ISACA

Artificial Intelligence Audit and Risk Management Toolkit

by ISACA Luxembourg AI Working Group

Catalin Tiganila

Monday, June 10, 2024

Agenda

About ISACA

Why the need for enhanced protection and control?

Risk Management Solution

We are a **global learning community**

ISACA by the Numbers

Global Non-Profit Professional Association for Individuals and Enterprises

170K+
Members

225
Chapters

2.8K+
Global chapter leader volunteers

300K+
Certifications issued

10K+
Enterprises served

In Pursuit of Digital Trust

Assurance

Security

Risk

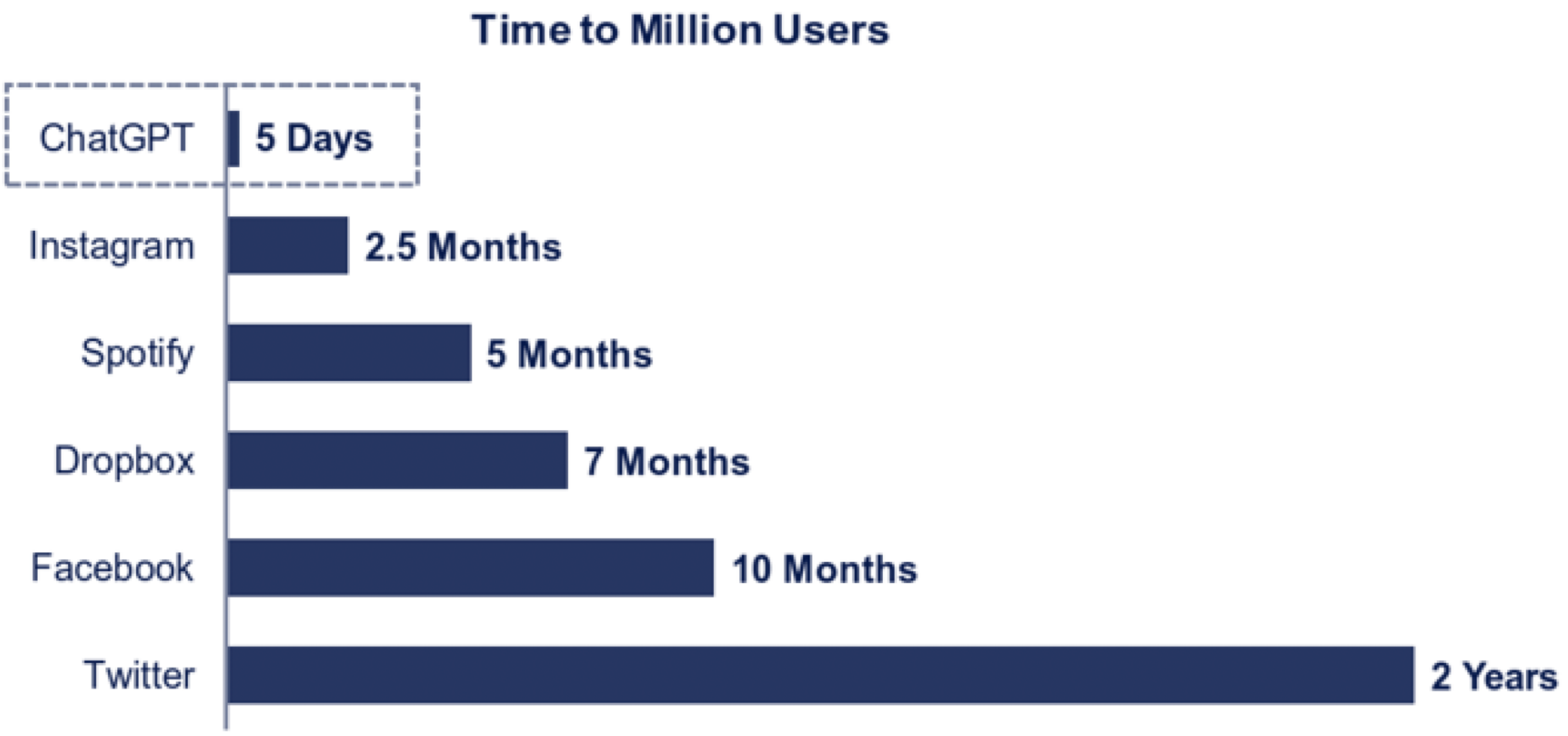
Governance

Quality

Privacy

Why the need for enhanced protection and control?

Why is there a need for AI control frameworks?



Source: Statista

Why there is a need for AI control framework(s)?

