Wednesday 10 July 2024

CURIA RATIONUM

EUROPEAN
COURT
OF AUDITORS

AI risks and audit

Ioannis Hartoutsios
Head of Task for IT audit
DATA team

AI risks and audit

- AI @ ECA
- The ECA's IT audit approach
- Impact of AI in our IT audit work
- A proposed GRC toolkit for AI by ISACA

AI @ ECA

- Goal 1 – Improve operational efficiency in audit through AI tools

- Goal 2 – *Build the ECA's ability to audit AI-based projects, systems and processes*

- Goal 3 – Add value and contribute to EU-wide and international discussions on AI

EUROPEAN COURT OF AUDITORS

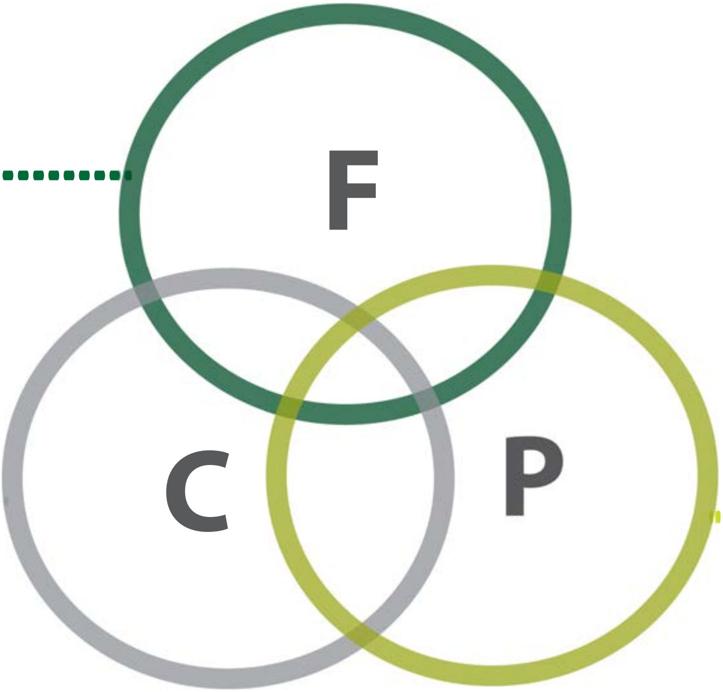
EN

Artificial Intelligence initial strategy and deployment roadmap

2024-2025

Source: ECA website - Artificial Intelligence initial strategy and deployment roadmap (europa.eu)

The ECA's IT audit approach



Financial Audit

IT controls over financial reporting systems

Compliance Audit (IS)

Compliance of IT systems with laws, regulations, rules, policies, standards and guidelines

Performance Audit (IS)

