AI Mavericks & Mythos

New priorities for the internal auditor

The Institute of Internal Auditors Netherlands

Tjakko de Boer

5 Juni 2026

IIA Congres 2026

IIA CONGRES 2026 PRIDE & PREJUDICE

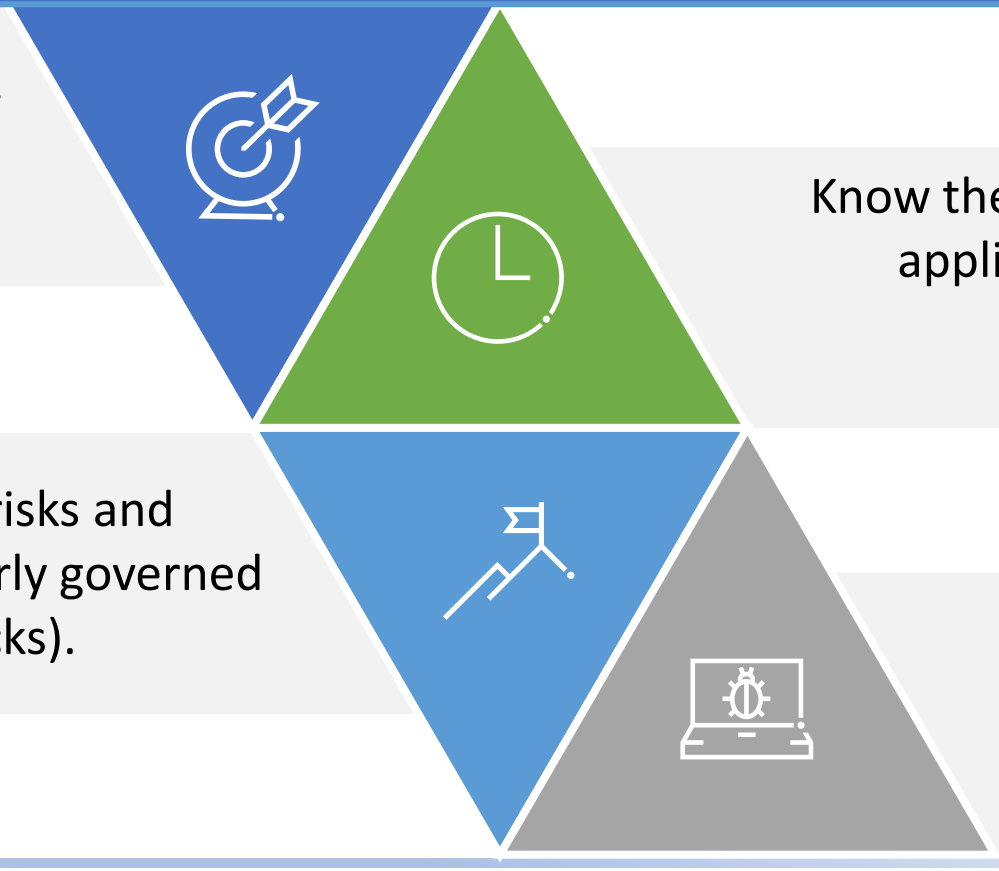
4 & 5 JUNI AFAS THEATER LEUSDEN


AFAS Theater
INTERNAL AUDIT CONFERENCE 2026
IIA
THE INSTITUTE OF INTERNAL AUDITORS
AI Mavericks and Mythos
New priorities for the internal auditor
MYTHOS
AI GOVERNANCE
Responsible.
Transparent.
Accountable.
AI THREATS
Emerging risks.
Real impact.
Proactive oversight.
INFORMATION SECURITY
Protect data.
Secure systems.
Build trust.
Including recent developments around Claude Mythos
Trust
Insight
Impact
INFORMATION SECURITY IS EVERYONE'S RESPONSIBILITY
AFAS Theater

Objective

Understand how AI is changing the information security risk landscape

Learn how AI-enabled threats can accelerate exploitation of security vulnerabilities (Mythos).



Know the regulations and standards applicable to AI-accelerated environments.

Understand the security risks and opportunities created by poorly governed AI adoption (Mavericks).

