

Auditor of the Future



*Every radical
technology
erases a
profession*



Linda Nyvelius

- Lawyer
- IIA Sweden CEO
- BR1GHT – Elevating GRC with top technology and domain knowledge
- Exclusive partner to TeamMate in the Nordics



Linda Nyvelius

Director Nordics
BR1GHT

Linda.Nyvelius@br1ght.eu



We stand out by focusing on driving technological improvements in all corporate governance areas. Our unique blend of skills allows us to provide strategic guidance while achieving operational enhancements. Therefore, we add value at every level in organisations. Through co-sourcing, delivered from our global service centers, we consistently boost quality and reduce control costs.

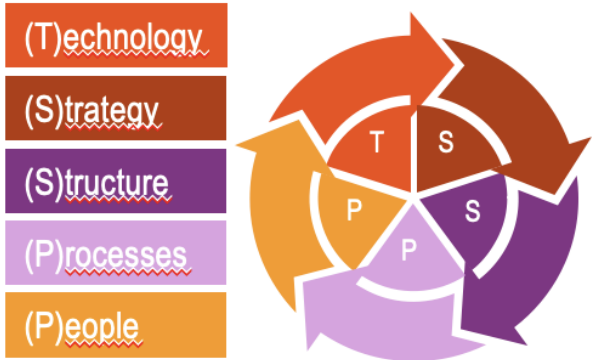


Our services

| | | |
|------------|------------|-------------|
| Technology | Consulting | Co-sourcing |
| | | |

Our methodology

Vision driven people enabling technology improvements: 5 elements working together.



Our beliefs

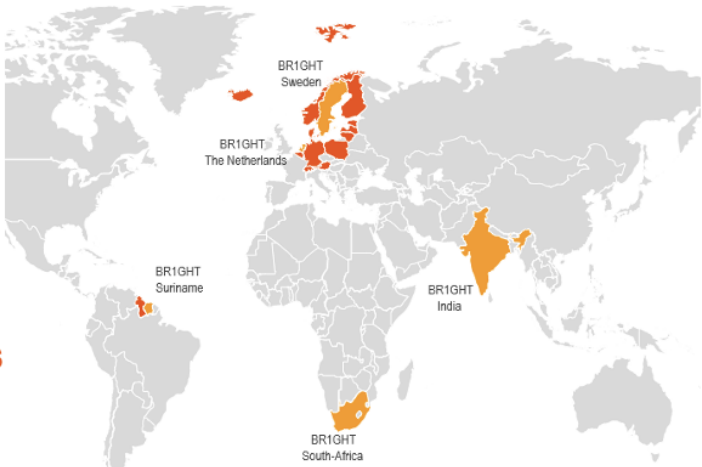
Our values binding us together

- Care from the heart
- One in divers1ty
- Develop yourself and the world
- Trust upfront
- Fun is more than a word
- Challenging leads to evolving

Where we stand

Our figures

- 90+ customers
- 14 countries
- 5 regional offices
- 2 service centres
- 3 governance areas
- 40+ specialists
- 13 core team members
- 17 business partners