Related to sound financial management

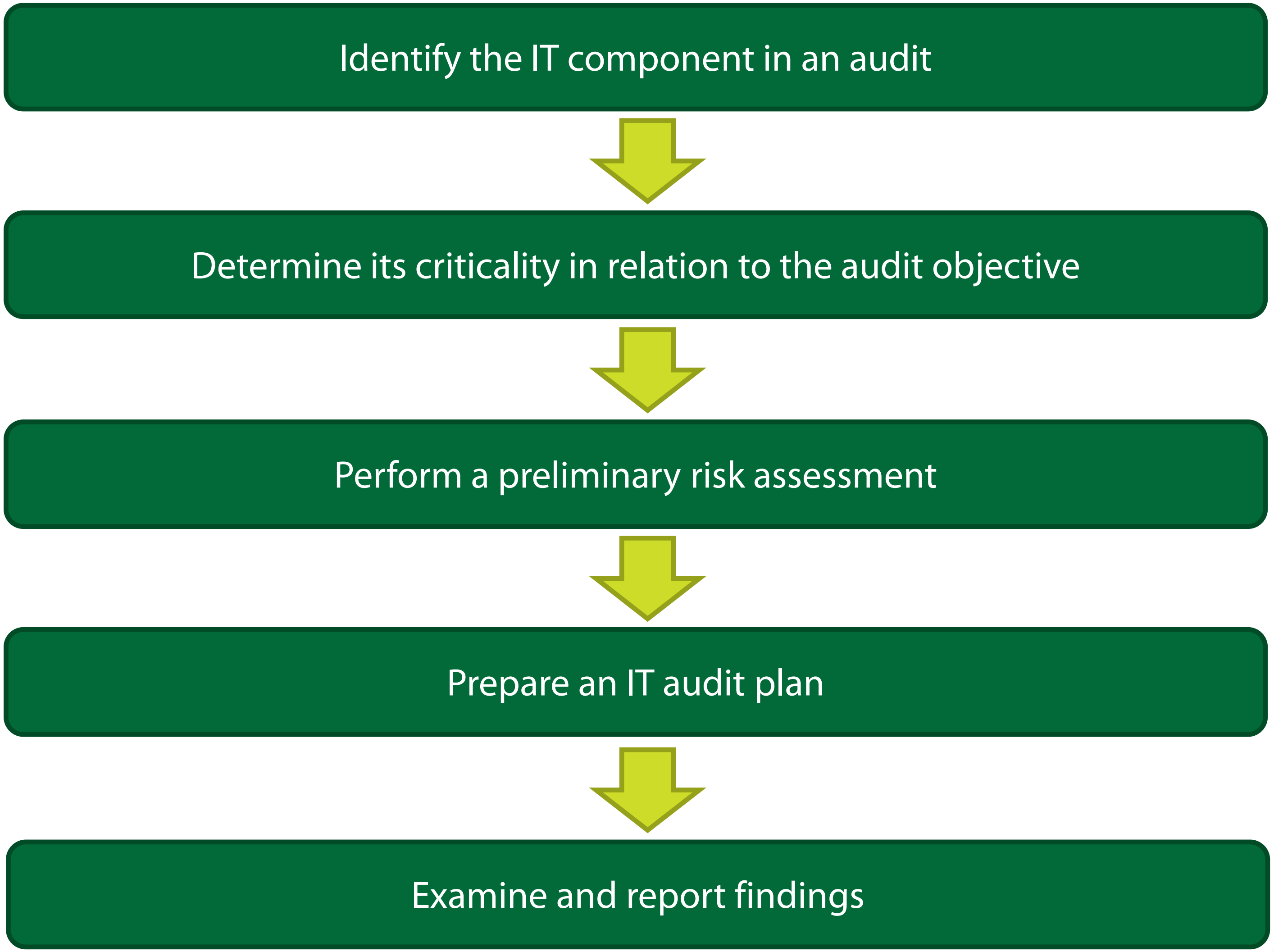
Economy, Efficiency and Effectiveness

Information system specific

Cross-cutting topics related to technology

Data reliability assessments

The ECA’s IT audit approach



Identify the IT component in an audit

Determine its criticality in relation to the audit objective

Perform a preliminary risk assessment

Prepare an IT audit plan

Examine and report findings

How AI impacts IT audit work at the ECA

- What would be the scope / timing of an AI audit?
  - Diverse definitions of AI lead to different understanding of AI audit
- Identifying the AI component
  - Increased use of AI technologies by our auditees
    - AI services fully operational or under study/development
    - Use AI components
  - AI governance by our auditees is useful (classification)
  - Challenge to train auditors to:
    - Identify AI components / services
    - Identify AI risks related to the audit area

