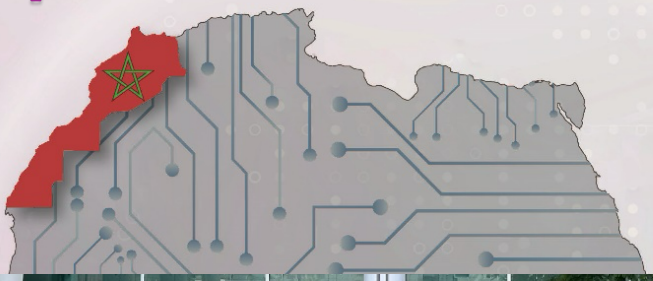
AMSSNuR

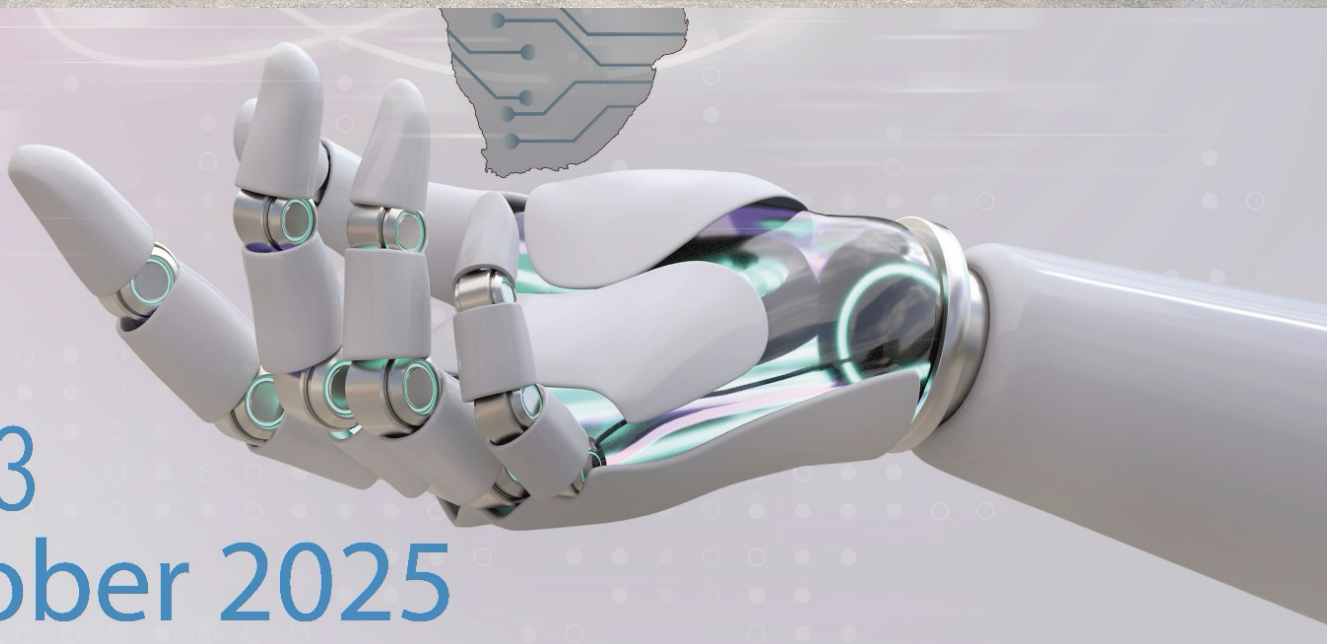
INSIDER THREAT MITIGATION

REGIONAL WORKSHOP FOR FRENCH-SPEAKING AFRICA

ADDRESSING THE NEXUS OF ARTIFICIAL INTELLIGENCE AND INSIDER THREAT MITIGATION

Compendium of Good Practices





21-23
October 2025

Rabat , Morocco

TABLE OF CONTENTS

Executive Summary

This compendium presents good practices for addressing the nexus of Artificial Intelligence (AI) and Insider Threat Mitigation (ITM), based on polling results and discussion sessions at the Regional Workshop.

The polling results show a strong and consistent participant view that AI adoption in insider threat mitigation must be governed by:

- **Regulatory frameworks**,
- **Data protection and privacy safeguards**,
- **Human oversight of AI-supported decisions**,
- **Relevant and high-quality training data**,
- **Oversight, accountability, and standards-based implementation**

The workshop also identified major implementation challenges, especially:

- Access to and sharing of quality data,
- Regulatory and institutional frameworks,
- Political will,
- Funding,
- Transparency and accountability,
- Skills and human resources gaps

Participants also assessed several priorities for a possible African Chapter under INFCIRC/908, with particularly strong interest in:

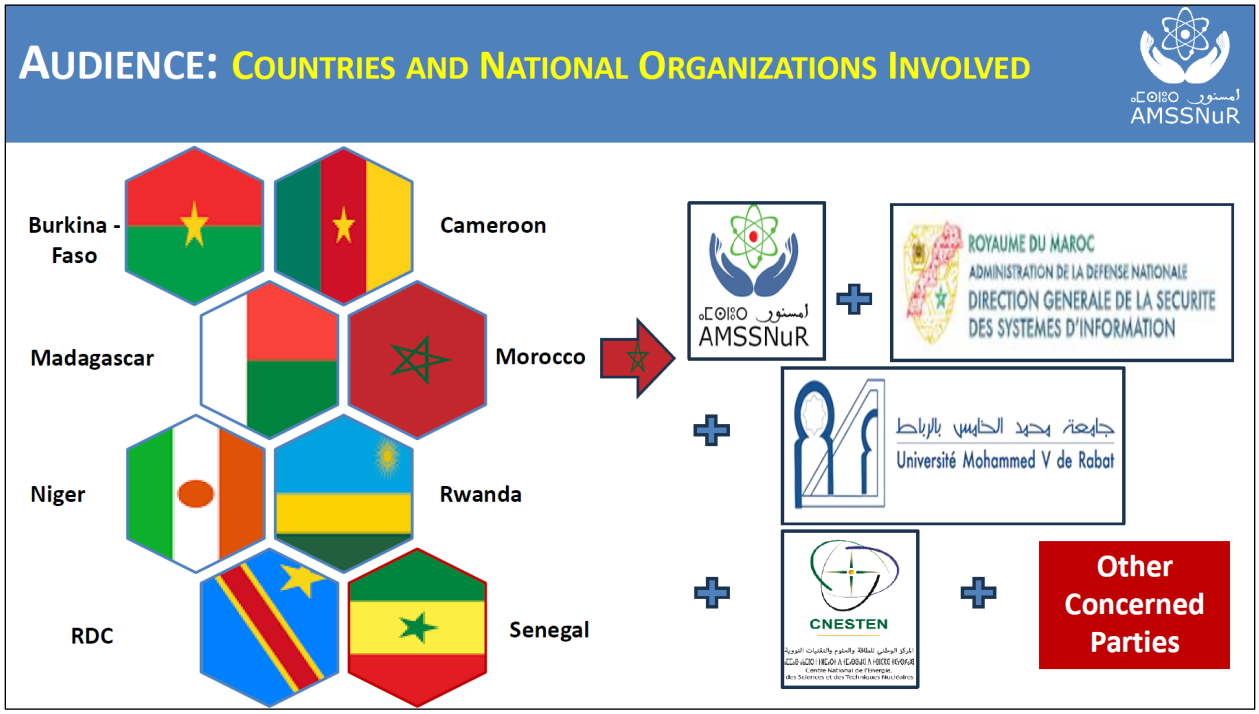
- Good practices for integrating AI into insider threat mitigation measures,
- Development of enabling regulatory frameworks,
- Inclusion of AI elements in cybersecurity regulations,
- Exercises and collaboration with other subscribers.