Equip Internal Audit to ask better questions in an AI-accelerated environment

Agenda

1. Introduction
2. Regulatory Context
3. Mythos: Defending against AI
4. AI Mavericks: Risks when adopting AI
5. Conclusions
6. Discussion and Questions

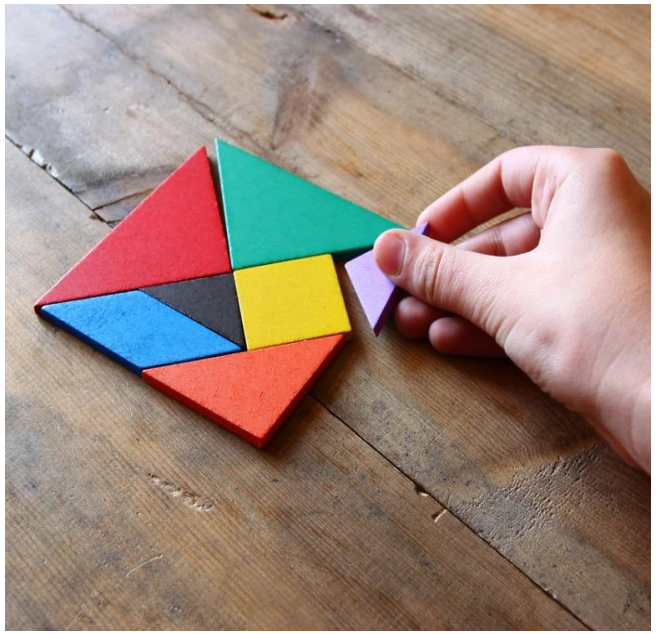
Regulatory Context

The EU Regulatory Puzzle

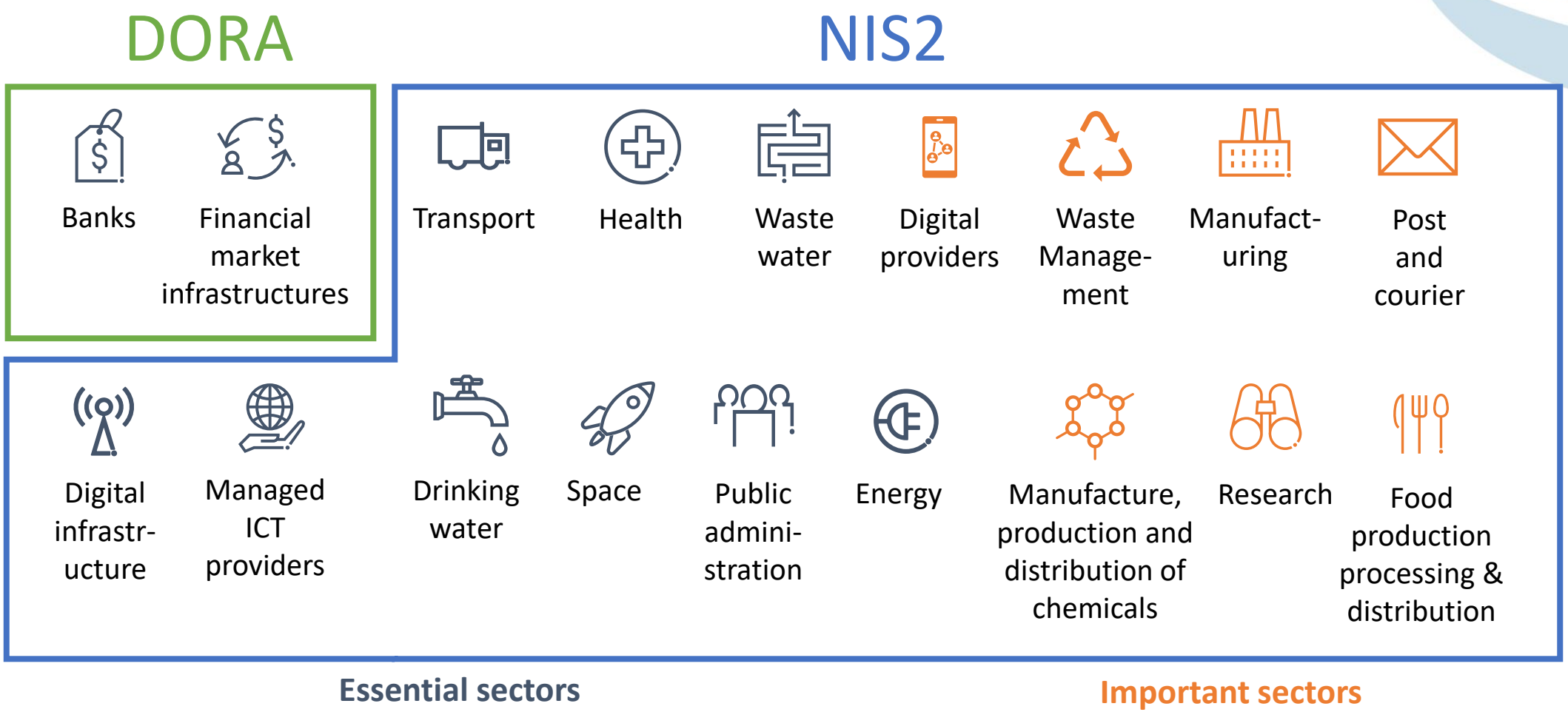
Shared aim: Manage the impact of AI and cybersecurity incidents on economy and society