How AI impacts IT audit work at the ECA

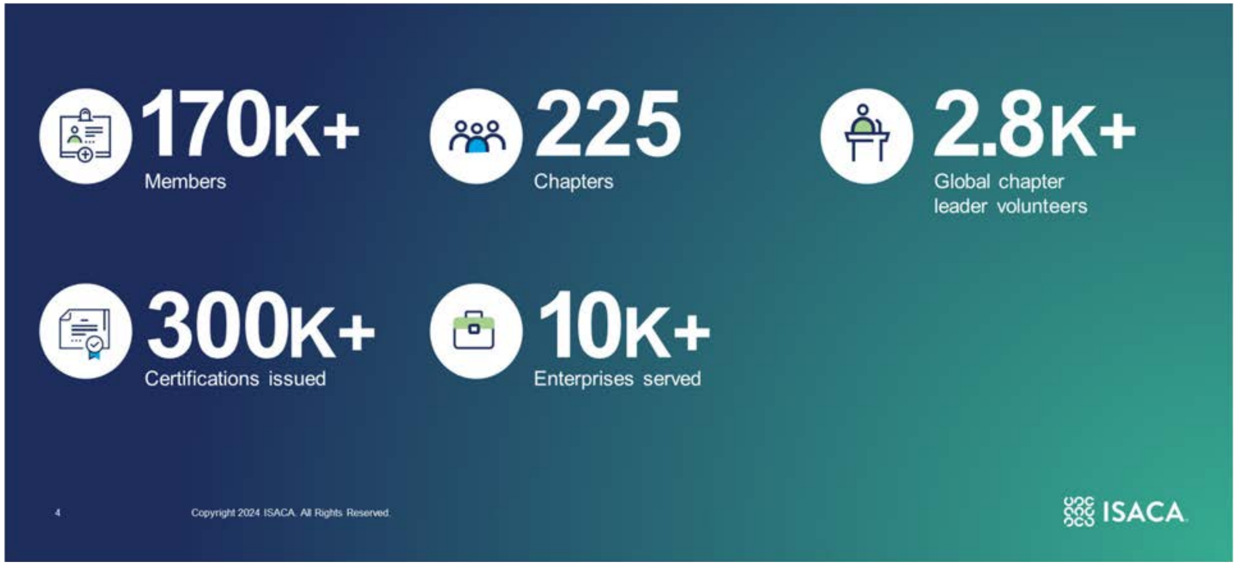
- Assessing elements of risk for AI systems
  - Emerging nature
    - Early adoption / Managing innovation
  - Software development risks
    - Agile approaches / AI service providers
  - Ethical risks
    - Biases / Discrimination / Privacy / Transparency
  - Technical risks
    - Complexity / Security / Data protection
  - Compliance risks
    - EU AI Act / GDPR / Internal AI policies
  - Business process risks
    - Traceability / Accountability/ Explicability (rules?)

How AI impacts IT audit work at the ECA

- Identifying IT audit criteria
  - ISO standards
    - 50+ standards published or under development
    - ISO/IEC 42001:2023 – AI management system
    - ISO/IEC 23894:2023 – AI Guidance on risk management
  - NIST
    - AI Risk Management Framework
  - OWASP
    - AI security overview, AI Top risks-LLM, AI Top 10 risks –ML
  - CRISP-DM for AI development
  - Industry specific AI frameworks (i.e. beyond the AI Act?)
  - ISACA AI resources (COBIT)

ISACA and AI

- ISACA is a global non-profit professional association



170K+
Members

225
Chapters

2.8K+
Global chapter leader volunteers

300K+
Certifications issued

10K+
Enterprises served

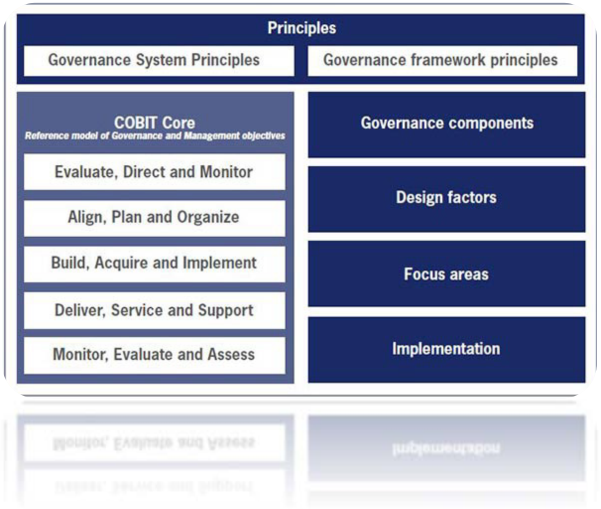
4

ISACA

- ISACA Luxembourg Chapter
  - AI working group
  - AI experts and IT auditors
  - Academia, Financial services, Audit, Consulting, Security, Public sector

IT loves frameworks but AI calls for changes

IT Framework (e.g., COBIT)