FIRST LINE

Controls

SAP-control technology selection and implementation

Finance technology (CPM) selection

SAP-control consulting

Controls implementation and automation

Flexible (SAP) control staff

Controls executing co-sourcing

SECOND LINE

Risk & Compliance

GRC technology selection, implementation, and enhancement

Strategic GRC support for boards

Best practice risk & compliance operations

Flexible GRC staffing

Co-sourcing of risk & compliance

THIRD LINE

Audit

AMS selection, TeamMate implementation & enhancement

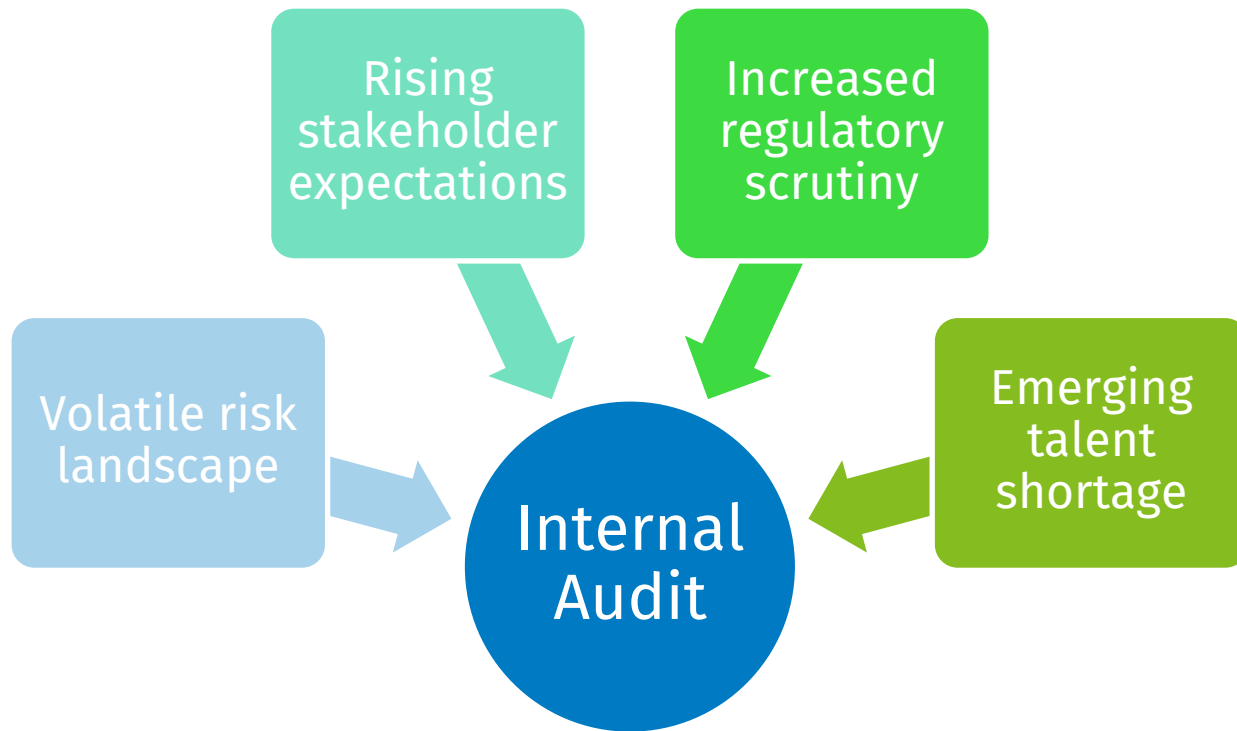
Strategic support to CAE & board(s)

Operational improvement Internal Audit

Auditors and CAE ad-interim

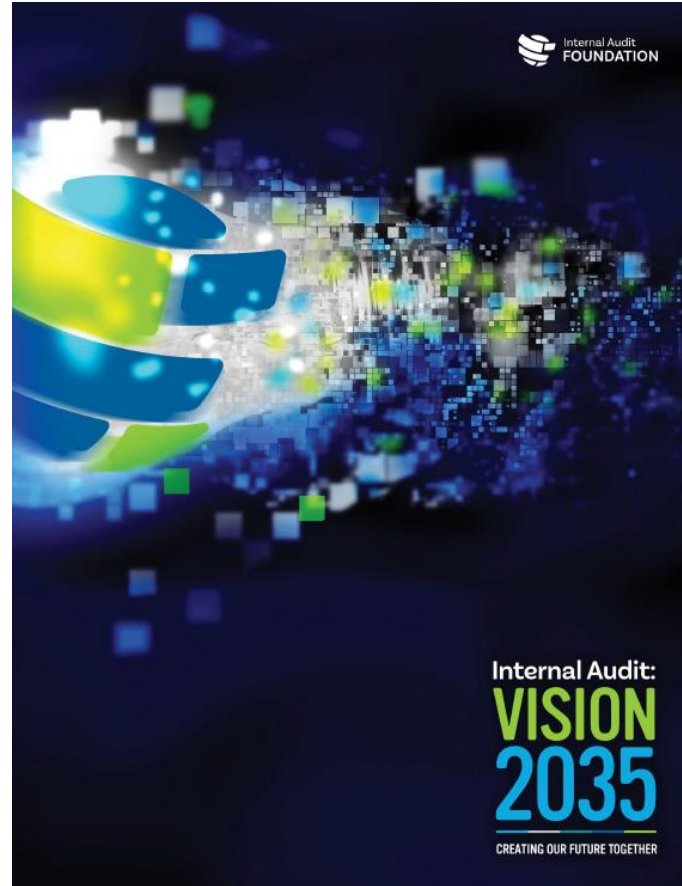
Co-sourcing of Internal Audit

Why should technology be on top of mind?