This compendium translates those polling results into practical good practices for governments, regulators, operators, and partner organizations.

1. Background

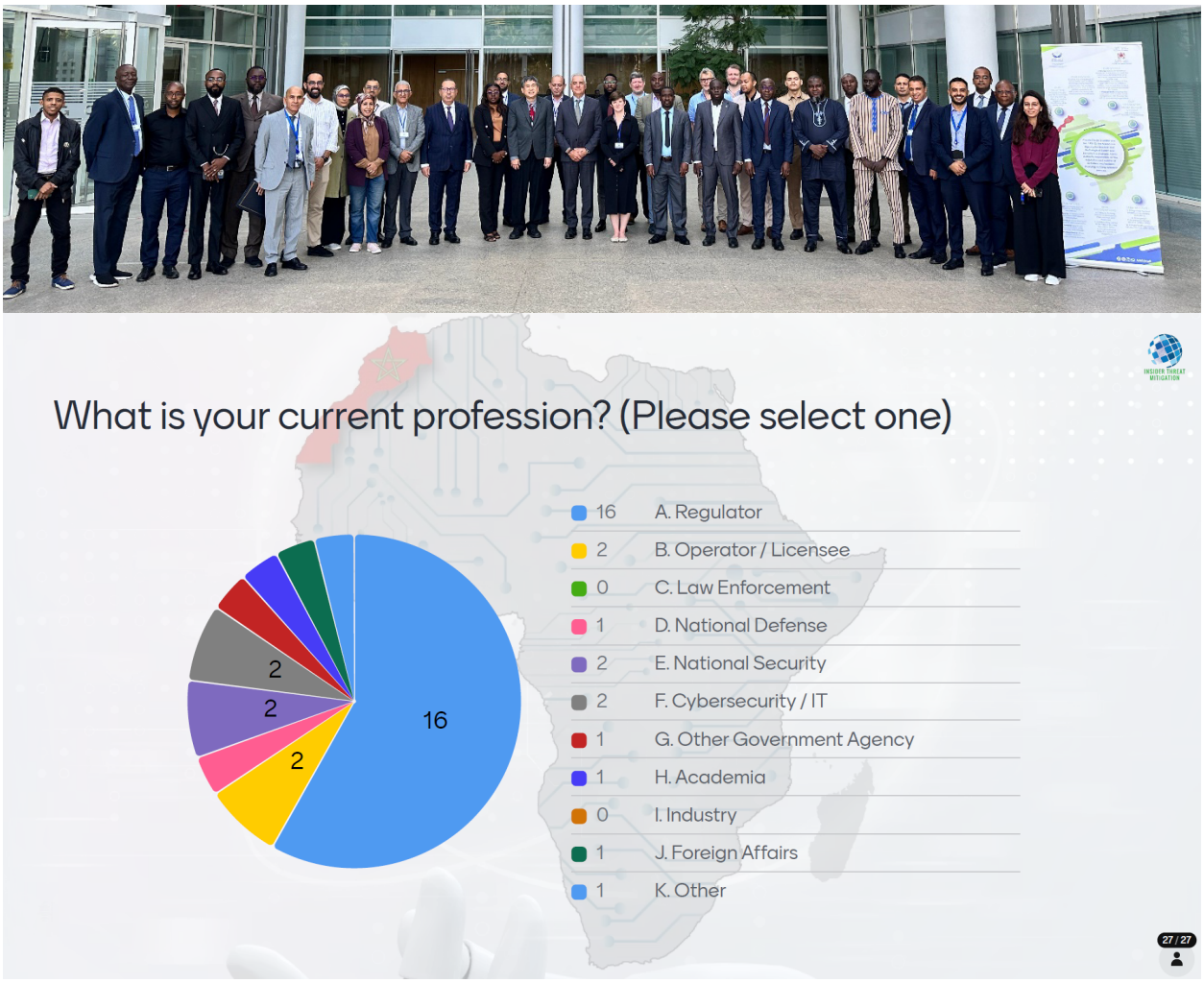
The Regional Workshop on Addressing the Nexus of Artificial Intelligence and Insider Threat Mitigation for French-Speaking Africa was held in Rabat, Morocco from 21 to 23 October 2025. It was hosted by AMSSNuR with support from DOE/NNSA under the Advancing INFCIRC/908 International Working Group.

This workshop was convened under the auspices of the Advancing INFCIRC/908 International Working Group as the first regional workshop under its "Impact from Technology" theme, reflecting the growing importance of understanding how emerging technologies, especially Artificial Intelligence, may affect nuclear security and insider threat mitigation. The workshop was designed to explore how AI technologies can enhance insider threat mitigation while also identifying associated risks and developing regionally relevant good practices for implementation.