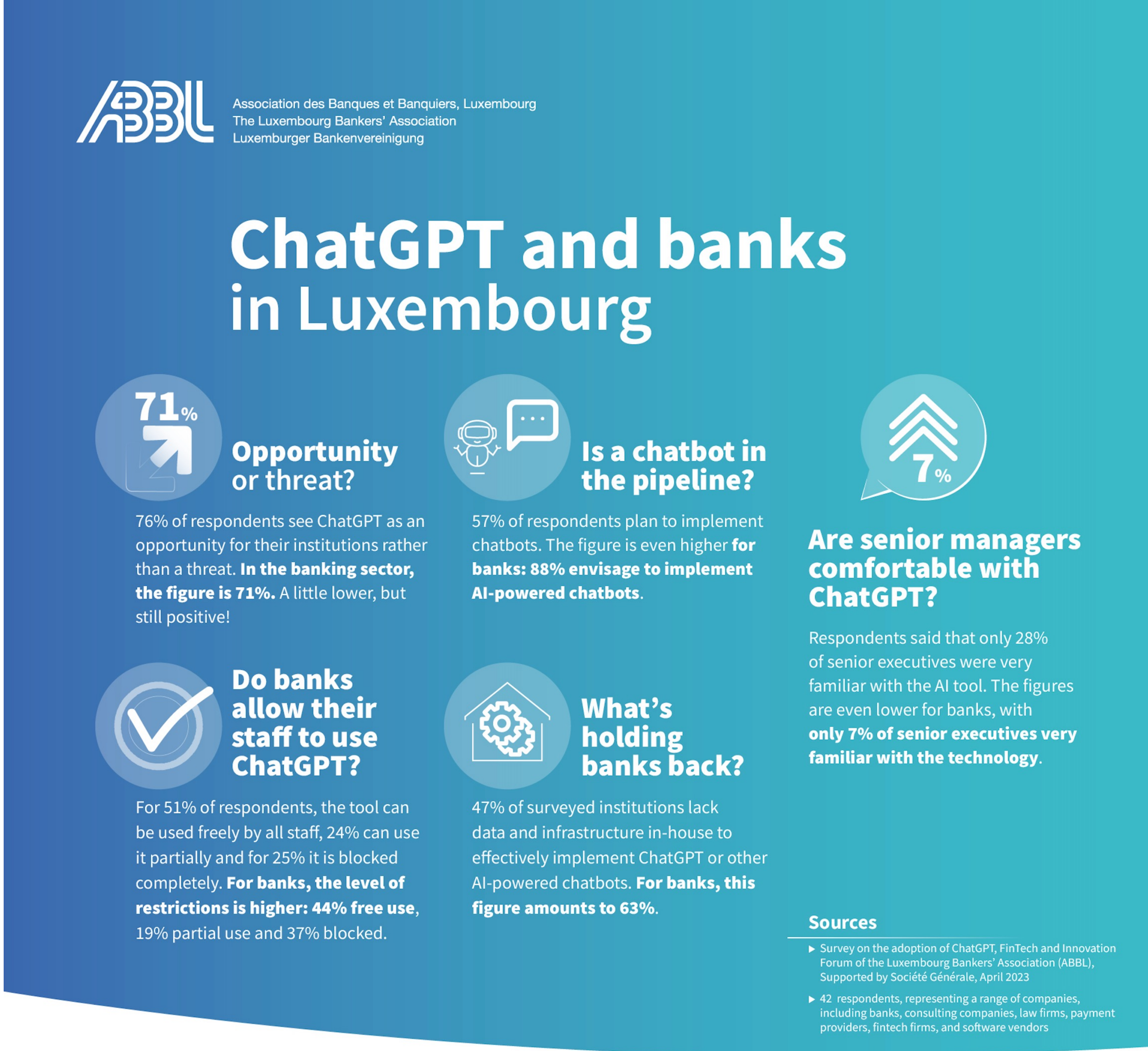
- 76% see ChatGPT as an opportunity

- 57% plan to implement chatbots

- 28% acknowledged Senior Management awareness on the technology

- 51% free use of GPTs

- 47% lack data or in-house infra to implement chatbots



Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

ChatGPT and banks in Luxembourg

71%

Opportunity or threat?

76% of respondents see ChatGPT as an opportunity for their institutions rather than a threat. **In the banking sector, the figure is 71%.** A little lower, but still positive!

Is a chatbot in the pipeline?

57% of respondents plan to implement chatbots. The figure is even higher **for banks: 88% envisage to implement AI-powered chatbots**.