Trustworthy AI and Digital Resilience on the EU's digital agenda:

- DORA
- NIS2
- Cybersecurity Act
- GDPR
- Cyber Resilience Act
- Data Act
- Digital Service Act
- Artificial Intelligence Act
- Cyber Solidarity Act
- PSD2
- Digital Euro Regulation
- MiCAR
- EU Health Data Space



Who is in scope?



DORA: Resilience in the financial sector

The DORA requirements are structured across 5 key pillars

Governance and ICT Risk Management

- ICT Risk Management Framework including an annual report
- Strategies, policies, procedures, tools and capabilities
- Accountable management body and clearly defined governance framework
- ICT processes, services and assets
- ICT Audits

Incident Response and Management

- Monitoring, handling and follow-up of ICT incidents to the regulator
- Implement a standardized classification approach
- Compulsory and standardized incident reporting

Digital Operational Resilience Testing

- Comprehensive testing program, with a focus on technical testing
- Threat-led tests performed by independent tester every 3 years

TPRM and Contract Management

- Register of information containing ICT providers and ICT services
- Guidelines for pre-contract assessment, ongoing assessment, contract arrange-ments, termination and stressed exits
- Right to access, inspect and audit including third-party involvement in digital operational testing

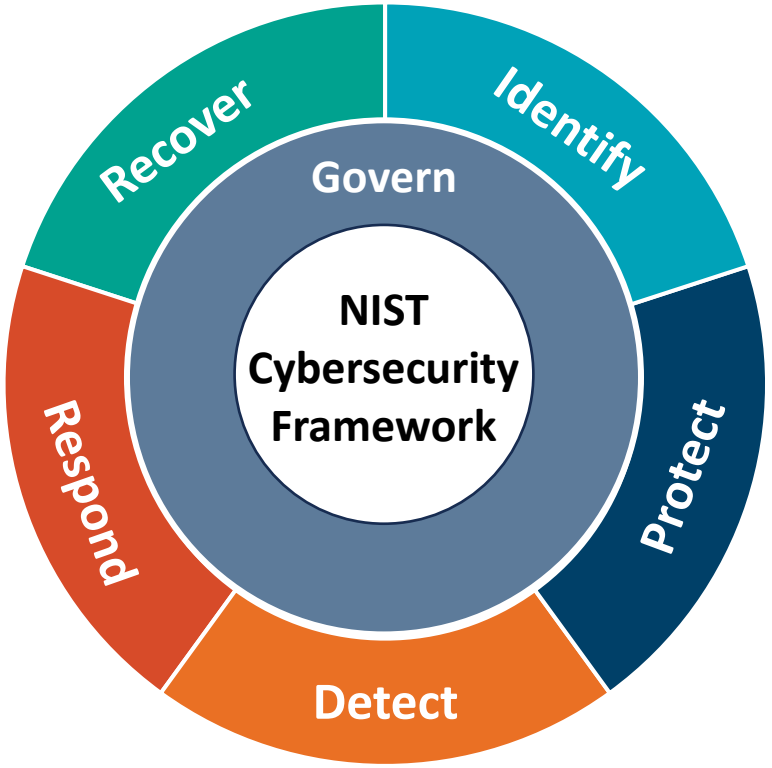
Information Sharing (Optional)