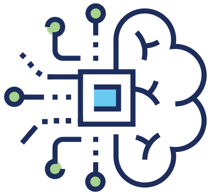
Principles

- Governance System Principles
- Governance framework principles

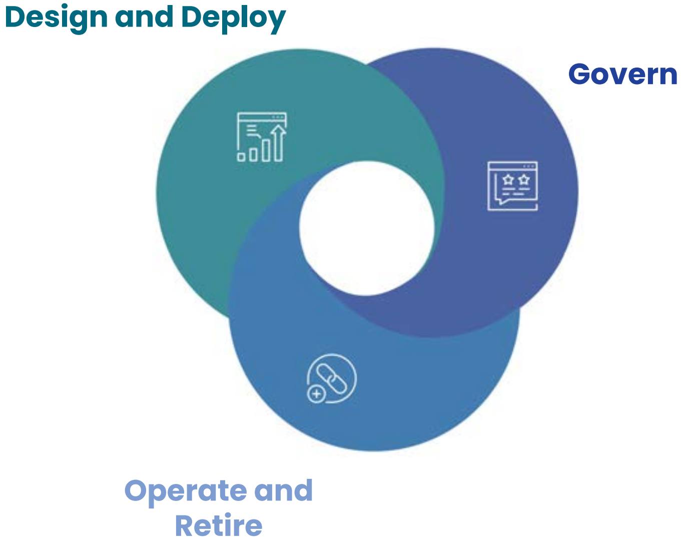
COBIT Core
Reference model of Governance and Management objectives

- Evaluate, Direct and Monitor
- Align, Plan and Organize
- Build, Acquire and Implement
- Deliver, Service and Support
- Monitor, Evaluate and Assess

- Governance components
- Design factors
- Focus areas
- Implementation



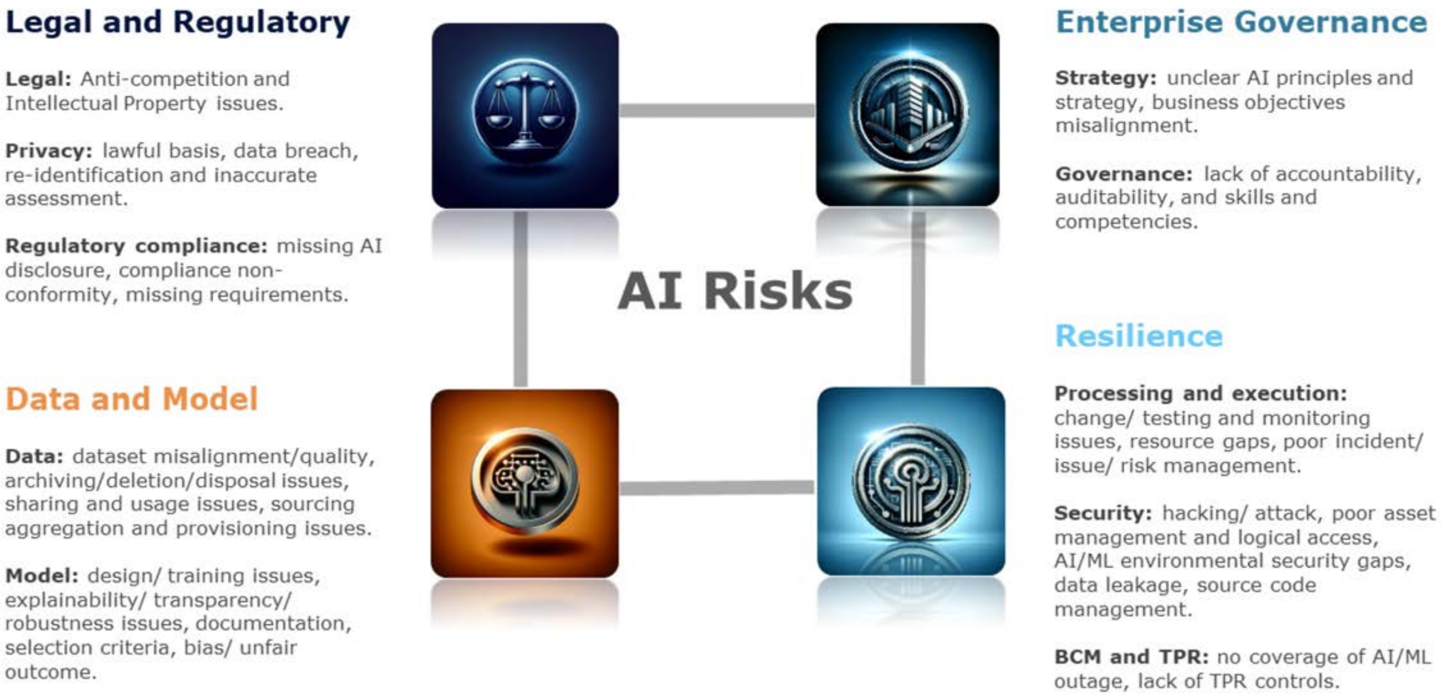
AI customized framework(s)



AI system lifecycle

A Governance Risk and Compliance (GRC) toolkit for AI

- Provides professionals with essential knowledge to govern, control and assess AI
- Assesses operational effectiveness of AI and associated processes and activities
- Addresses a comprehensive set of AI risks



Legal and Regulatory

Legal: Anti-competition and Intellectual Property issues.