- Create a free flow of relevant and accurate information
- Cooperate with other assurance providers
- Let humans do what only humans can do – automate everything else

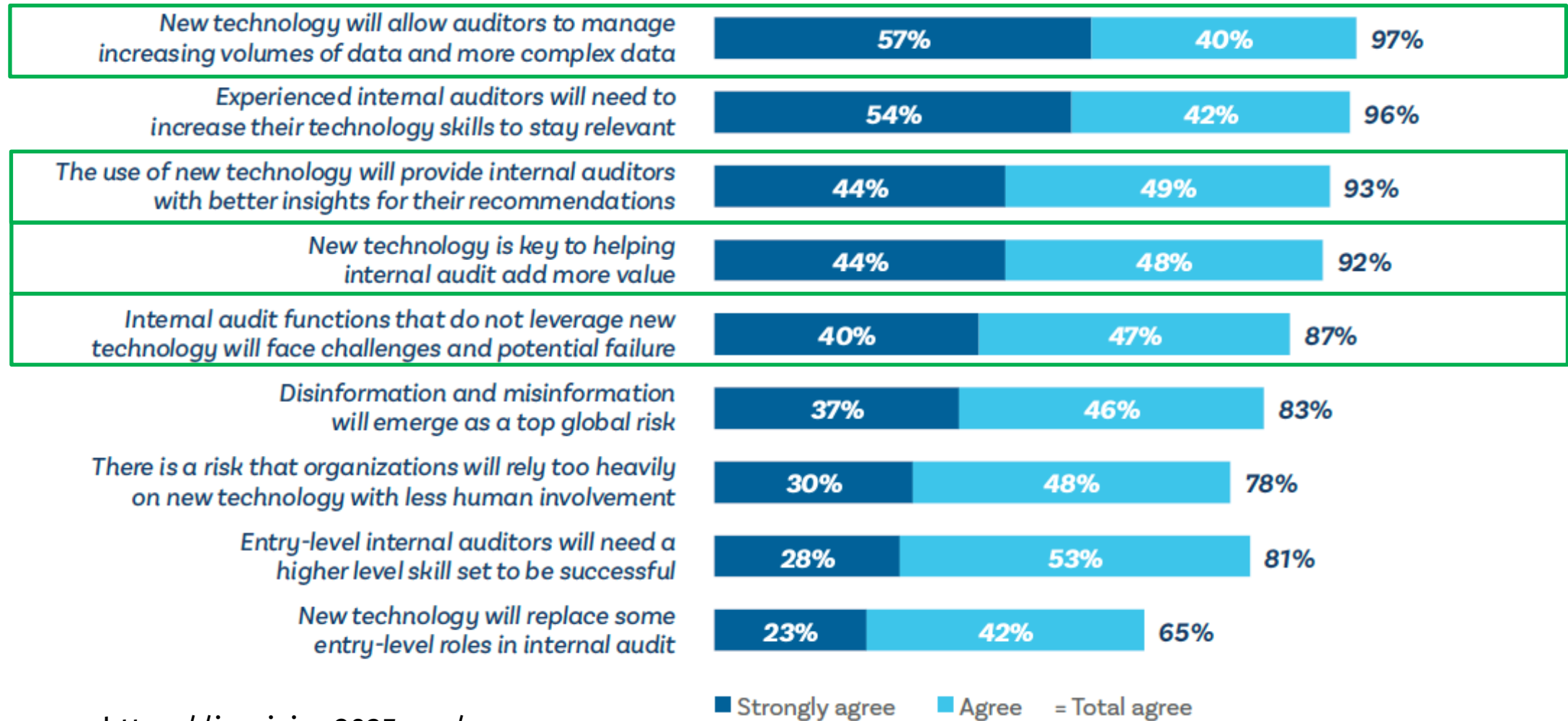
Internal Auditing in the Future: Vision 2035



<https://ia-vision2035.org/>

- Quantitative and qualitative research carried out globally over a 12-month period
 - IIA members
 - Internal Audit Leaders
 - Board and Audit Committee
 - Senior Executives
 - Regulators and other stakeholders
- More than 7000 contributors