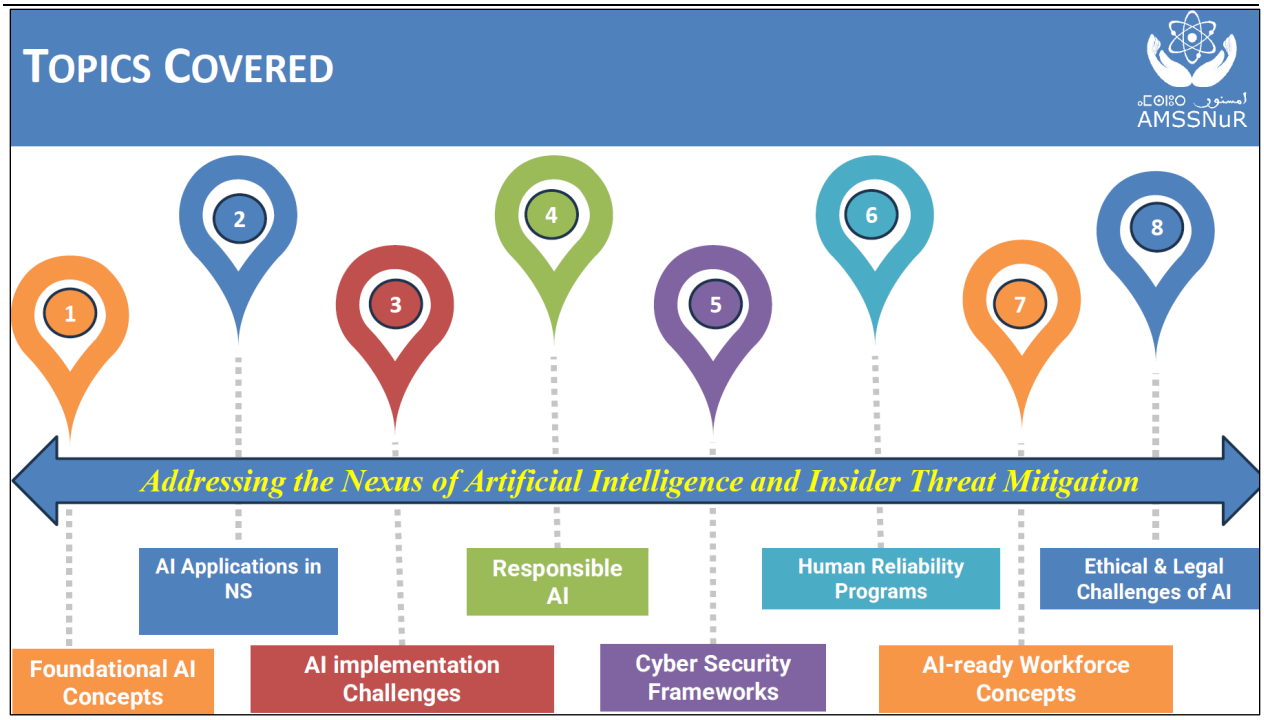
The event brought together participants from across French-speaking Africa, as well as experts and partner representatives from outside the region (See Figure above). The workshop included representation from 7 African countries, Morocco, Belgium, and the United States, participation from approximately 35 attendees, and broad engagement from regulatory, operational, cybersecurity, academic, and other concerned stakeholders. Morocco was represented by AMSSNuR (Regulatory Body), CNESTEN (Operator), DGSSI (National Cybersecurity Regulator), the University of Rabat, and

other concerned parties. A group photograph and the distribution of professions present at this regional workshop are presented in the figure below.



The workshop formed part of the broader evolution of the Advancing INFCIRC/908 International Working Group. Working Group efforts following the 2024 Symposium were reframed around two key themes: Human Factors and Impact from Technology. This regional workshop was the first regional event and focused specifically on the technology theme. Participants recognized that the nexus of AI and insider threat mitigation is especially well suited for regional discussion because the ideas, risks, and implementation approaches are likely to have cross-border relevance and impact.

The workshop explored a broad range of interrelated topics as shown below:



Moroccan institutions presented the current national situation regarding the nuclear safety and security regulatory framework, capacity building, cybersecurity law, and insider threat mitigation measures at the nuclear research center. The workshop also benefited from expert contributions from the United States and Belgium, whose representatives shared knowledge and experience relevant to insider threat mitigation and the responsible use of AI.

In his opening remarks, Mr. Saïd Mouline, Director General of AMSSNuR, emphasized that "artificial intelligence holds promising potential for advancing nuclear and radiological applications in the medical, industrial, and energy sectors. As safety and security regulatory authorities, we must thoroughly understand these emerging technologies in order to develop the regulations, guidelines, and authorizations necessary for their safe and responsible implementation."

Mr. Saïd Mouline also highlighted the importance of this workshop as a platform for exchanging ideas on the common challenges related to artificial intelligence and insider threats, particularly regarding the detection and prevention of risky behaviors and their integration into existing physical protection systems. This initiative is in line with AMSSNuR's ongoing efforts to promote a sustainable safety and security culture and strengthen the resilience of nuclear security regimes in Africa and beyond.

Participants were highly engaged throughout the workshop. Attendees asked many questions, actively contributed concerns and perspectives, and participated enthusiastically in scenario-based discussions, mini-exercises, and other interactive sessions. The use of French as the workshop

language was noted as an important factor in creating a relaxed atmosphere that encouraged open dialogue and active participation.

The workshop generated strong interest in future African cooperation. Country specific action included:

Cameroon	Expressed interest in subscribing to INFCIRC/908, noting lack of sub-Saharan African representation
Senegal	Plans to integrate AI literacy training into universities and increase AI research publications
Rwanda	Committed to bringing information home despite newer nuclear program status
Madagascar	Will share information with organizations despite government transition period

Participants also suggested creating an African, or specifically French-speaking African, subchapter or working group under the Advancing INFCIRC/908 International Working Group to continue exploring the nexus of AI and insider threat mitigation. Additional next steps identified included making workshop materials available online and exploring a possible side event at IAEA CyberCon26 in May 2026 to present the workshop's outcomes and future regional directions.

This compendium uses the workshop polling results, discussion sessions, and reported outcomes to identify good practices. It is intended to translate workshop insights into practical actions for governments, regulators, operators, and partner organizations seeking to address AI-enabled insider threat mitigation in a responsible, lawful, and regionally relevant manner.