7%

Are senior managers comfortable with ChatGPT?

Respondents said that only 28% of senior executives were very familiar with the AI tool. The figures are even lower for banks, with **only 7% of senior executives very familiar with the technology**.

Do banks allow their staff to use ChatGPT?

For 51% of respondents, the tool can be used freely by all staff, 24% can use it partially and for 25% it is blocked completely. **For banks, the level of restrictions is higher: 44% free use**, 19% partial use and 37% blocked.

What's holding banks back?

47% of surveyed institutions lack data and infrastructure in-house to effectively implement ChatGPT or other AI-powered chatbots. **For banks, this figure amounts to 63%**.

Sources

- Survey on the adoption of ChatGPT, FinTech and Innovation Forum of the Luxembourg Bankers' Association (ABBL), Supported by Société Générale, April 2023
- 42 respondents, representing a range of companies, including banks, consulting companies, law firms, payment providers, fintech firms, and software vendors

Audit and Risk Management Solution

What are the risk considerations with AI technology?

Business Risks

- exposure a company or organization has to factor(s) that will lower its profits or lead it to fail its objectives (e.g., strategic, environmental, market, credit, operational, compliance, risks).

IT Risks

- exposure to specific technological risks that can generally impact the ability of the organization continue its activity, its reputation, can have legal or regulatory consequences or commercial negative impact.

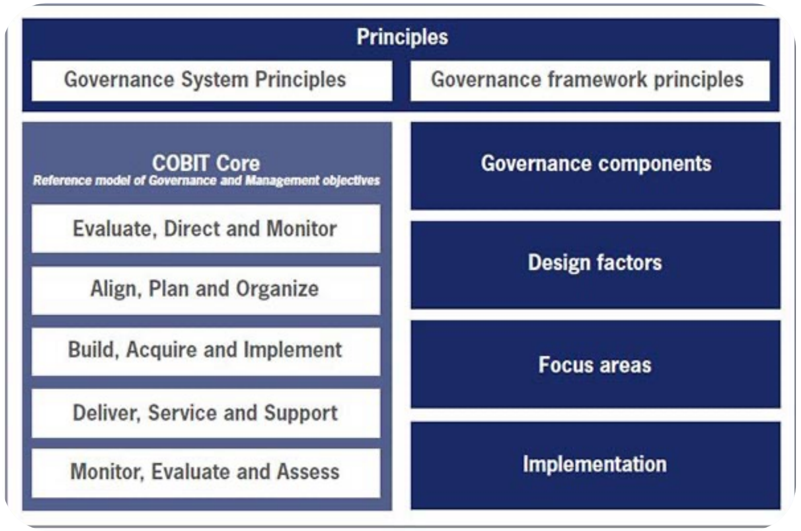
AI Risks

- exposure a company or organization has to factors that are influenced or generated by the use of AI and that can lead to negative outcomes in terms of achieving business or organization objectives

EXISTING FRAMEWORKS HAVE A PARTIAL OR NO COVERAGE OF AI RISKS

IT loves frameworks but AI calls for changes

IT Framework (e.g., COBIT)



Principles

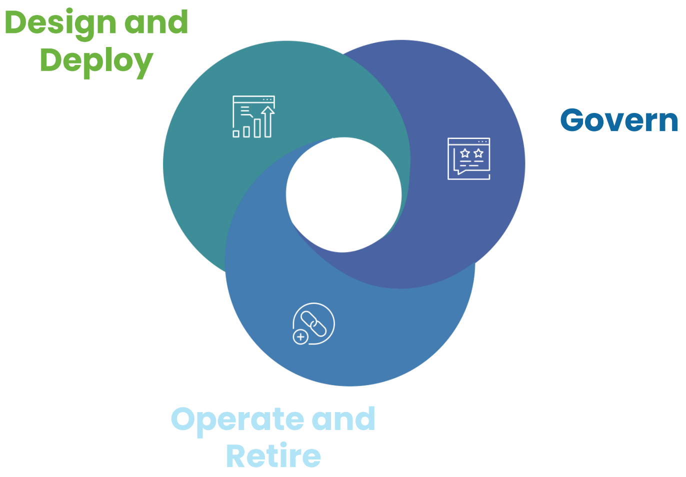
Governance System Principles | Governance framework principles

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)



Design and Deploy

Govern

Operate and Retire

Our proposed risk framework for AI

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.