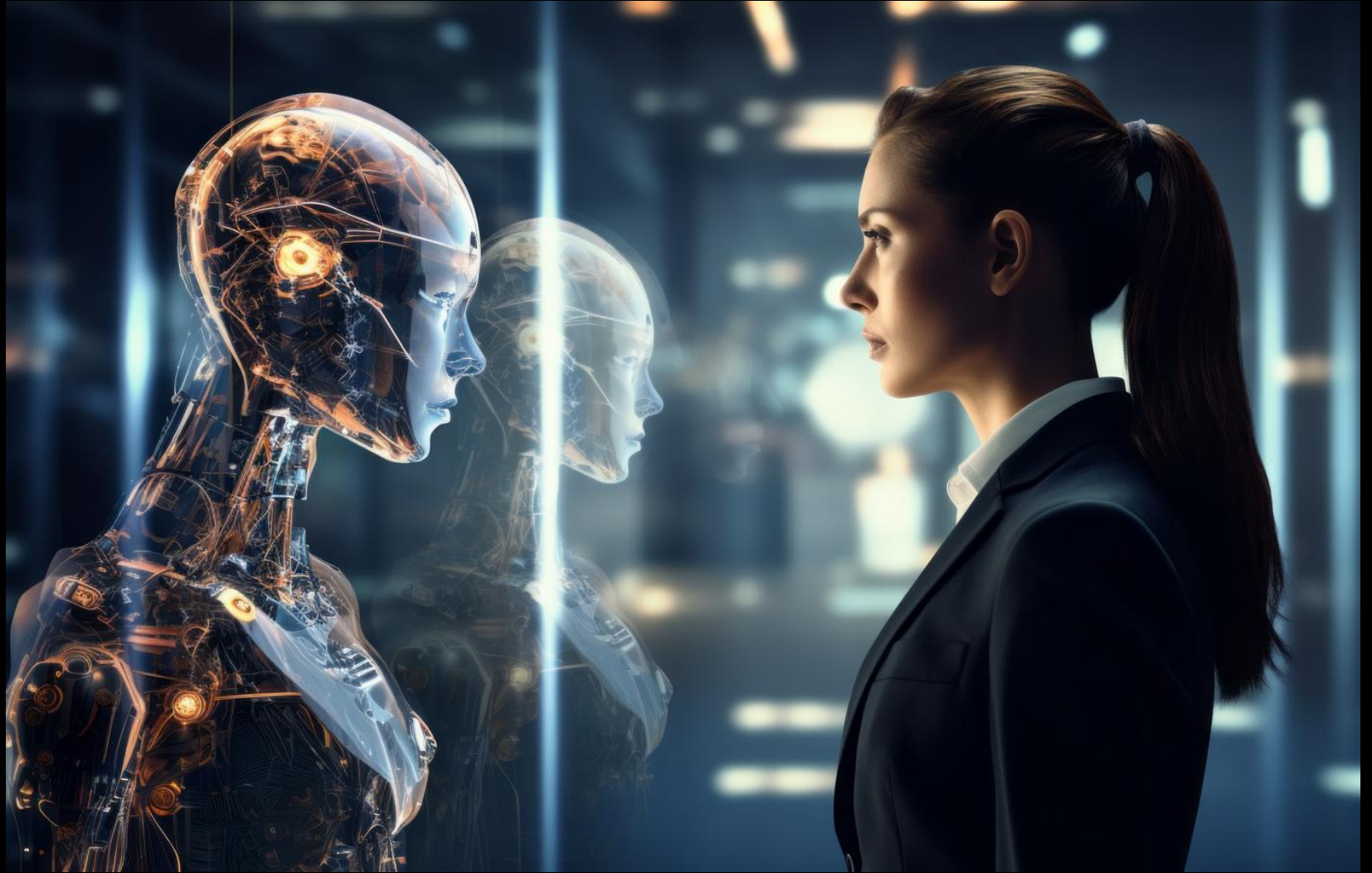
New Technologies' Impact on the Future of Internal Audit



<https://ia-vision2035.org/>

Auditor of the Future, Oslo, May 2025

What is AI really?

