WEBINAR RECORDED

PECB

AI, IoT, and Blockchain: Rethinking Risk Management and Compliance

FEBRUARY 26 03:00 PM CET

Irene Odion
Information Security & Compliance Manager, WorkJam

Carl Carpenter
CEO of Arrakis Consulting

#GlobalLeadingVoices

The Tech Trio - Synergy Explained

A Convergence of Technologies

- **AI (Artificial Intelligence):** Predictive analytics, anomaly detection, faster and automated decision-making.
- **IoT (Internet of Things):** Real-time data collection, physical asset monitoring, expands the attack surface with connected devices that can provide near real time data but also possibly vulnerable.
- **Blockchain:** Immutable, decentralized, and transparent ledger for data integrity.
- **Concept:** Together, they can form a self-optimizing, secure, and intelligent ecosystem. IoT creates the data, Blockchain immutes the data, AI interpret the data

Public

Why This Matters Now

IoT devices are *rapidly* becoming a part of *everything*

Digital transformation is accelerating in more industries and in more technical areas.

Data volume, complexity, and risk are increasing. Convergence of data from IoT (data), AI (intelligence), and Blockchain (immutable trust) is a force multiplier for more modern, complex, and distributed environments.

With the increase in potential data volume and complexity, increasingly difficult to analyze quickly and accurately

New threats and more demanding and changing regulations: GDPR, CCPA, ISO 42001, NIST, CMMC

Public

How They Work Together

- IoT → Generates data
- AI → Interprets and acts
- Blockchain → Records and verifies

- Together they create:
  - Automated ecosystems
  - Real-time intelligence
  - Distributed trust

  …But also introduce systemic interdependence.

Public

Contradictions Between Them

- Transparency vs Privacy
  - *Blockchain openness vs data minimization*

- Automation vs Accountability
  - *AI decisions vs human responsibility*

- Immutability vs Right to Erasure
  - *Permanent records vs privacy laws*

- Speed vs Oversight
  - *Millisecond execution vs governance review cycles*

These are governance dilemmas — not technical glitches.

Opportunities Created by Convergence

- Predictive risk detection
- Automated compliance checks
- Transparent audit trails
- Faster operational decisions
- Reduced fraud

Shift from reactive response to proactive mitigation.

Rethinking Risk Management (AI + IoT)

Proactive & Predictive Insights

Use Case: Predictive Maintenance (e.g., detecting machine failures via IoT sensors + AI analysis). Manufacturing plants will have heavy use of IoT.

Real-time Anomaly Detection and Response: Identifying irregular patterns in data streams instantly with automated response when possible.

Shift: From reactive "after-the-fact" to proactive "pre-event" mitigation.

Security & Risks - AI

- Algorithmic bias
- Lack of explainability
- Model drift
- Data poisoning
- Overreliance on automation
- Shadow AI in the organization

- AI risk = Decision risk at scale

Security & Risks – IoT & Blockchain

IoT Risks:

- Massive attack surface
- Weak device authentication / protection
- Supply chain exposure

Blockchain Risks:

- Smart contract flaws
- Governance ambiguity
- Irreversible errors

IoT expands exposure.
Blockchain makes errors permanent.

Public

Best practices & Solutions

Ensuring legacy concepts are still applied (micro-segmentation, etc.…)

Unified policies for AI, IoT, Blockchain

Continual risk assessments & penetration testing (most environments require annual, consider monthly)

Training & awareness

Use of managed security services

What Rethinking Risk & Compliance Looks Like

Traditional Model → Integrated Model

- Periodic audits → **Continuous monitoring**
- Siloed controls → **Ecosystem governance**
- Human-only review → **Human + machine oversight**
- Reactive compliance → **Predictive compliance**

Governance must become:

- Continuous
- Technology-aware
- Integrated across ecosystems.

Aligned with **ISO 31000** (Enterprise Risk Integration), **ISO/IEC 27001** (Expanded Security Scope), **ISO/IEC 42001** (AI Governance Accountability) principles. For IoT / OT, alignment with **IEC 62443. An integrated and comprehensive governance model is critical.**

Benefits of the Integrated Approach

Enhanced Security & Data Integrity: Tamper-proof data.

Improved Transparency & Trust: Verifiable systems.

Operational Efficiency: Reduced fraud and manual work.

Better Risk Management: Predictive algorithms identify disruptions early.

Strategic Roadmap for Implementation

Start Small: Pilot in high-impact areas.

Data Governance: Ensure clean, standardized data from IoT sensors.

Hybrid Models: Combine on-chain security with off-chain efficiency.

Human-in-the-Loop: Balance automation with human oversight.

Public

Trust is the Real Outcome

When governed correctly:

- AI → Trusted decisions
- IoT → Reliable visibility
- Blockchain → Verifiable integrity

The ultimate competitive advantage is trust.

Organizations that govern these technologies effectively will not just reduce risk; they will create trust.

Q&A

THANK YOU

✉ carl@arrakisconsulting.com in https://www.linkedin.com/in/carlatarrakis/

✉ ireneodion@protonmail.com in https://www.linkedin.com/in/renee-odion/