

Regional Webinar

AI in Information Security Enhancing Risk Management and Business Continuity

PECB REGIONAL WEBINARS

Agenda

- Introduction
- AI Shaping the Threat Landscape
- Leveraging AI to enhance Information Security
- Leveraging AI to enhance Risk Management and Business Continuity
- Future Outlook & Way Forward

Introduction

- Presented by: **Mohammed Abdul-Fatawu**
- Business Continuity Partner-Operations by Day & Management Systems Enthusiast 24/7
- Senior Lead Auditor ISO-IEC 27001, 2230, 9001,45001,42001,14001etc.
- Certified Artificial Intelligence Professional-CAIP, NIST Cybersecurity Consultant etc.

AI in Information Security

AI Shaping the Threat Landscape

AI Trends & Their Implications

Leaderships Confidence in AI's Potential

87%

Understanding of GenAI benefits

45%

AI provides a competitive edge

Regulatory and Data Challenge

57%

Uncertainty over regulation

17%

Confidence in data readiness

Cybersecurity Concerns

10%

Confidence in existing cybersecurity measures

60%

Willingness to increase cybersecurity investment



Africa CEO Outlook Report 2024

Information Security is Evolving

The reality: AI serves as both defensive shield and offensive weapon in cybercriminals' arsenals.

The threat landscape grows more sophisticated, faster-moving, and increasingly unpredictable through AI-powered attacks that challenge traditional security models.

Weaponisation for Scale and Sophistication

Technical Barrier Reduction

AI democratises complex attack techniques, enabling less skilled actors to execute sophisticated campaigns

Volume Amplification

Automated reconnaissance and vulnerability exploitation increase attack frequency exponentially

Complexity Enhancement

Multi-vector attacks coordinate seamlessly across different systems and entry points

Hyper-Realistic Social Engineering

Personalised Phishing

Generative AI crafts grammatically perfect, contextually relevant spear-phishing messages that bypass traditional filters and deceive trained employees.

Deepfake Deception

Convincing audio and video impersonations of senior executives manipulate employees into unauthorised actions like wire transfers.

Adaptive Malware

Polymorphic malware adapts code in real-time, evading signature-based detection and traditional antivirus solutions.



AI in Information Security

Leveraging AI to Enhance Information Security

AI in Information Security Trends

- Shadow AI
- AI-enhanced attacks
- Use of Local Models
- AI-Enhanced Security Solutions

AI as the Defensive Force Multiplier

Artificial intelligence transforms defensive capabilities, providing organizations with smarter, faster tools to combat evolving threats.

Enhanced Detection Speed

AI processes massive data volumes in real-time, identifying threats human analysts might miss

Predictive Threat Intelligence

Machine learning models anticipate attack patterns before they fully materialise

AI-Powered Security Capabilities

Capability	AI Mechanism	Business Impact
Threat Detection	ML analysis of network traffic and user behavior patterns	• Automated anomaly flagging reduces alert fatigue
Phishing Prevention	NLP analysis of email content and metadata	Blocks sophisticated spear-phishing before inbox delivery
Insider Threat Monitoring	UEBA profiling of employee behaviour baselines	Flags unusual access patterns outside normal working hours
Vulnerability Management	Predictive analytics and attack simulation	Proactive patching prevents lateral movement attacks