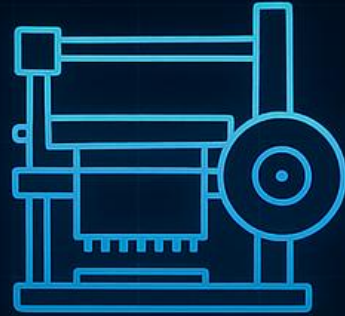


“Just” another disruptor

AGRICULTURE



INDUSTRIAL
REVOLUTION



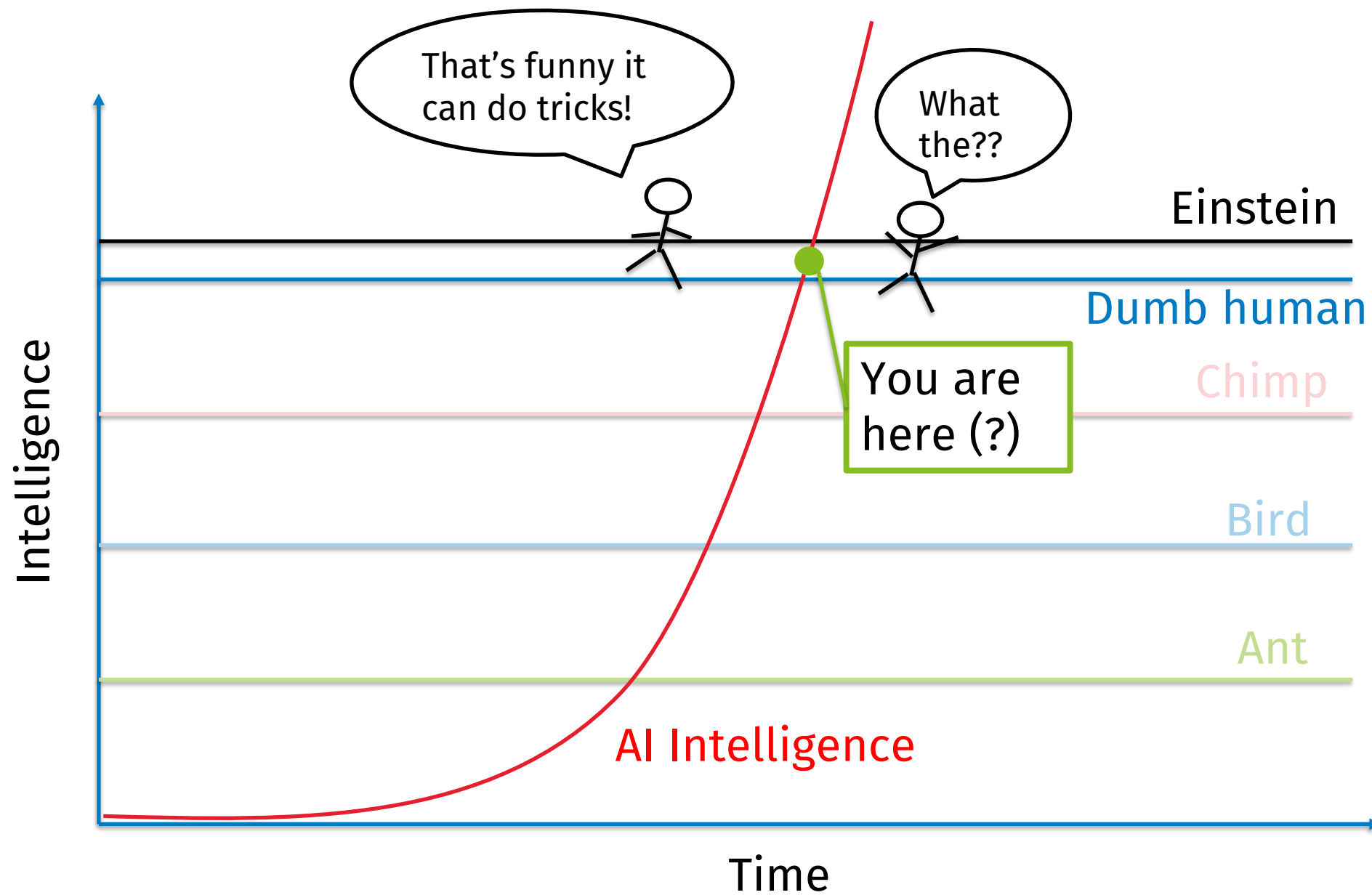
INTERNET



ARTIFICIAL
INTELLIGENCE



...or is it different this time?



Intelligence?

- 1950s: Rule based systems

```
if (hour >= 5 && hour < 12) {  
    System.out.println("Good morning!");  
} else if (hour >= 12 && hour < 18) {  
    System.out.println("Good afternoon!");  
} else {  
    System.out.println("Good evening!");  
}
```

