alignment	**Bias in datasets and models, Lack of explainability, Intellectual property issues- Inadequate validation**
AI Customer (AI user)	Adopt AI responsibly in business or daily use, Apply provider/producer guidance correctly, Ensure lawful and ethical use of AI outputs	**Misinterpretation of AI results- Over reliance on AI (automation bias) Liability for harmful decisions- Lack of internal expertise**
AI Partner (system integrator, data provider, evaluator, auditor)	Supply data, integration services, audits, or evaluations, Ensure interoperability with other systems, Provide independent assurance on fairness, security, compliance	**Data quality issues- Conflicts of interest in evaluation/auditing- Inaccurate or incomplete integrations, Supply chain vulnerabilities**
AI Subject (data subjects, affected individuals)	Provide data (directly or indirectly), Participate as the population AI systems act upon, Exercise rights over personal data (e.g., GDPR)	**Privacy violations, Discrimination or unfair treatment, Lack of consent/awareness, Limited ability to challenge decisions**
Relevant Authorities (policy makers, regulators)	Define AI-related regulations, standards, and ethical frameworks, Monitor compliance through audits, enforcement, and certification, Provide guidance for responsible adoption	**Regulatory gaps or delays, Over regulation stifling innovation Jurisdictional conflicts, Limited technical expertise for oversight**

ISO/IEC 27001 vs ISO/IEC 42001

Consider them as **Complementary**, not **Competing** in creation of AI Trusted operation

Requirements	ISO 9001:2015	ISO 14001:2015	ISO/IEC 27001:2022	ISO 22301:2019	ISO/IEC 42001:2023
Leadership and commitment	5.1	5.1	5.1	5.1	5.1
Policy	5.2	5.2	5.2	5.2	5.2
Objectives	6.2	6.2	6.2	6.2	6.2
Documented information	7.5	7.5	7.5	7.5	7.5
Internal audit	9.2	9.2	9.2	9.2	9.2
Management review	9.3	9.3	9.3	9.3	9.3
Continual improvement	10.3	10.3	10.1	10.2	10.1

ISO/IEC 27001 vs ISO/IEC 42001

Consider them as **Complementary**, not **Competing** in creation of AI Trusted operation

Information security backbone

ISO/IEC 27001

- Access control
- Asset protection
- Secure operations
- Supplier security
- Audit and improvement

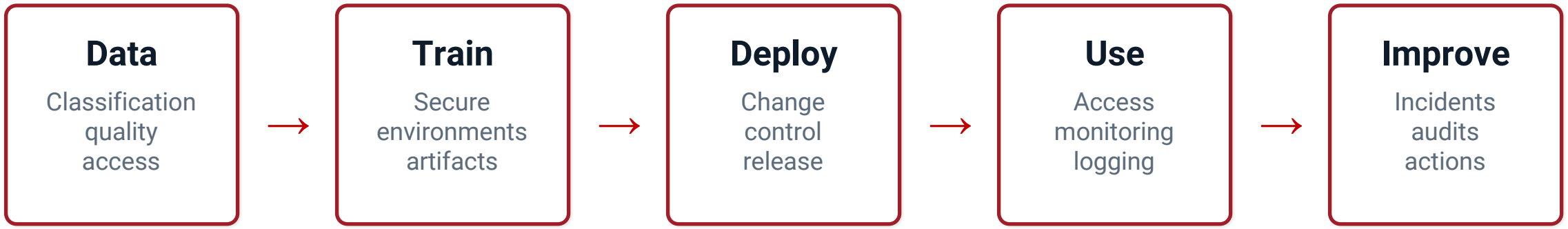
Responsible AI management

ISO 42001

- AI governance
- Use-case oversight
- Impact / risk framing
- Transparency expectations
- Human oversight

Governance & Control Gaps in AI

Identifying blind spots in AI governance structures



Governance | Policy, scope, risk method, responsibilities

Operational security | Identity, access, supplier security, logging, change control

Assurance | Monitoring, internal audit, management review, corrective action

Result: AI systems are governed, secured, and reviewable across the lifecycle.

PECB

Regulatory & Stakeholder Expectations

How do you currently demonstrate transparency or explainability in AI-driven decisions?

NORTH AMERICA
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- California Consumer Privacy Act (CCPA)
- New York State Department of Financial Services Cybersecurity Regulation (23 NYCRR 500)
- Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)
- Personal Information Protection Act (PIPA)

EUROPE
- GDPR
- NIS 2 Directive
- The EU Cybersecurity Act

ASIA
- Cybersecurity Law (China)
- Personal Data Protection Act (Singapore)
- Information Technology Act (India)
- Act on the Protection of Personal Information (Japan)

SOUTH AMERICA
- General Personal Data Protection Act (Brazil)
- Personal Data Protection Law (No. 25,326) (Argentina)
- Peru's Data Protection Law (No. 29733)

AFRICA
- Protection of Personal Information Act (POPIA) (South Africa)
- Cybersecurity and Cybercrime Act 2021(Mauritius)
- Organic Act No. 2004-63 on the Protection of Personal Data (Tunisia)
- Cybersecurity Act, 2020 (Act 1038) (Ghana)
- Data Protection Act, 2019 (Kenya)
- Nigeria Data Protection Regulation (NDPR) 2019

OCEANIA
- The Privacy Act 1988 (Australia)
- Privacy Act 2020 (New Zealand)
- Cybercrime Act 2001 (Fiji)

Practical Alignment & Implementation

What would be your first step in aligning AI governance with your existing security framework?

1. Define and establish	
1.1	Leadership and project approval
1.2	Roles and responsibilities
1.3	The organization and its context
1.4	AIMS scope
1.5	Analysis of the existing system
1.6	AI policy
1.7	AI risk management
1.8	Statement of Applicability

2. Implement and operate	
2.1	Selection and design of controls
2.2	Implementation of controls
2.3	Management of documented information
2.4	Communication
2.5	Competence and awareness
2.6	Management of AI operations

3. Monitor and review	
3.1	Monitoring, measurement, analysis, and evaluation
3.2	Internal audit
3.3	Management review

4. Maintain and improve	
4.1	Treatment of nonconformities
4.2	Continual improvement

THANK YOU

✉ dbejtullahu@bconsulted.al

in https://www.linkedin.com/in/driton-s-bejtullahu-1095333a/