- Guidelines on information sharing arrangements for cyber threats and vulnerabilities

NIS2: Resilience in critical sectors

- Risk assessment and security policies
- Incident handling
- Business continuity, disaster recovery & crises management
- Supply chain security
- Security in networks, systems development and maintenance
- Security assessment policies and procedures
- Cyber hygiene, training & (board) awareness
- Cryptography policies & procedures
- HR security, access control and asset management
- Reporting obligations

NIST Cybersecurity Framework 2.0



Cyber resilience regulations and standards

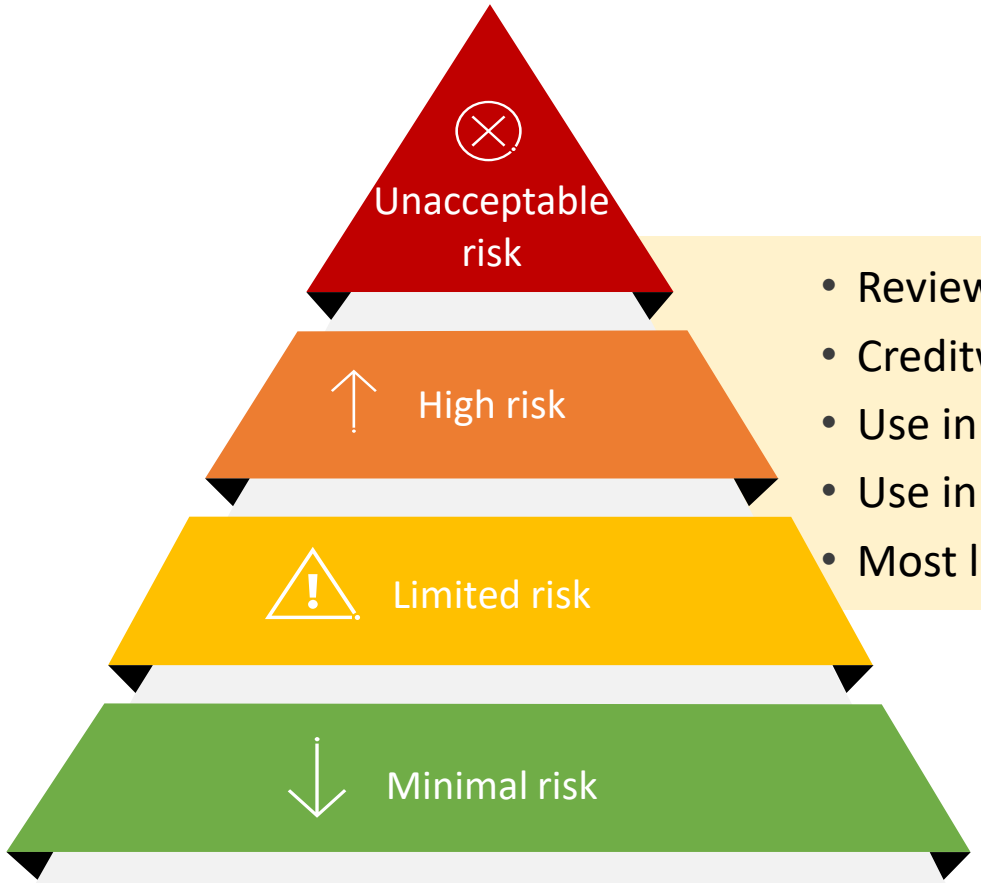
Shared Theme	DORA	NIS2	NIST CSF 2.0
Governance & Oversight	ICT Governance	Management Body	Govern (GV)
Risk Management	ICT Risk Mgmt	Security Measures	Identify (ID)
Incident Response	Incident Reporting	Incident Notification	Detect + Respond
Third-Party / Supply Chain	Third-Party Risk	Supply Chain	Identify (partial)
Resilience & Recovery	TLPT & Testing	Business Continuity	Protect + Recover