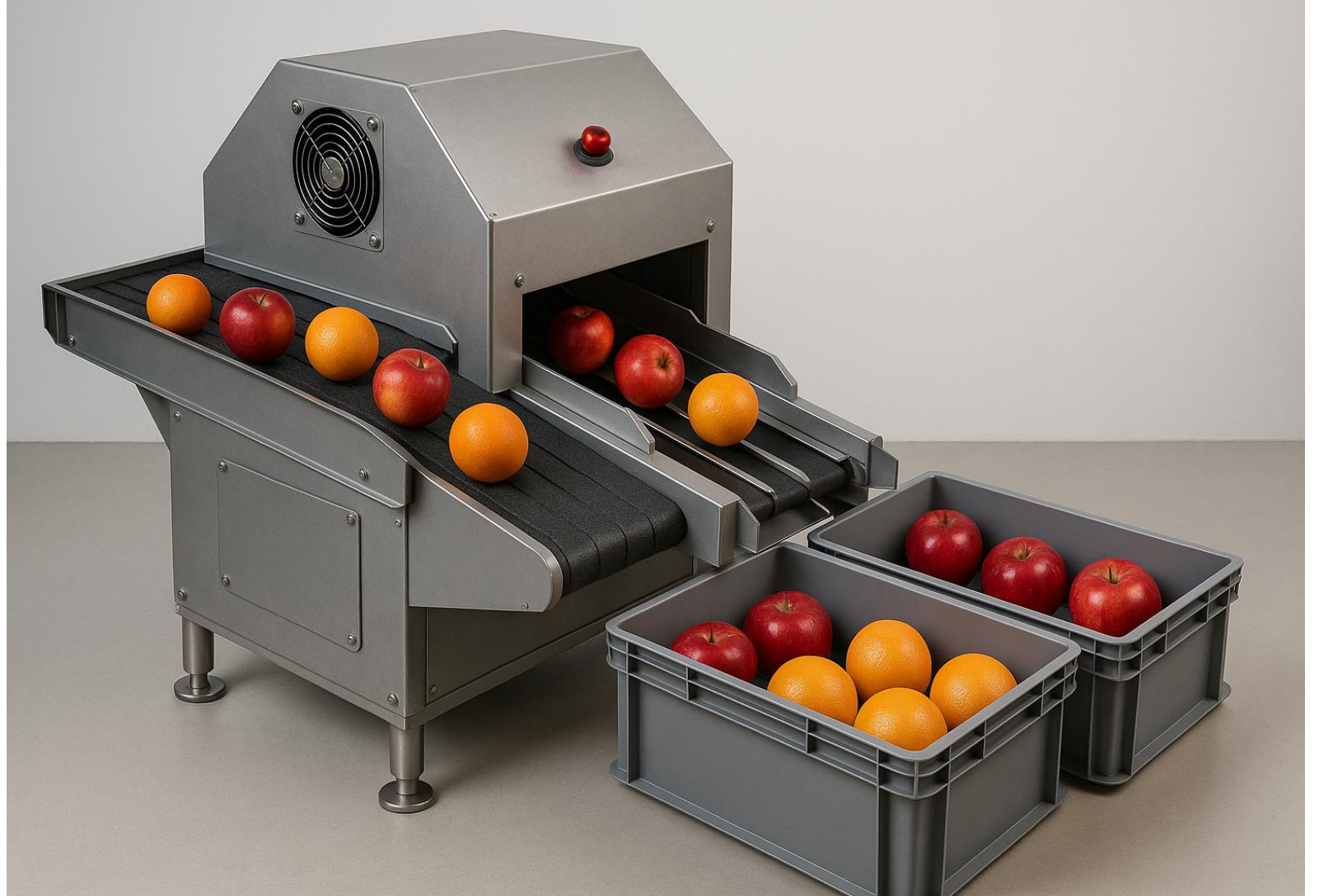
- 1990s:
Binary search

```
public static int binarySearch(String[] names, String target) {  
    int left = 0;  
    int right = names.length - 1;  
  
    while (left <= right) {  
        int middle = (left + right) / 2;  
        int comparison = target.compareTo(names[middle]);  
  
        if (comparison == 0) {  
            return middle; // Found the name!  
        } else if (comparison < 0) {  
            right = middle - 1; // Look to the left  
        } else {  
            left = middle + 1; // Look to the right  
        }  
    }  
  
    return -1; // Not found  
}
```


Intelligence?