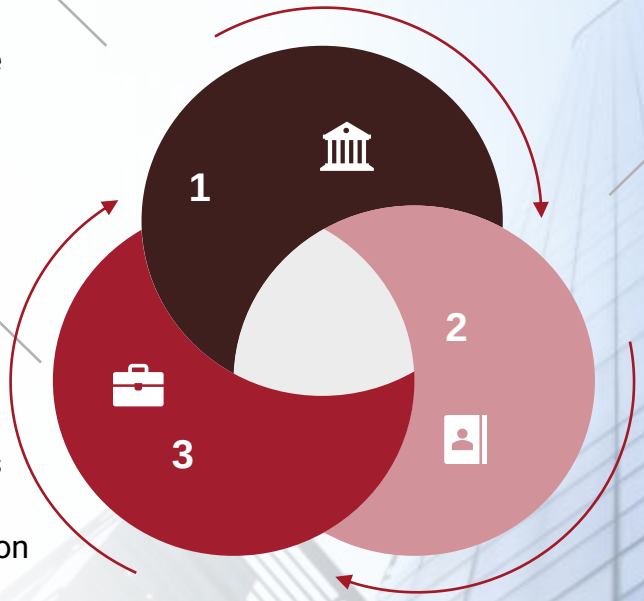
AI Supporting Compliance Frameworks

ISO/IEC 27001 Monitoring

AI-driven systems provide real-time evidence logs, constantly checking configurations against security standards for consistent control enforcement.

GDPR Compliance

Automated PII classification ensures data processing aligns with privacy regulations whilst monitoring retention and access rights.



Dynamic Risk Assessment

AI maps threats to business assets automatically, transforming risk management from periodic to a continuous process.

AI in Information Security

Leveraging AI to Enhance Risk Management and Business Continuity

Strengthening Risk Management Through AI

1

Business Impact Mapping

Links security events to critical revenue-generating systems for prioritised risk mitigation

2

Predictive Analytics

Forecasts attack likelihood using threat intelligence, enabling proactive defense strategies

3

Adaptive Security Posture

Self-evolving systems learn from blocked attacks, continuously refining detection models

Leveraging the NIST AI Risk Management Framework

A voluntary framework that provides a structured approach to building trustworthy AI systems—emphasizing transparency, accountability, and human-centric outcomes throughout the entire lifecycle.

Core Purpose and Objectives

Identify and Manage Risks

Recognize and address risks to individuals, organisations, and society from AI systems throughout their deployment.

Promote Trustworthy AI

Support the design, development, and use of responsible AI that stakeholders can rely upon and trust.

Enable Robust Governance

Establish comprehensive governance, risk assessment, and continuous monitoring processes for AI systems.

NIST AI Risk Management Framework Cont'

The Framework is built around four major functions, with key characteristics that apply across all of them.

The Core

The four major functions

- Govern, Map, Measure, and Manage
- This provides a continuous risk management cycle that guides organisations through systematic AI oversight.

Characteristics

Valid & Reliable

Performs consistently as intended across diverse conditions

Safe

Minimises physical and psychological harm

Secure & Resilient

Withstands attacks, recovers from failures

Accountable & Transparent

Decisions are auditable and understandable

Explainable

Outcomes comprehensible to users and stakeholders

Privacy-Enhanced

Protects sensitive data ar upholds rights

Fair

Reduces bias, ensures equitable outcomes

AI-Enhanced Business Continuity Management

Scenario Simulation

AI simulates complex disaster scenarios, identifying cascading failures and interdependencies that human planners might overlook.

Automated Recovery

AI-driven orchestration isolates affected systems, triggers failovers, and accelerates data recovery, dramatically reducing MTTR.

Crisis Communication

Natural language generation tools draft incident reports and stakeholder communications, ensuring consistency during critical first hours.

Key Takeaways for Security Leaders

Embrace the Dual Nature

AI amplifies both threats and defences—successful organisations leverage its defensive capabilities whilst preparing for AI-powered attacks.

