WEBINAR RECORDED

PECB

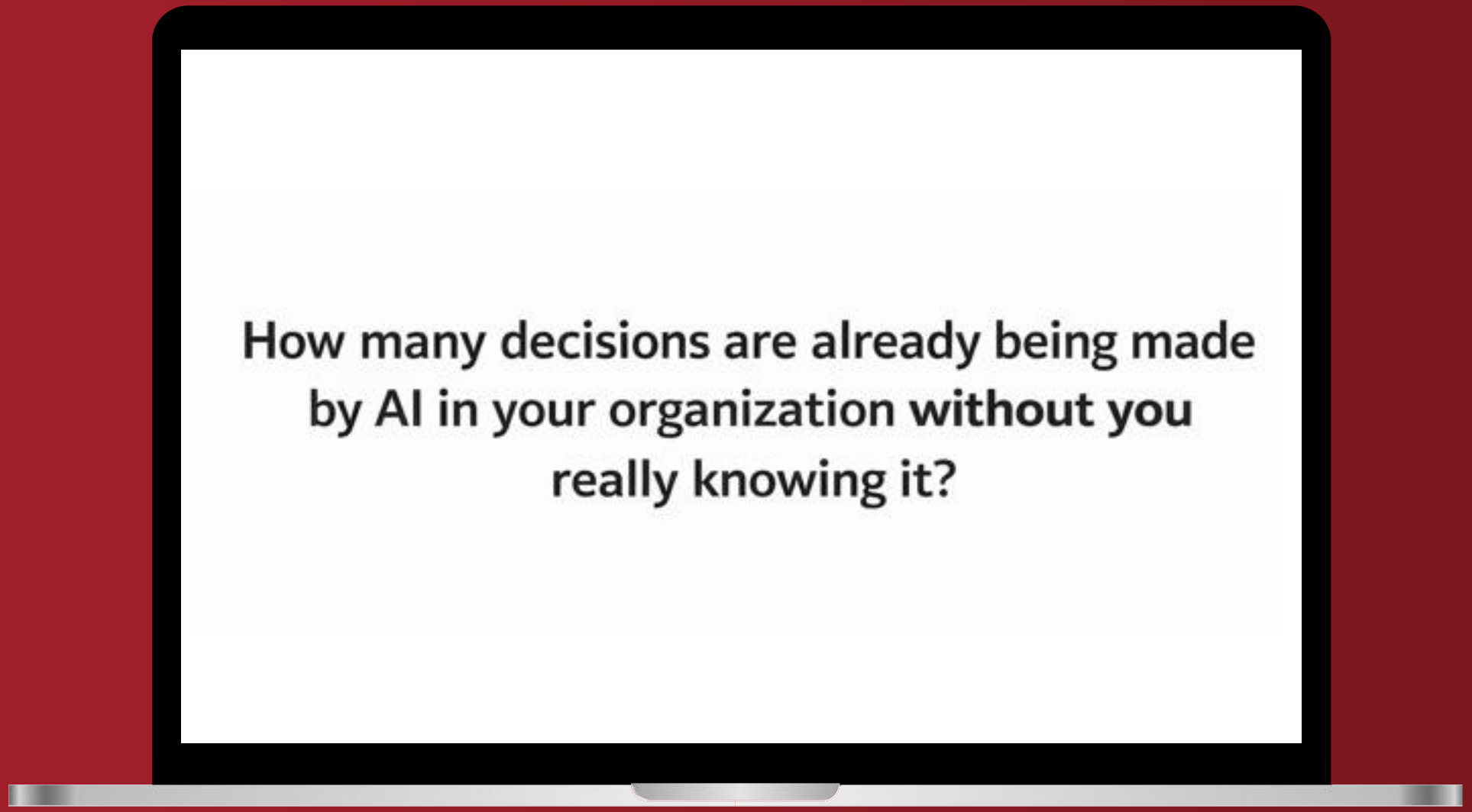
AI and Cybersecurity in 2026: What Auditors, Implementers, and Organizations Must Prepare For

JANUARY 29 | 03:00 PM CET

Bassem Lamouchi

Cybersecurity and Cloud Strategist

#GlobalLeadingVoices


How many decisions are already being made by AI in your organization without you really knowing it?

Agenda

- What has fundamentally changed with AI
- Why organizations are not prepared today
- Why 2026 is a turning point (regulation & standards)
- What auditors, implementers, and organizations must prepare for
- Practical roadmap and key takeaways

PECB

Meet the Speaker

Exp. Bassem LAMOUCHI

- Cybersecurity and Cloud Strategist
- Expert in AI security, governance, and risk management
- Lead Auditor and international trainer (ISO 27001, ISO 42001, Pentesting and Ethical Hacking)
- Specialist in AI audits and secure AI implementations
- Advisor to organizations on regulatory and cyber resilience readiness

Contact :

- b.lamouchi@tunisiancloud.com
- /in/bassemlamouchi

PECB

Reality Check

- Artificial Intelligence is no longer experimental.