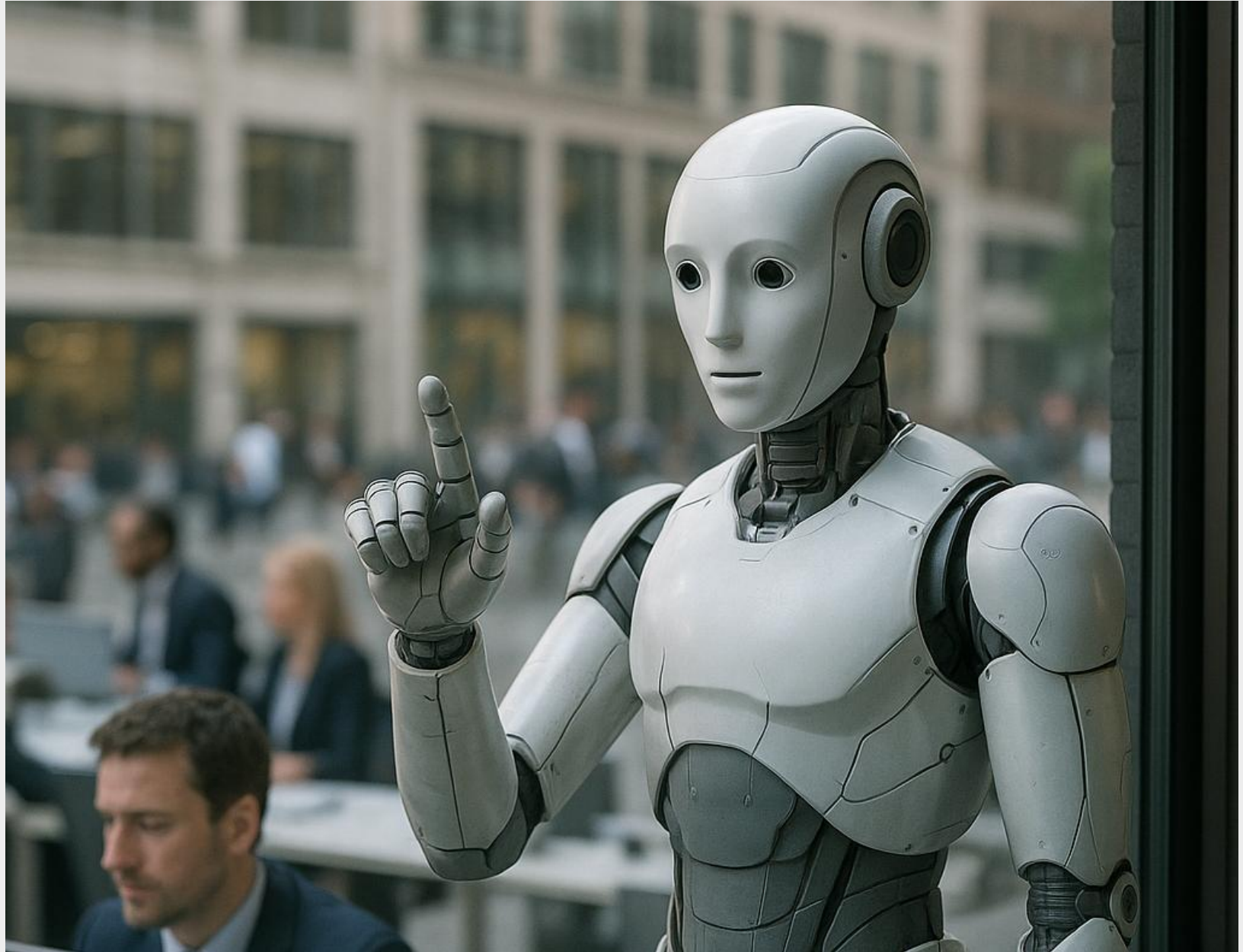
Intelligence?



Intelligence?

- LLMs that can now act as:
 - Lawyers (Passed Uniform Bar Exam)
 - Therapists (Passed National Clinical Mental Health Counselling Examination)
 - Doctors (Passed all parts of exams in USA and Korea)
 - Authors of books
 - Interior designer
 - Etc....

Intelligent but
not conscious...
and looking for a
position on your
team!



Advice on how to start applying AI

Things to take advantage of



It's always available and eager

An assistant at your fingertips – day and night, never gets tired, never gets offended.



Great at context-based search

It can do research and summarize great amounts of data in a short time.



It can even “reason” and create

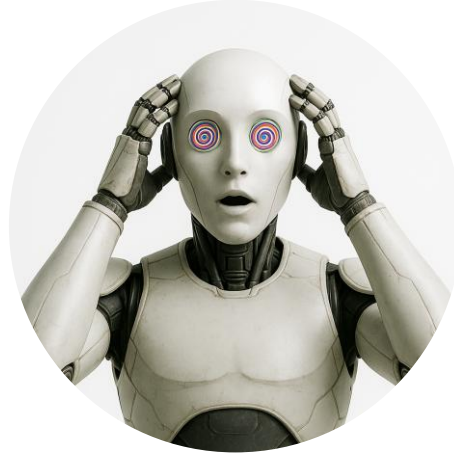
It can get your work 80% done and then you can course correct, fact-check and take it to the next level. Save time compared to starting on a blank page.