AI Risks

Enterprise Governance

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

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

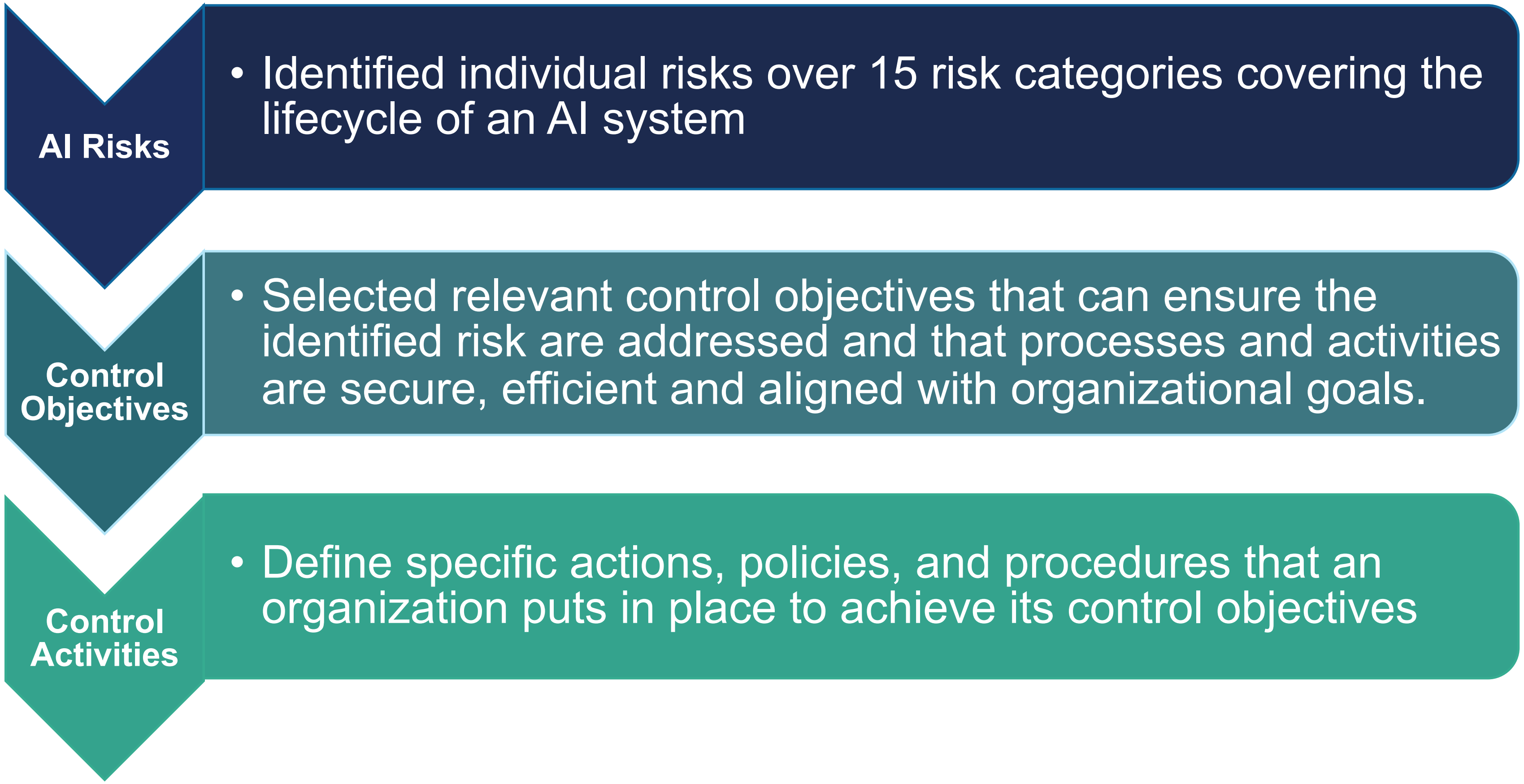
Resilience

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.

Control activities are mapped to risks



AI Risks

- Identified individual risks over 15 risk categories covering the lifecycle of an AI system

Control Objectives

- Selected relevant control objectives that can ensure the identified risk are addressed and that processes and activities are secure, efficient and aligned with organizational goals.