- It is already involved in:
  - Recruitment and candidate screening
  - Credit and risk scoring
  - Monitoring and anomaly detection
  - Recommendations and prioritization
  - Automated approvals and denials

- Most of these decisions happen quietly.

From Tools to Decision-Makers

- In the past, technology supported human decisions.
- Today, AI increasingly **makes** decisions.

- Humans often:
  - configure the system,
  - provide the data,
  - but no longer review every outcome.

- This is a fundamental shift.

What Makes AI Fundamentally Different

- AI systems are:
  - Fast and scalable
  - Partially autonomous
  - Continuously learning
  - Sometimes opaque or non-explainable

- Traditional control models were not designed for this.

Who Is Really in Control?

- Control is no longer only about:
  - users,
  - procedures,
  - approvals.

- Control now depends on:
  - data quality
  - model design
  - training processes
  - external vendors and platforms

- Responsibility becomes blurred.

A New Category of Risk

- AI introduces risks that are:
  - Non-intentional
  - Systemic
  - Difficult to detect
  - Capable of scaling instantly

- These risks do not behave like traditional IT risks.

The Illusion of Readiness

- Many organizations believe they are prepared because they have:
  - security policies
  - IT controls
  - risk registers
  - compliance programs

- But most of these were designed **before AI decisions existed**.

The Blind Spots

- Common gaps observed today:
  - No inventory of AI systems
  - No clear AI ownership
  - No defined accountability
  - Limited traceability of decisions
  - Weak or no AI governance framework

Traditional Audits vs AI Reality

- Audits are often:
  - Periodic
  - Static
  - Evidence-based on documentation
- AI systems are:
  - Dynamic
  - Continuously evolving
  - Influenced by data and behavior
- This creates a structural mismatch.

Silent Exposure

- Organizations may already be exposed to:
  - Legal and regulatory liability
  - Ethical and reputational risks
  - Biased or unfair decisions
  - Loss of trust and transparency
- Often without realizing it.

Real Case – Anonymized

- AI decisions not documented
- No clear ownership
- Issue detected during audit
- Regulatory and reputational impact

Why 2026 Is a Turning Point

- 2026 is not about predictions.
- It is about:
  - regulatory enforcement,
  - maturing standards,
  - increased audit expectations.
- The tolerance for ungoverned AI will decrease significantly.

Regulatory Acceleration

- Globally, regulations are converging on:
  - accountability
  - transparency
  - risk-based AI management
  - documented governance

- Organizations will be expected to **prove control**, not intentions.

Standards Are Catching Up

- Management system standards are evolving to address:
  - emerging risks
  - governance and oversight
  - decision accountability
  - evidence-based assurance
- Audits will increasingly include AI-related controls.

New AI Requirements & Standards

Emerging AI Requirements

- These are not future requirements — they are today's audit criteria.
  - Risk-based AI governance
  - Accountability for AI decisions
  - Documentation & traceability
  - Human oversight
  - Continuous monitoring

- If an organization cannot demonstrate these five elements, it will not pass an AI audit in 2026.

What Will No Longer Be Acceptable

- After 2026, the following will not be sufficient:
  - “We didn’t know AI was used”
  - “The vendor is responsible”
  - “It’s automated, not our decision”

- Responsibility remains with the organization.

What Auditors Must Prepare For

- Auditors will need to:
  - Understand AI-driven processes
  - Ask new types of questions
  - Evaluate governance, not just controls
  - Assess accountability and traceability

- Auditing AI is auditing decision systems.

What Implementers Must Prepare For

- Implementers must design AI with:
  - governance by design
  - traceability by default
  - explainability where possible
  - auditable decision paths

- Technical excellence alone is no longer enough.

What Organizations Must Prepare For

- Organizations must accept that:
  - accountability cannot be delegated
  - AI decisions are business decisions
  - risk ownership stays at the top
- Leadership involvement is mandatory.

A Shared Responsibility Model

- Effective AI governance requires collaboration between:
  - IT and data teams
  - Risk and compliance
  - Legal and ethics
  - Executive management

- AI governance is not a silo.

The Real Challenge

- The main challenge is not technology.
- It is:
  - governance maturity
  - decision transparency
  - organizational culture
  - leadership awareness

- AI exposes governance weaknesses.

A Practical Roadmap

Step 1: Identify AI Usage

- Where is AI used?
- For which decisions?
- Internal systems
- External tools & vendors
- AI inventory

A Practical Roadmap

Step 2: Govern

- Roles & responsibilities
- Decision rules
- Risk criteria & limits
- Approval processes
- Governance framework

A Practical Roadmap

Step 3: Audit & Improve

- Regular AI audits
- Control effectiveness
- Risk reassessment
- Traceability & evidence
- Continuous improvement

Key Takeaways

- AI is already making decisions
- Most organizations are not fully prepared
- 2026 will change expectations
- Governance is central to AI trust
- Preparation must start now

Final Message

- The question is no longer:
  - **“Will AI impact audits and governance?”**

- The real question is:
  - **“Are we ready to take responsibility for AI decisions?”**

THANK YOU

✉ b.lamouchi@tunisiancloud.com

in bassemlamouchi