IIA's Cybersecurity Topical Requirement

- Effective per February 2026
- Mandatory to apply under IIA's IPPF
- Minimum baseline for assurance and advisory engagement
  - With cybersecurity as a subject
  - With cybersecurity identified as a risk
- 3 Areas: Governance, Risk Management, and Control Processes
- 17 Key Control Criteria
- Maps to NIST CSF

EU AI ACT

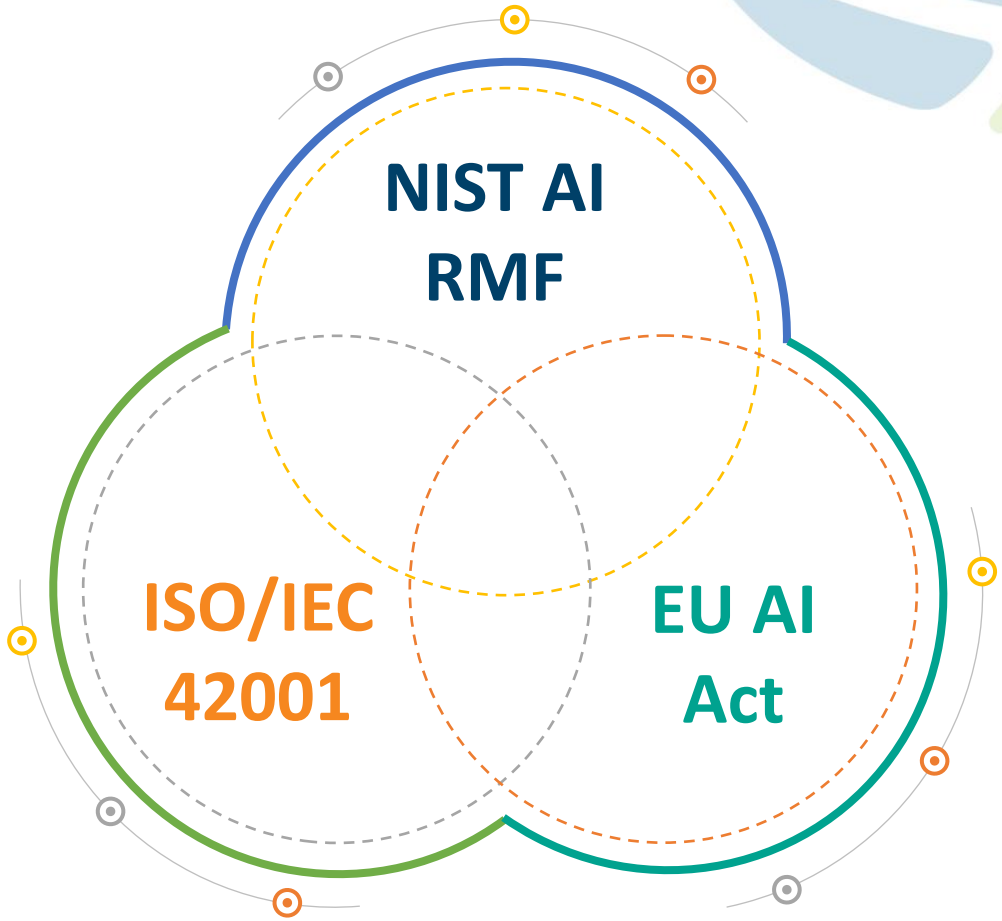
Risk classification



- Review or filter applications that evaluate applicants in interviews or tests
- Creditworthiness checks and credit score evaluations
- Use in critical infrastructure (road traffic, GWE, heat, etc.)
- Use in medical devices
- Most likely, Credit Risk systems, KYC and transaction monitoring systems

Dominant Themes in AI Standards

Safety, Security & Resilience	Transparency & Accountability
Privacy	Ethics & Fairness
Validity & Reliability	Explainability & Interpretability
Data Quality & Integrity	