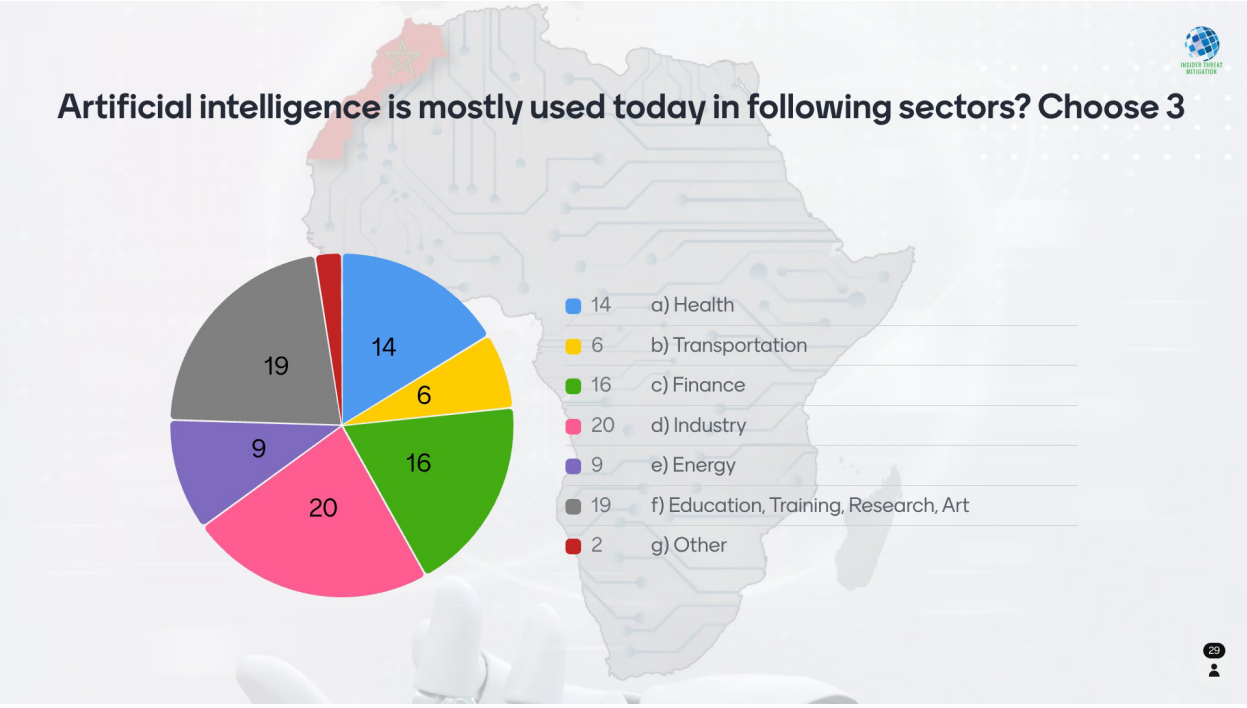
2. Key Polling Themes

The anonymous polling results addressed the following key topics:

Poll Topic	Relevance to AI and Insider Threat Mitigation
Sectors where AI is mostly used today	Helps frame participant understanding of AI maturity and current use cases
Ethical and legal measures to regulate AI	Directly relevant to governance of AI-enabled insider threat mitigation
Potential impacts of AI	Identifies perceived risks and opportunities
Challenges of using AI to mitigate insider threats	Highlights practical barriers to implementation
Priorities for a possible African Chapter of INFCIRC/908	Indicates regional cooperation priorities
Top ideas participants will share with colleagues	Shows strongest takeaways and likely enduring lessons

3. Summary of Polling Results

3.1 Perceived Current Sectors of AI Use

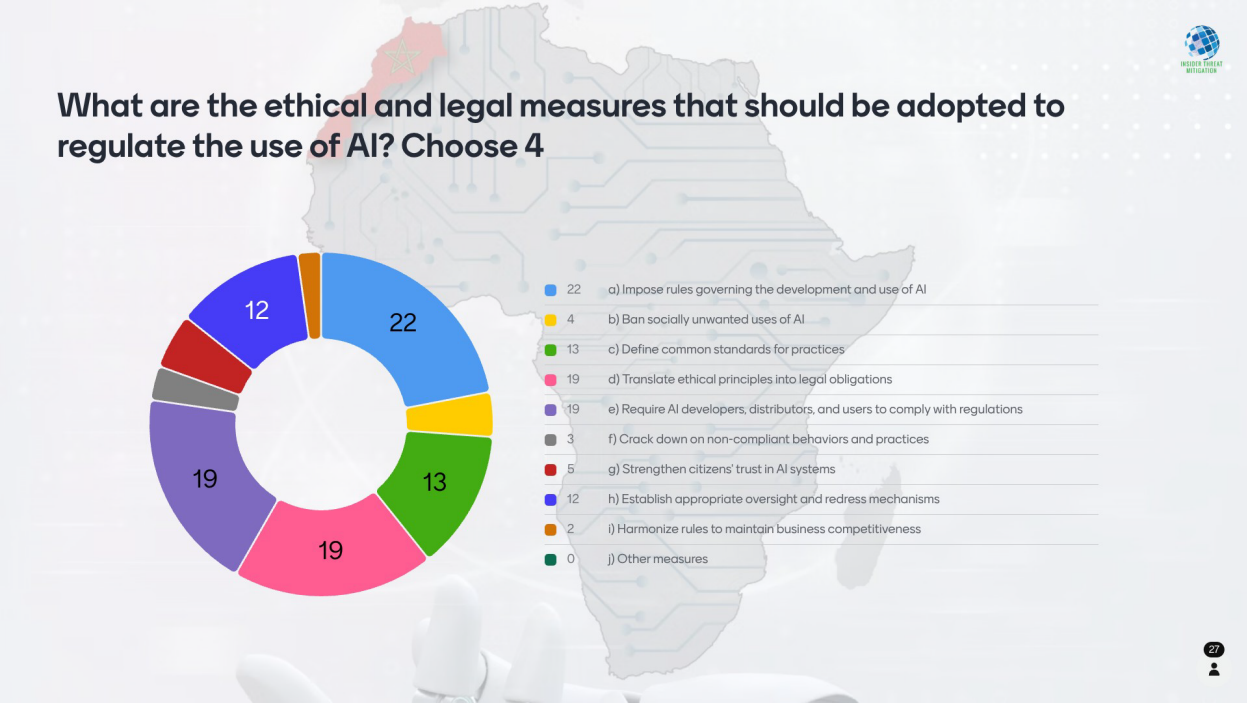


Participants appear to view AI as already established across multiple high-value sectors, especially finance, industry, health, and education. This matters for insider threat mitigation because it suggests that workshop participants understand AI as an operational tool with cross-sector relevance, not merely experimental or consumer technology.

Good practice implication

Organizations should draw lessons from mature AI sectors when designing AI-enabled insider threat mitigation measures, especially around governance, safety, data controls, and workforce training.

3.2 Ethical and Legal Measures to Regulate the Use of AI



The most frequently repeated participant choices strongly suggest the following measures were viewed as priorities:

- Impose rules governing the development and use of AI
- Require AI developers, distributors, and users to comply with regulations
- Translate ethical principles into legal obligations
- Define common standards for practices
- Establish appropriate oversight and redress mechanisms

Other measures that appeared, though less consistently, included:

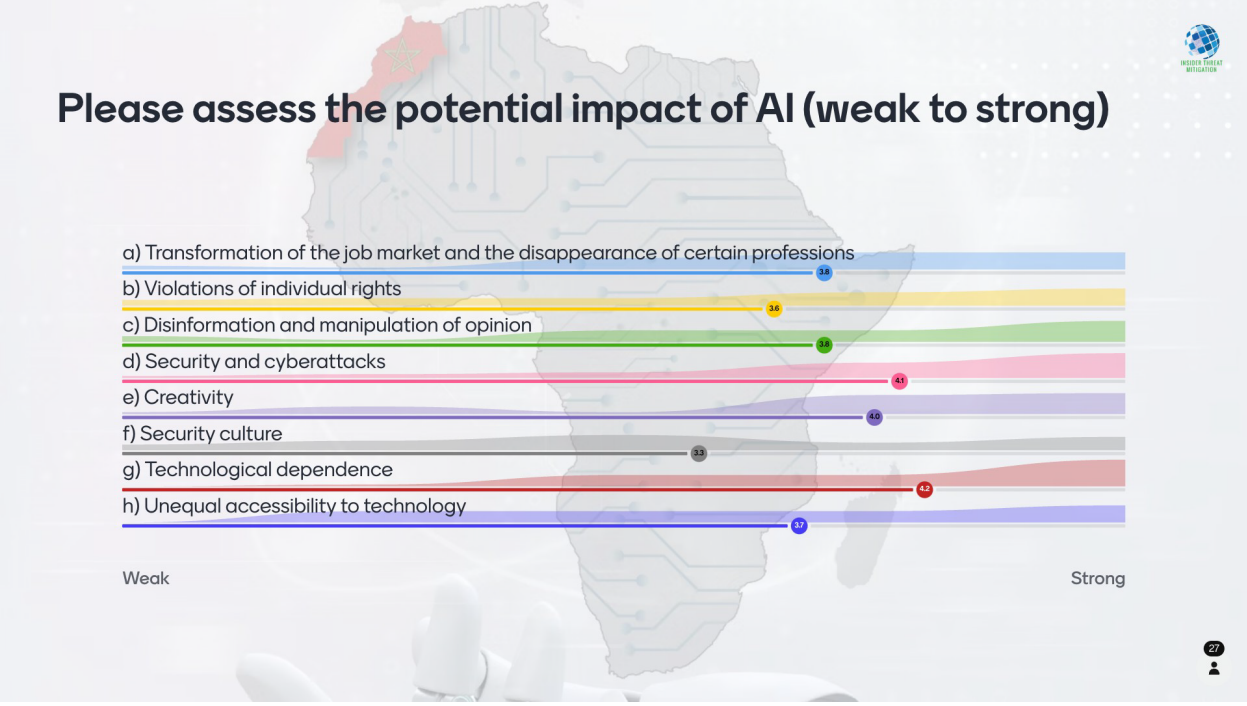
- Banning socially unwanted uses of AI
- Cracking down on non-compliant behaviors
- Strengthening citizens' trust in AI systems
- Harmonizing rules to maintain competitiveness

Participants clearly favored a governance-heavy approach. The polling suggests that participants do not see ethical AI as voluntary guidance alone. Instead, they favor moving from broad principles to enforceable rules, compliance obligations, standards, and oversight.

Good practice implication

AI for insider threat mitigation should never be implemented as an informal add-on. It should operate within a clear framework of law, policy, standards, compliance, and oversight.

3.3 Perceived Potential Impacts of AI



Participants assessed the impact of AI ranging from weak to strong across several categories:

- Transformation of the job market
- Violations of individual rights
- Disinformation and manipulation
- Security and cyberattacks
- Creativity
- Security culture
- Technological dependence
- Unequal accessibility to technology

The extracted rows show many high ratings, especially for:

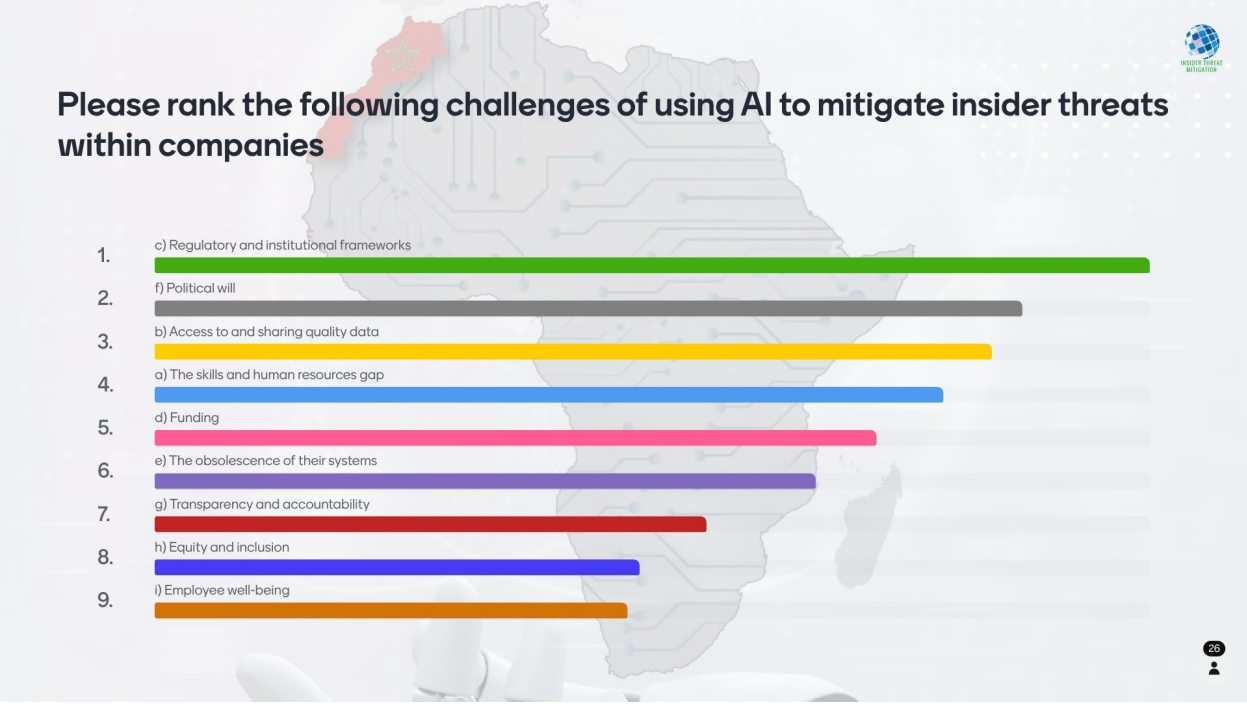
- Security and cyberattacks
- Technological dependence
- Transformation of the job market
- Violations of individual rights
- Disinformation and manipulation

Participants appear to perceive AI as high-impact, especially in areas involving security, dependence, and rights. This is highly relevant to insider threat mitigation because those same areas affect trustworthiness assessments, organizational resilience, monitoring activities, and incident response.

Good practice implication

Any use of AI in insider threat mitigation should be treated as a high-consequence activity requiring risk assessment, legal safeguards, and human review.

3.4 Main Challenges of Using AI to Mitigate Insider Threats



The polling results indicate that the most important challenge areas are:

- Regulatory and institutional frameworks
- Political will
- Access to and sharing quality data
- Skills and human resources gap
- Funding
- Obsolescence of systems
- Transparency and accountability

Discussions on this topic specifically concluded that participants recognized:

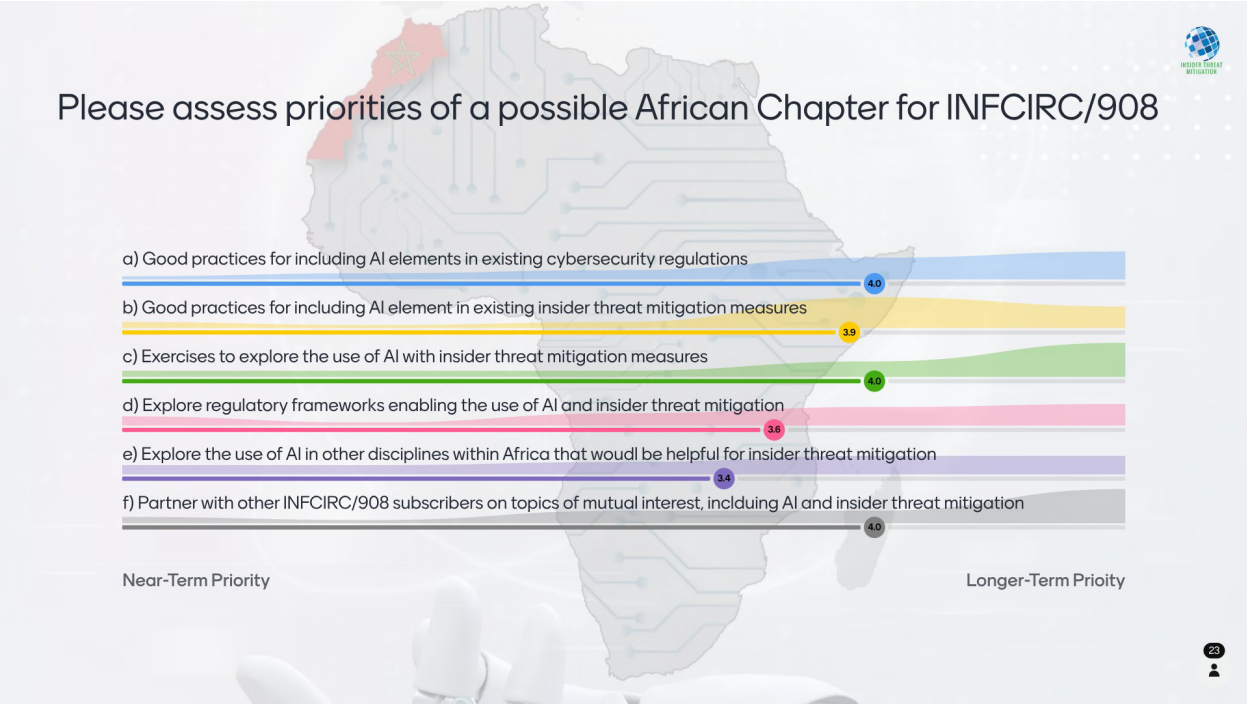
- Regulatory frameworks,
- Political will,
- Privacy restrictions,
- Data access

as primary implementation challenges, which also aligns closely with the polling results.

Good practice implication

Successful AI adoption for insider threat mitigation depends less on buying tools and more on solving institutional, legal, human, and data challenges first.

3.5 Priorities for a Possible African Chapter for INFCIRC/908



Participants assessed priorities for a possible African Chapter in the following areas:

- Good practices for including AI elements in existing cybersecurity regulations
- Good practices for including AI elements in existing insider threat mitigation measures
- Exercises to explore the use of AI with insider threat mitigation measures
- Explore regulatory frameworks enabling the use of AI and insider threat mitigation
- Explore the use of AI in other disciplines within Africa helpful for insider threat mitigation
- Partner with other INFCIRC/908 subscribers on topics of mutual interest

The participant responses show many high ratings across these categories, especially around:

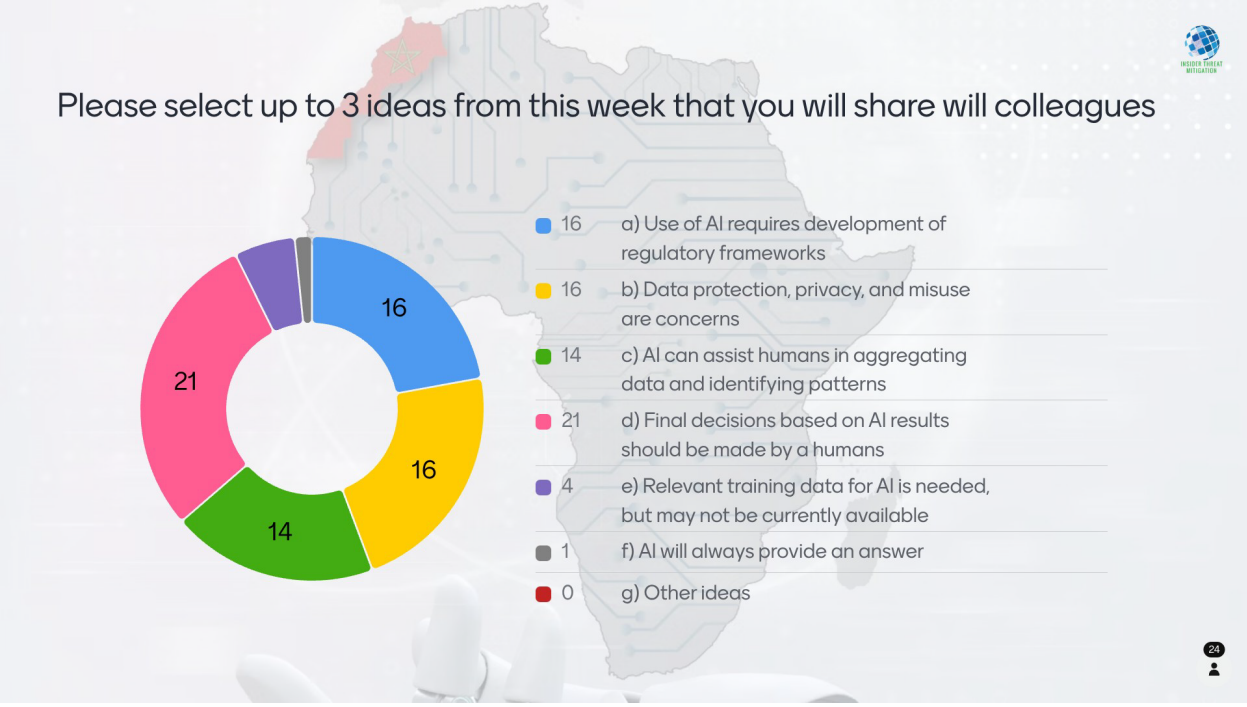
- Integrating AI into insider threat mitigation measures,
- Regulatory frameworks,
- Cybersecurity regulations,
- Partnering with other subscribers.

Participants want practical, regionally relevant, and collaborative next steps, not only conceptual discussion.

Good practice implication

Regional cooperation should focus on implementation tools, exercises, model frameworks, and peer exchange.

3.6 Top Ideas Participants Will Share with Colleagues



This is one of the clearest and most useful sets of polling results. The most repeated takeaway ideas selected by participants were:

- Use of AI requires development of regulatory frameworks
- Data protection, privacy, and misuse are concerns
- AI can assist humans in aggregating data and identifying patterns
- Final decisions based on AI results should be made by humans
- Relevant training data for AI is needed, but may not be currently available

The response, “AI will always provide an answer,” appears less like an endorsed principle and more like a discussion prompt or cautionary observation.