Integrate Strategically

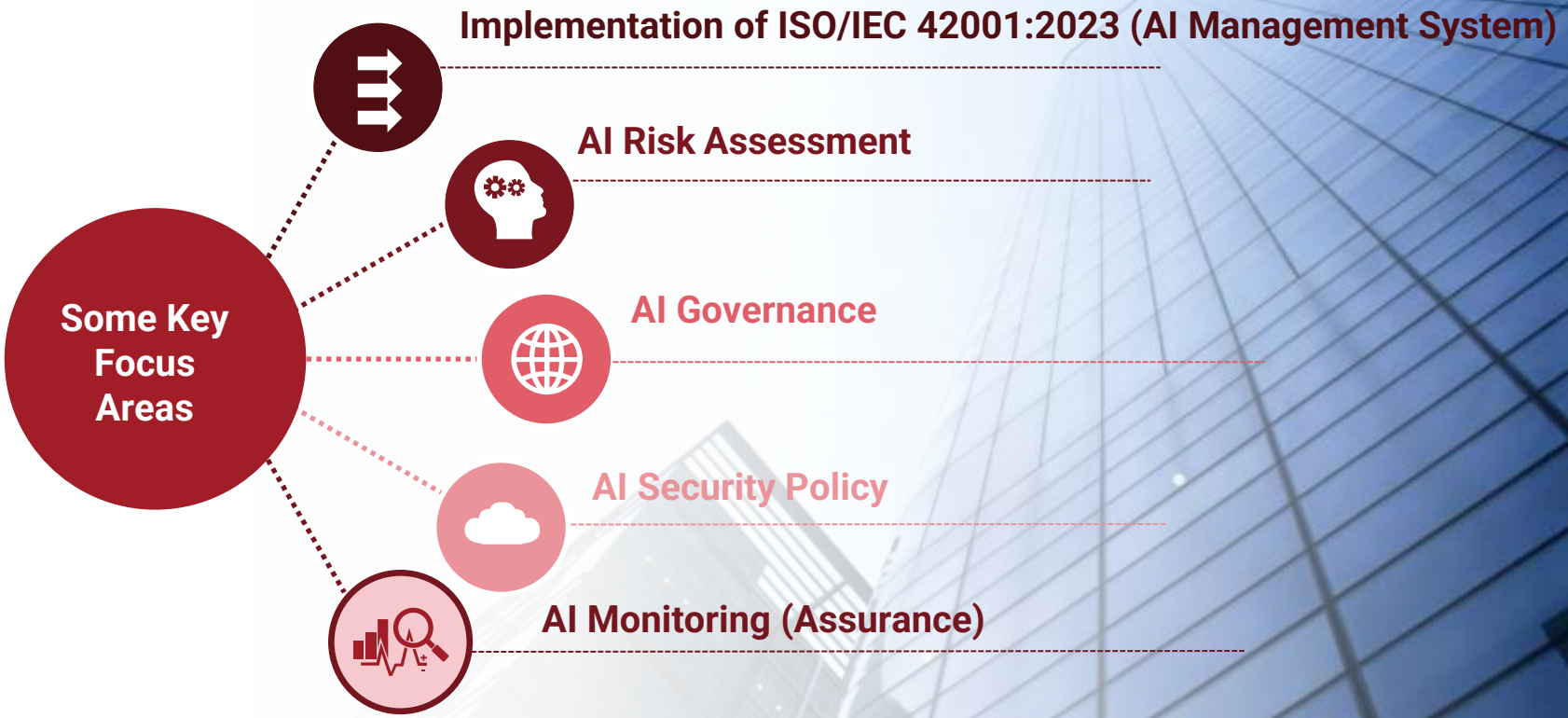
Deploy AI across threat detection, compliance monitoring, and business continuity for comprehensive resilience.

Evolve Continuously

Adaptive AI systems require ongoing refinement and human oversight to maintain effectiveness against emerging threats.

Future Outlook & Way Forward

Way Forward


Some Key Focus Areas
Implementation of ISO/IEC 42001:2023 (AI Management System)
AI Risk Assessment
AI Governance
AI Security Policy
AI Monitoring (Assurance)

Q&A Session



Contact Information

- PECB Trainer Profile: https://pecb.com/en/trainer/info/5424
- LinkedIn: www.linkedin.com/in/abdul-fatawu-mohammed
  Phone: +233246625517
- Email: continuitylinksest2023@outlook.com

For any questions or comments, please contact us using the email below

- support@pecb.com