Mythos: Defending against AI

72%

of Mythos identified vulnerabilities was exploitable

Minutes

of expected exploit time, down from days or weeks

20+ yrs

Age of some long-lived flaws Mythos surfaced

150

Companies in Project Glasswing receiving early access

Why Mythos matters

BEFORE – Security by Friction

Cybersecurity relied on factors that slowed attackers down

Security based on complexity, lack of knowledge, ignorance

Stability of systems was leading

Change was slow, defenders had more time

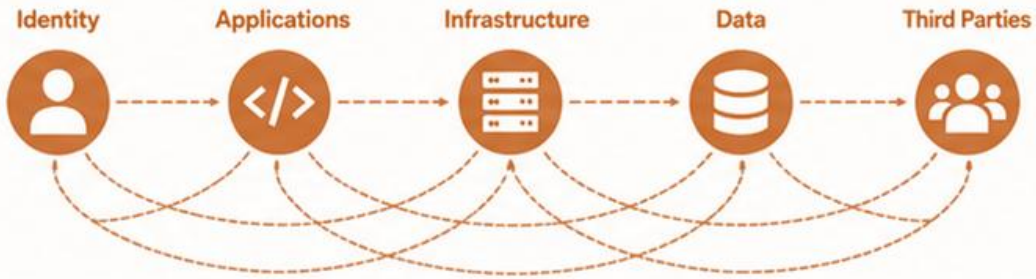
NOW – AI Compresses the Attack Chain

AI systems can now do what used to take humans much longer to achieve

Accelerate exploit pathways from months to days or even hours

Discover vulnerabilities at machine speed and at scale, connecting vulnerabilities elevates the risks

Reason across complex environments turning isolated weaknesses into sophisticated attack paths



Entering a new Era for Cybersecurity

CONSEQUENCES – Resilience must match AI speed

Defenders must assume speed, scale and sophistication

See faster
Continuous visibility into assets, vulnerabilities and attack paths

Decide faster
AI-informed risk prioritization and scenario-based decisions

Respond faster
Automated, orchestrated and measurable response at speed

Era in which AI capability, cybersecurity and digital resilience are increasingly inseparable

How should organizations respond

1

Automate asset inventory updates

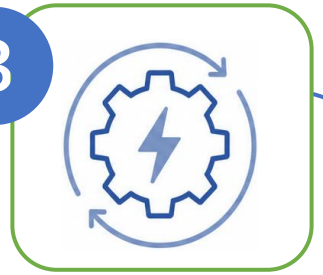
Maintain continuously updated visibility across infrastructure, cloud, SaaS, and AI assets.

2

Reduce technical debt

Legacy systems and outdated dependencies create persistent exposure.

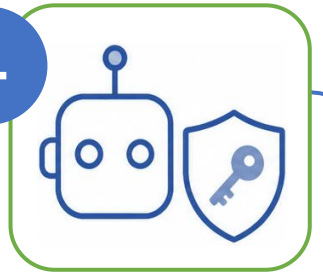
3



Speed up patching and change management

Enable rapid testing, staged rollout, rollback, and emergency change.

4



Treat non-human identities as an attack surface

Govern service accounts, API keys, bots, and AI agents like privileged access.

5

Defend with AI

Use AI for detection, prioritization, triage, and response.

AI Mavericks: Risks when adopting AI

Risky behaviors of AI Mavericks

1. 