Privacy: lawful basis, data breach, re-identification and inaccurate assessment.

Regulatory compliance: missing AI disclosure, compliance non-conformity, missing requirements.

Data and Model

Data: dataset misalignment/quality, archiving/deletion/disposal issues, sharing and usage issues, sourcing aggregation and provisioning issues.

Model: design/ training issues, explainability/ transparency/ robustness issues, documentation, selection criteria, bias/ unfair outcome.

Enterprise Governance

Strategy: unclear AI principles and strategy, business objectives misalignment.

Governance: lack of accountability, auditability, and skills and competencies.

Resilience

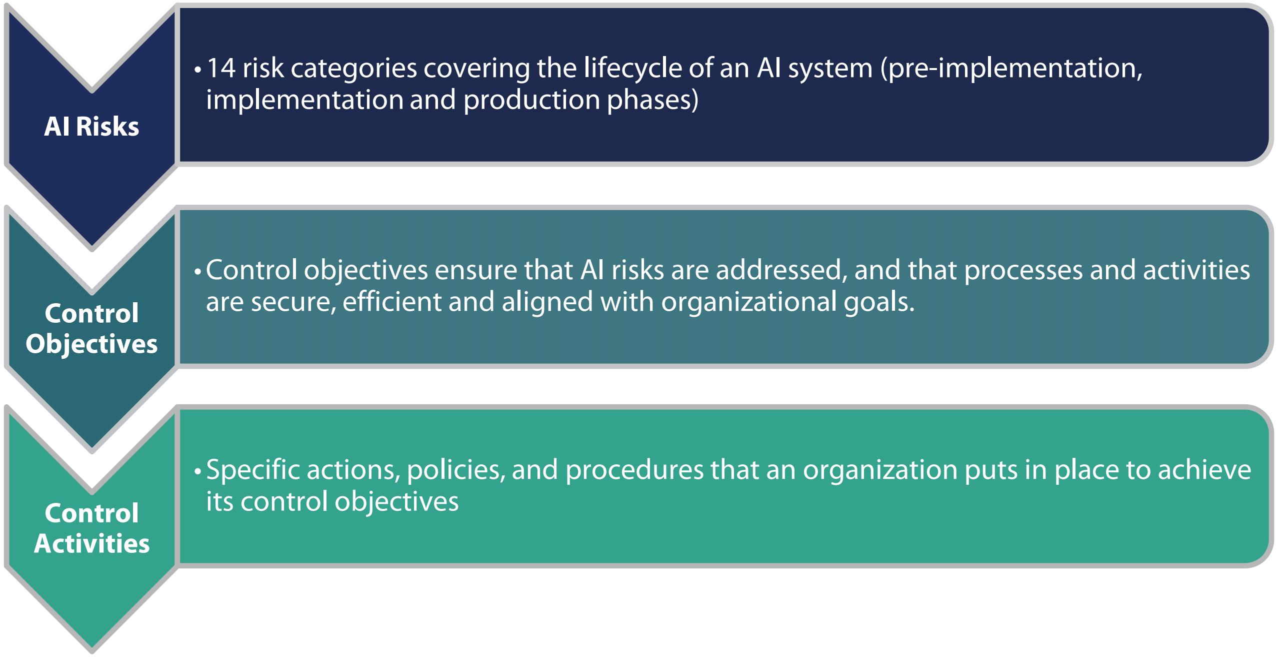
Processing and execution: change/ testing and monitoring issues, resource gaps, poor incident/ issue/ risk management.

Security: hacking/ attack, poor asset management and logical access, AI/ML environmental security gaps, data leakage, source code management.

BCM and TPR: no coverage of AI/ML outage, lack of TPR controls.

Structured around AI risks

- Control activities are mapped to AI risks
- Guidance on how to assess control activities



AI Risks

- 14 risk categories covering the lifecycle of an AI system (pre-implementation, implementation and production phases)

Control Objectives

- Control objectives ensure that AI risks are addressed, and that processes and activities are secure, efficient and aligned with organizational goals.