These takeaways are highly actionable. They show that participants left the workshop with a grounded understanding of both AI’s usefulness and its limits.

Good practice implication

A mature AI-insider threat program must be:

- Regulated
- Privacy-aware
- Human-centered
- Data-dependent
- Practical rather than overly automated

4. Compendium of Good Practices

4.1 Establish Regulatory Frameworks Before Deployment

Good practice: Develop and adopt regulatory and institutional frameworks before deploying AI for insider threat mitigation.

Why this matters: The most repeated takeaway in the polling results was that the use of AI requires development of regulatory frameworks. Participants also ranked regulatory and institutional frameworks as a major challenge.

Actions:

- define legal authority for AI-supported monitoring and analysis,
- align AI use with national cybersecurity and privacy laws,
- clarify which agencies or offices have oversight responsibility,
- establish formal policy on acceptable and prohibited AI use,
- define accountability for operators, developers, and users.

4.2 Protect Data Privacy and Prevent Misuse

Good practice: Build strong data governance and privacy safeguards into all AI-enabled insider threat activities.

Why this matters: One of the most frequently selected workshop takeaways was that data protection, privacy, and misuse are concerns. The workshop narrative also identified privacy restrictions and data access as major barriers.

Actions:

- apply data minimization,
- establish role-based access controls,
- use secure storage and transfer mechanisms,
- define data retention and deletion requirements,
- conduct privacy impact reviews,
- restrict use of sensitive personnel data unless clearly authorized,
- monitor for misuse of collected data.

4.3 Keep Humans Responsible for Final Decisions

Good practice: Require that final decisions based on AI results be made by humans.

Why this matters: This was one of the most repeated concluding ideas in the polling results, and it aligns with workshop discussions emphasizing human authorized actions rather than AI-authorized actions.

Actions:

- ensure AI outputs are advisory, not determinative,
- require human review before disciplinary or security actions,
- define escalation and appeal procedures,
- train decision-makers to question AI outputs,
- maintain records of human decisions and rationale.

4.4 Use AI to Support Pattern Detection, Not Replace Judgment

Good practice: Use AI as a support tool for aggregating data and identifying patterns, while preserving expert judgment.

Why this matters: Participants repeatedly selected the idea that AI can assist humans in aggregating data and identifying patterns. This suggests they see AI's value in analysis support, not autonomous control.

Actions

- use AI for anomaly detection, data fusion, trend analysis, and alert prioritization,
- validate AI outputs against operational expertise,
- compare automated recommendations with human assessments,
- avoid treating correlations as proof of insider threat activity,
- incorporate multidisciplinary review.

4.5 Ensure Availability of Relevant Training Data

Good practice: Do not deploy AI models unless relevant, sufficient, and trustworthy data are available.

Why this matters: Participants frequently selected the takeaway that relevant training data are needed but may not currently be available. Access to quality data was also a major implementation challenge.

Actions:

- assess data quality before development,
- validate that data reflect actual operating conditions,
- document data gaps and limitations,
- avoid overfitting to foreign or non-representative contexts,
- update datasets and models over time,
- establish data-sharing protocols where legally permissible.

4.6 Create Oversight, Redress, and Accountability Mechanisms

Good practice: Establish mechanisms to oversee AI use, handle complaints, review errors, and assign responsibility.

Why this matters: Participants repeatedly selected oversight and redress mechanisms, common standards, and compliance obligations among the most important legal and ethical measures.

Actions

- designate a responsible oversight body,
- define audit and review schedules,
- create procedures to challenge erroneous AI-supported outcomes,
- log model outputs and resulting actions,
- define liability and corrective action pathways,
- require periodic review of system performance and fairness.

4.7 Translate Ethical Principles into Enforceable Practice

Good practice: Move from general ethical principles to clear operational requirements.

Why this matters: Participants frequently selected “translate ethical principles into legal obligations” as a preferred measure.

Actions

- incorporate ethics into policy, procurement, testing, and operations,
- convert principles such as fairness, transparency, and proportionality into measurable controls,
- define prohibited use cases,
- ensure that ethical review is part of system approval.

4.8 Develop Common Standards and Harmonized Practices

Good practice: Use common standards to promote consistency across institutions and countries.

Why this matters: Participants repeatedly selected “define common standards for practices,” and regional cooperation was a strong theme throughout the workshop.

Actions

- create standard terminology and governance models,
- develop shared evaluation criteria for AI-enabled ITM systems,
- align technical and procedural controls where feasible,
- support regional templates for policies and exercises.

4.9 Build an AI-Ready Workforce

Good practice: Invest in AI literacy and workforce capacity across regulatory, security, technical, and management functions.

Why this matters: The workshop narrative showed strong interest in AI literacy and workforce development. Skills and human resources gaps were also identified as a challenge.

Actions

- train leaders and practitioners on AI capabilities and limitations,
- define workforce roles such as users, evaluators, and reviewers,
- include scenario-based training,
- build local expertise in data governance, analytics, and oversight,
- partner with universities and training institutions.

4.10 Address Institutional Readiness, Not Just Technology

Good practice: Assess institutional readiness before adopting AI.

Why this matters: Participants highlighted challenges involving political will, funding, obsolete systems, regulatory barriers, and data access. These are institutional issues, not merely technical ones.

Actions

- assess policy, legal, technical, workforce, and budget readiness,
- identify legacy system constraints,
- secure leadership support,
- establish phased implementation,
- pilot low-risk use cases first.

4.11 Integrate AI into Existing Insider Threat and Cybersecurity Programs

Good practice: Incorporate AI into existing programs rather than building isolated tools or disconnected processes.
Why this matters: Participants rated as high priorities: good practices for including AI in 1) cybersecurity regulations and 2) insider threat mitigation measures.

Actions

- align AI initiatives with insider threat governance structures,
- integrate with cybersecurity monitoring and physical protection where appropriate,
- ensure HR, legal, cybersecurity, and security teams coordinate,
- update incident response playbooks to account for AI-supported analysis.

4.12 Use Exercises and Regional Collaboration to Build Confidence

Good practice: Use exercises, workshops, and peer partnerships to test approaches and build regional capacity.

Why this matters: Participants rated exercises and partnership with other INFCIRC/908 subscribers as important priorities for a possible African Chapter.

Actions

- conduct scenario-based tabletop exercises,
- share case studies and lessons learned,
- establish regional points of contact,
- develop collaborative working groups,
- pilot regional guidance documents and sample frameworks.