Using unapproved AI tools for company work

2. 
Uploading confidential, personal, or client data into public AI tools

3. 
Bypassing IT, procurement, or security review to adopt AI solutions

4. 
Building AI Prototypes without governance, risk, legal, or privacy involvement

5. 
Using AI-generated code, scripts, or content without validation or testing

6. 
Connecting AI tools directly to internal systems or data sources without authorization

7. 
Automating business decisions without human oversight or accountability

8. 
Circumventing policies by using personal accounts, shadow SaaS, or unofficial plugins

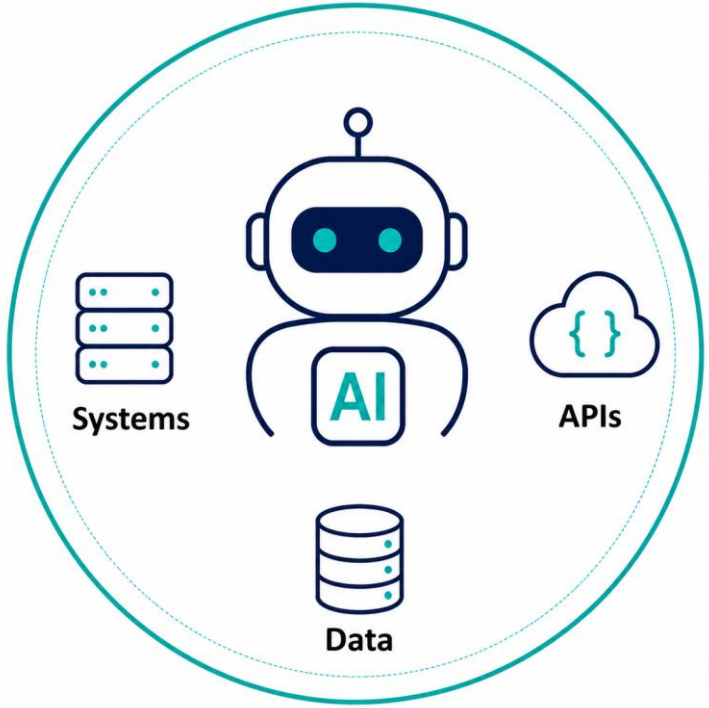
9. 
Relying on AI outputs without checking accuracy, bias, or source quality

10. 
Failing to document AI use cases, owners, risks, and controls

Mavericks and Access Management Challenges

1 **Non-human identities**

2 **Persistent 24/7 access**



3 **Broad permissions**

4 **Segregation of Duties bypass**

Shadow AI

5 **Limited accountability**

Govern AI agents like privileged access — registered, owned, approved, monitored and revocable

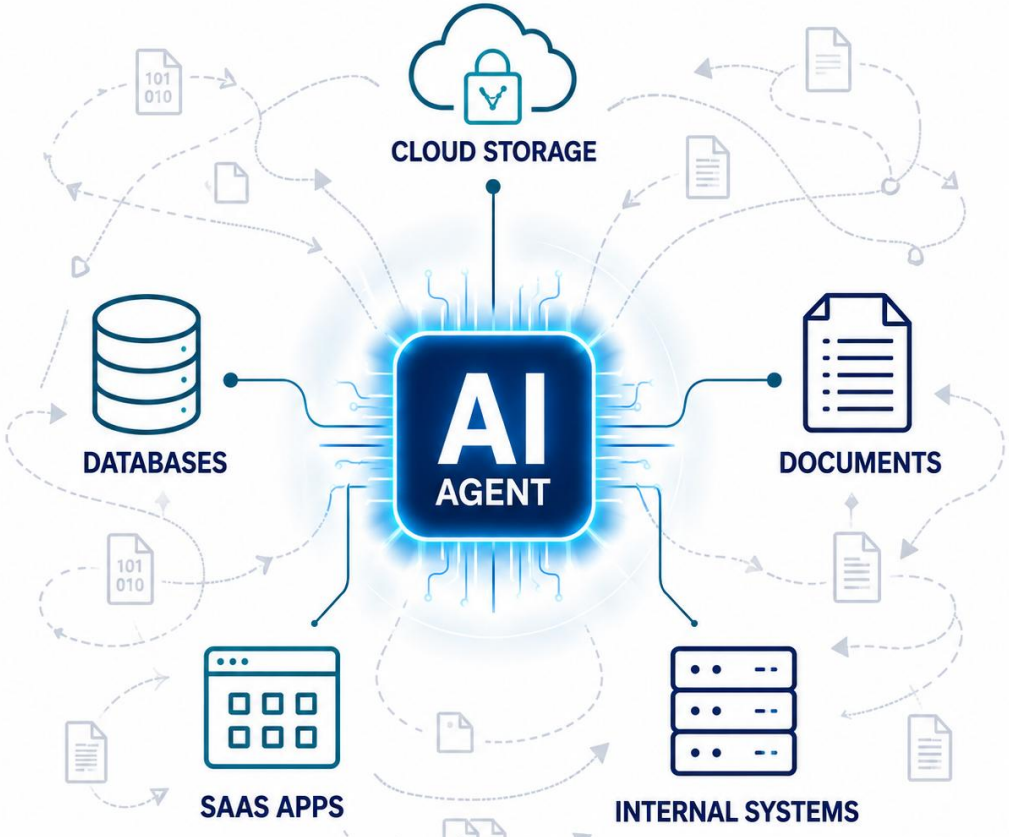
Mavericks and Data Governance Challenges