Control Activities

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

59

Individual AI related Risks

40

Control Objectives

127

Control Activities

AI Control Objectives and Control Activities (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

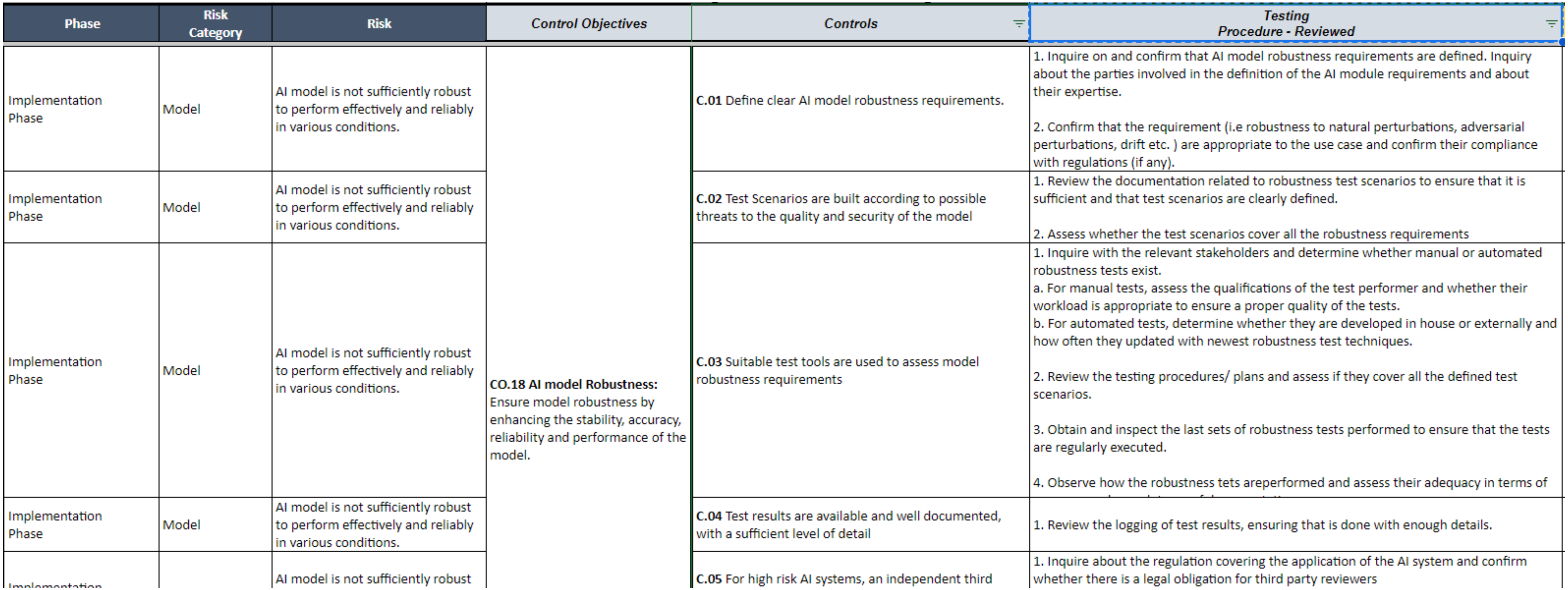
Assessment procedure

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.

AI Control Framework Demo



Phase	Risk Category	Risk	*Control Objectives*	*Controls*	*Testing Procedure - Reviewed*
Implementation Phase	Model	AI model is not sufficiently robust to perform effectively and reliably in various conditions.	**CO.18 AI model Robustness:** Ensure model robustness by enhancing the stability, accuracy, reliability and performance of the model.	**C.01** Define clear AI model robustness requirements.	1. Inquire on and confirm that AI model robustness requirements are defined. Inquiry about the parties involved in the definition of the AI module requirements and about their expertise. 2. Confirm that the requirement (i.e robustness to natural perturbations, adversarial perturbations, drift etc.) are appropriate to the use case and confirm their compliance with regulations (if any).
Implementation Phase	Model	AI model is not sufficiently robust to perform effectively and reliably in various conditions.		**C.02** Test Scenarios are built according to possible threats to the quality and security of the model	1. Review the documentation related to robustness test scenarios to ensure that it is sufficient and that test scenarios are clearly defined. 2. Assess whether the test scenarios cover all the robustness requirements
Implementation Phase	Model	AI model is not sufficiently robust to perform effectively and reliably in various conditions.		**C.03** Suitable test tools are used to assess model robustness requirements	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 performer 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 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 inspect the last sets of robustness tests performed to ensure that the tests are regularly executed. 4. Observe how the robustness tets areperformed and assess their adequacy in terms of
Implementation Phase	Model	AI model is not sufficiently robust to perform effectively and reliably in various conditions.		**C.04** Test results are available and well documented, with a sufficient level of detail	1. Review the logging of test results, ensuring that is done with enough details.
Implementation		AI model is not sufficiently robust		**C.05** For high risk AI systems, an independent third	1. Inquire about the regulation covering the application of the AI system and confirm whether there is a legal obligation for third party reviewers

Thank you!

www.isaca.org