5. Recommended Good Practice Framework

Area	Good Practice
Governance	Establish legal, regulatory, and institutional frameworks before deployment
Human Oversight	Keep final decisions with authorized humans
Privacy	Protect data, privacy, and against misuse
Data Quality	Use relevant, high-quality, legally accessible training data
Accountability	Create audit, review, redress, and compliance mechanisms
Ethics	Translate ethical principles into enforceable obligations
Standards	Develop common standards and harmonized practices
Workforce	Build AI literacy and institutional capacity
Readiness	Address political, technical, and organizational prerequisites
Integration	Embed AI into existing insider threat and cybersecurity systems
Regional Cooperation	Use exercises, partnerships, and knowledge exchange

6. Recommended Priorities for Future African Regional Work

Based on the polling results and workshop discussions, the following should be prioritized for future regional cooperation:

Recommended Priority	Basis in Polling Results
Develop model regulatory frameworks	Strong emphasis on regulation and enabling legal frameworks
Produce good practices for AI in insider threat programs	Directly aligned with highly rated African Chapter priorities
Develop guidance on privacy and data protection	Repeated concern in concluding takeaways
Create human oversight principles for AI-supported decisions	Strong concluding takeaway
Develop shared standards and oversight approaches	Frequently selected ethical and legal measure
Conduct practical exercises	Highly rated future priority

Support regional knowledge exchange with other subscribers	Highly rated collaboration priority
Improve access to quality data and data governance	Identified as a major challenge
Expand AI literacy and workforce readiness	Recurrent workshop theme

7. Conclusion

The workshop polling results show a clear and practical consensus among participants. They do not view AI as a standalone technical solution to insider threat risk. Instead, they see AI as a potentially valuable tool that must be embedded within strong governance, privacy protections, human oversight, and reliable data practices.

The strongest messages from the polling results are:

Key Message	Meaning
AI requires regulatory frameworks	Governance must come first
Privacy and misuse are major concerns	Data protection is essential
AI can help identify patterns	AI is useful as decision support
Humans must make final decisions	Human accountability cannot be removed
Relevant training data may be lacking	Implementation must be grounded in data realism

These results provide a solid basis for a regional compendium of good practices and for future African cooperation on the responsible use of AI in insider threat mitigation.

The participants considered INFCIRC/908 Joint Statement as a platform to develop more cooperation and to learn from each other.

Annex A: Poll-Derived Good Practice Statements

1. AI use for insider threat mitigation should be authorized by law, policy, and institutional governance.
2. Personal data used by AI systems should be protected through strict privacy and security controls.
3. AI outputs should inform, not replace, human judgment.
4. Final personnel and security decisions should remain under human authority.
5. AI systems should only be used when relevant training data are available and understood.
6. Oversight, accountability, and redress mechanisms should be established before operational use.
7. Ethical principles should be converted into enforceable obligations, standards, and procedures.
8. Regional cooperation should support exercises, standards, model regulations, and peer learning.

Annex B: Agenda of the Regional Workshop for French-Speaking Africa: Addressing the Nexus of Artificial Intelligence and Insider Threat Mitigation (Rabat, Morocco, 21 - 23 October 2025)

DAY 1: Exploring Impacts of Artificial Intelligence and Insider Threat Mitigation Tuesday, 21 October 2025		
TIME	TOPIC	PRESENTER
9:30 – 9:40 am	Welcome Remarks: AMSSNuR, DG	Saïd Mouline
9:40 – 9:50 am	Welcome Remarks: DOE/NNSA	Frank Wong
9:50 – 10:00 am	Group Photo	All
10:00 – 10:10 am	Introductions	All
10:10 – 10:40 am	Keynote Speaker: Nuclear and Radiation Safety and Security Regulatory Capacity Building: AMSSNuR approach and experience	Taib Marfak
10:40 – 10:55 am	Morning Break	All
10:55 – 11:45 am	What is AI and Insider Threat Mitigation?	Jessica Baweja
11:45 – 12:10 pm	Plenary Panel Session I: Impacts of AI on Preventive Measures: Facilitated Discussion	Jessica Baweja
12:10 – 1:10 pm	*Working Lunch: "How can using AI work well?"*	
1:10 – 1:40 pm	Plenary Panel Session II: Impacts of AI on Physical Protection Systems	Frank Wong & Chris Spirito
1:40 –2:10 pm	Plenary Panel Session III: Impacts of AI on Cybersecurity Systems: Benefits & Challenges	Chris Spirito & Frank Wong
2:10 – 3:25 pm	Interactive Session I: Typhon-Intrusion-ARA	All
3:25 – 3:40 pm	*Afternoon Break*	*All*
3:40 – 4:45 pm		All
4:45 – 5:00 pm	Day 1 Wrap Up	All

DAY 2: Using Artificial Intelligence with Insider Threat Mitigation Wednesday, 22 October 2025		
TIME	TOPIC	PRESENTER
9:00 – 9:10 am	Day 1 Recap	All
9:10 – 9:45 am	Keynote Speaker: The Security of Moroccan Cyberspace: Legislative Framework and Challenges of Law 05-20 on Cybersecurity (DGSSI)	Zakaria Yartaoui
9:45 – 10:45 am	Plenary Facilitated Discussion I: Responsible AI for Insider Threat	Jessica Baweja
10:45 – 11:00 am	*Morning Break*	*All*
11:00 – 12:00 pm	Plenary Facilitated Discussion II: AI-based Behavioral Recognition	Justin Kinney
12:00 – 1:00 pm	*Working Lunch: "How can using AI cause problems?"*	
1:00 – 2:00 pm	Plenary Facilitated Discussion III: Cybersecurity and Resilience of Critical Infrastructures	Pr. MRABET and Chris Spirito
2:00 – 2:45 pm	Interactive Session I (45 min): AI Interface with Employee Life Cycle Processes	Frank Wong
2:45 – 3:30 pm	Interactive Session III (45 min): AI/ML for nuclear and radioactive material theft detection	Frank Wong
3:30 – 3:45 pm	*Afternoon Break*	*All*
3:55 – 4:40 pm	Interactive Session II: Gula Hospital and AI	Frank Wong
4:40 – 5:00 pm	Day 2 Wrap Up	All

DAY 3: Good Practices: Artificial Intelligence & Insider Threat Mitigation Thursday, 23 October 2025		
Time	TOPIC	PRESENTER
9:00 – 9:10 am	Day 2 Recap	All
9:10 – 9:45 am	Keynote Speaker: Convergence of AI and Insider Threat Mitigation: What's Next? (CNESTEN experience)	Youssef Harraq
9:45 – 10:30 am	AI-Ready Workforce	Jessica Baweja
10:30 – 10:45 am	*Morning Break*	*All*
10:45 – 11:45 am	Plenary Facilitated Discussion II: Ethical and Legal Challenges using AI with Insider Threat Mitigation	AMSSNuR
11:45 – 1:00 pm	*Working Lunch: "Moving Forward: A Good Balance"*	
1:00 – 2:00 pm	Interactive Roundtable Discussion (with Regional Experts, Capacity Building Challenges including education and training, HRD, …)	Taib Marfak, AMSSNuR
2:00 – 3:00 pm	Participant Roundtable	All Participants, AMSSNuR, Frank Wong
3:00 – 3:30 pm	Workshop Wrap Up • Certificates • Evaluation • Closing Remarks • Recommendations for next steps	