1. Shadow IT

Copies, outputs and fabricated data outside approved repositories

3. Data Protection

DLP, encryption and access controls may not follow AI-driven data flows



2. Data visibility & classification

Unclear where sensitive data sits, how it is labelled and used

4. Regulated data & retention

Personal, confidential and regulated data is used without clear rules

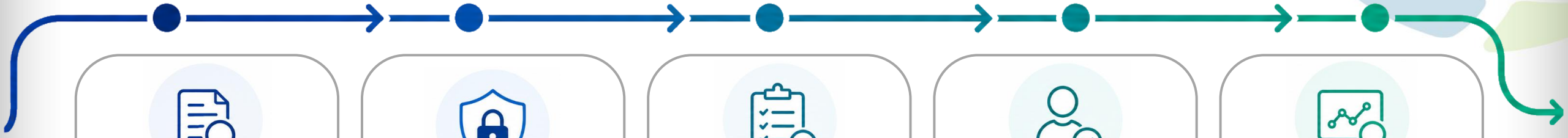
AI amplifies existing data governance issues by creating, copying and moving data faster than controls can follow

The Era of AI risks

AI Risk Management to secure data, ensure trustworthy outcomes, and be compliant—at the same time

Conclusions

From Cyber Risk to AI Governance



Known

Organizations need visibility over where AI is used, by whom, with what data, and for what purpose.

Controlled

AI access to systems, data, APIs, and workflows should be limited, approved, monitored, and aligned with risk appetite.

Validated

AI outputs, decisions, models, and security use cases should be tested for reliability, bias, explainability, security, and resilience.

Accountable

Every AI system or agent should have a clear business owner, risk owner, control owner, and escalation path.

Continuously monitored

AI behavior, data exposure, model drift, prompt injection, misuse, and control degradation should be monitored over time.

Where can you expect AI initiatives

Conversation with Management

Value Identification	Data	Skills	Ecosystem	Experimen-tation	Change Management
Where should we apply AI?	Do we have the data and is it ready?	Do we have the talent we need to unlock the value?	Where to build / buy / partner?	Do we have a capacity to test & learn quickly?	Do we have an organized plan to execute?

Five Audit Focus Areas

01	02	03	04	05
Governance & Risk Oversight	**Audit Plan & Change Readiness**	**IT Asset Management & Attack Surface**	**Vulnerability & Patch Management**	**Containment, Resilience & Recovery**
• Shared CIO/CISO narrative • Audit Committee briefing cadence	• AI governance • Vulnerability management • Patching • Emergency change • Asset inventory • Resilience • Third-party dependencies	• IT Asset inventory • Visibility of shadow resources • Rapidly identify new vulnerabilities	• Vulnerability life-cycle management • Severity and exposure context for prioritization • Exception handling • Management of remediation speed and aging	• Response exercise effectiveness, • Backup restoration • Segmentation and failover, • Rapidly contain-ment of exposure during zero-day or pre-patch scenarios.

Repositioned Internal Audit ahead of the threat

- ✓ A shared view of exposure with the CISO
- ✓ A focused audit plan against the highest-risk disciplines
- ✓ An informed Audit Committee with a tracked metric framework

Key Takeaways

1 AI compresses cyber risk timelines

See faster, decide faster, and respond faster.
AI-accelerated security, asset and patch management.

2 Agentic AI creates new control challenges

Shadow AI, Shadow data, models, and security use cases should be tested for reliability, bias, explainability, security, and resilience.

3 Internal Audit must evolve assurance

AI access to systems, data, APIs, and workflows should be limited, approved, monitored, and aligned with risk appetite.

Tjakko de Boer RE CIA

Managing Director Technology Consulting

Tjakko.deboer@protiviti.com

protiviti®

Scan to link on LinkedIn

Instituut van Internal Auditors Nederland

IIA CONGRES 2026 PRIDE & PREJUDICE 4 & 5 JUNI AFAS THEATER LEUSDEN