Control Activities

- Specific actions, policies, and procedures that an organization puts in place to achieve its control objectives

36

Individual AI related Risks

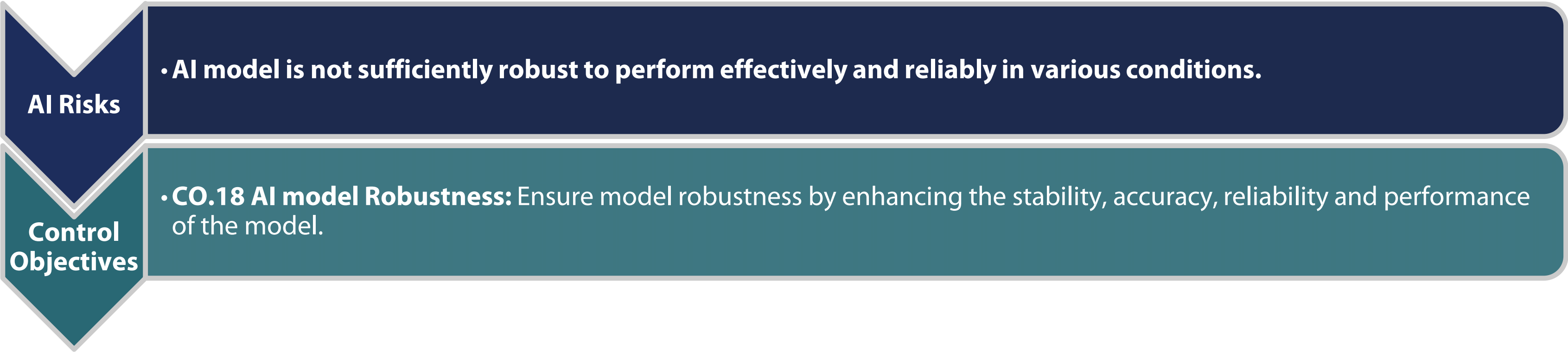
41

Control Objectives for AI

133

Control Activities for AI

An example



AI Risks

- AI model is not sufficiently robust to perform effectively and reliably in various conditions.

Control Objectives

- **CO.18 AI model Robustness:** Ensure model robustness by enhancing the stability, accuracy, reliability and performance of the model.

Control Activities

C.01 Define clear AI model robustness requirements.

C.02 Test Scenarios are built according to possible threats to the quality and security of the model.

C.03 Suitable test tools are used to assess model robustness requirements.

C.04 Robustness test results are available and well documented, with a sufficient level of detail.

C.05 For high-risk AI systems, an independent third-party review of the system robustness is commissioned and performed.

C.06 Mitigation strategies are planned in case robustness issues are identified

Assessing control activities(example)

Control Activities

- C.03 Suitable test tools are used to assess model robustness requirements

Audit Procedures to test the control activities	**1.** Inquire with the relevant stakeholders and determine whether manual or automated robustness tests exist.
	a. For manual tests, assess the qualifications of the test performers and whether their workload is appropriate to ensure a proper quality of the tests.
	b. For automated tests, determine whether they are developed in house or externally and how often they are updated with newest robustness test techniques.
	2. Review the testing procedures/ plans and assess if they cover all the defined test scenarios.
	3. Obtain and review the last sets of robustness tests performed to ensure that the tests are regularly executed.
	4. Observe how the robustness tests are performed and assess their adequacy in terms of coverage and completeness of documentation.
	5. Reperform the tests using different tools to confirm that similar / uniform test result are obtained.

Future work on auditing AI

- ISACA
    - AI GRC toolkit version 1.0 is available to all ISACA Luxembourg Chapter members
    - Future work
        - Enrich (control activities, testing procedures and tools)
        - Align with ISO standards and EU AI Act requirements

Contact details

Ioannis Hartoutsios

Head of Task for IT Audit

DATA team

ioannis.hartoutsios@eca.europa.eu

Want to know more about ECAs work:

Website: **https://www.eca.europa.eu/**

Twitter **@EUAuditors**

LinkedIn: linkedin.com/company/euauditors

Videos on YouTube: **EUAuditorsECA**

CURIA RATIONUM

EUROPEAN COURT
OF AUDITORS