Things to think about



It's confident

It does not know what it does not know and can speak with great authority that is not always warranted.



It tends to hallucinate

"I don't know" is not part of its vocabulary so it tends to make things up.



It's Enthusiastic

Whatever you say, it will agree wholeheartedly and very flattering. It will follow where you lead, even in the wrong direction.

Risks and mitigations

- Hallucinations
 - Human in the loop
 - Transparency
 - Feedback loop
- Black box
 - Click-through to reasoning
 - Sources clearly stated
- Poor data input
 - Define sources
 - Source credibility scoring
 - Sort out dated information
- Sensitive data leaks
 - Never expose data to open models
 - Boxed off models
 - Local LLMs
 - PII blockers
- Over-trusting the models
 - Human sign-offs and checkpoints
 - Training in limitations
 - Disclaimers

Adoption of GenAI by the Internal Audit Profession

TeamMate Partnered with the IIA Global Research Foundation to Understand Use Cases for Generative AI



Solving the riddle:

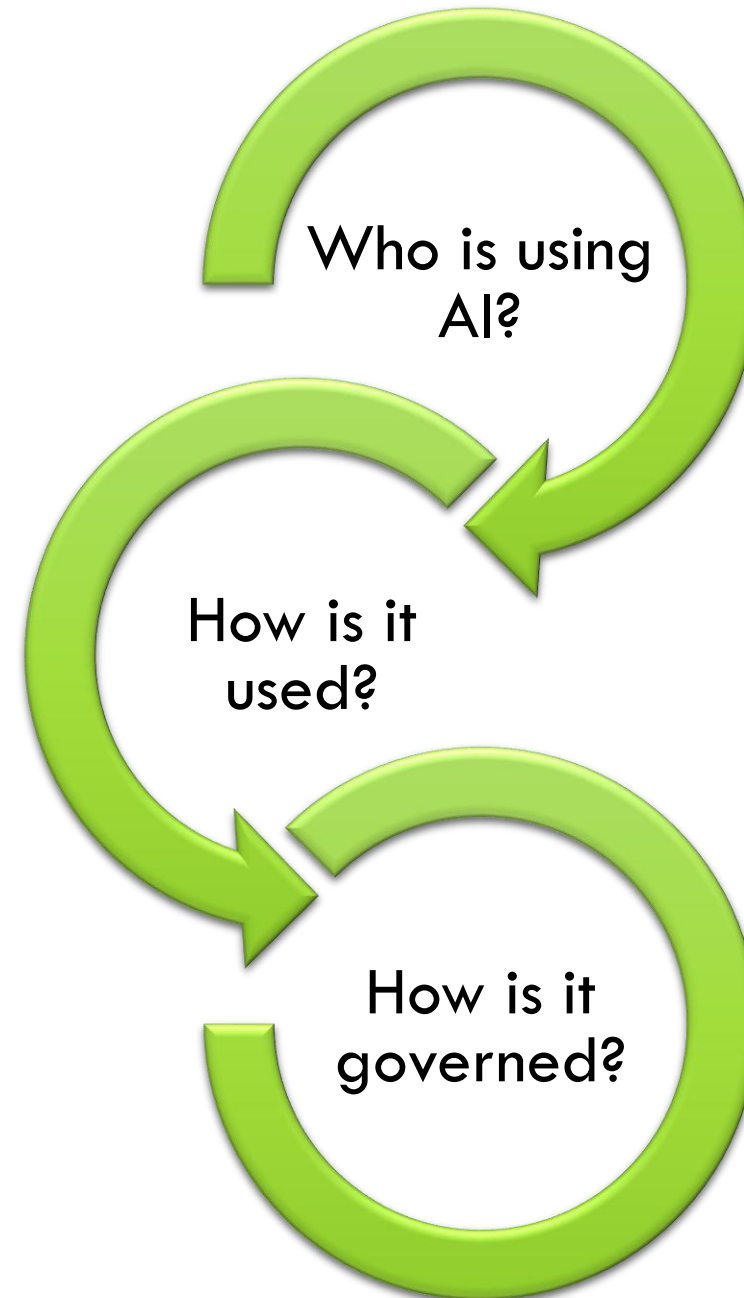
Harnessing Generative AI
for internal audit activities



<https://www.theiia.org/en/content/research/foundation/2024/solving-the-riddle-harnessing-generative-ai-for-internal-audit-activities/>

- Survey of IIA Global members
- Understand adoption by IIA members
- Results driving roadmap for delivery in TeamMate+

Survey Objectives



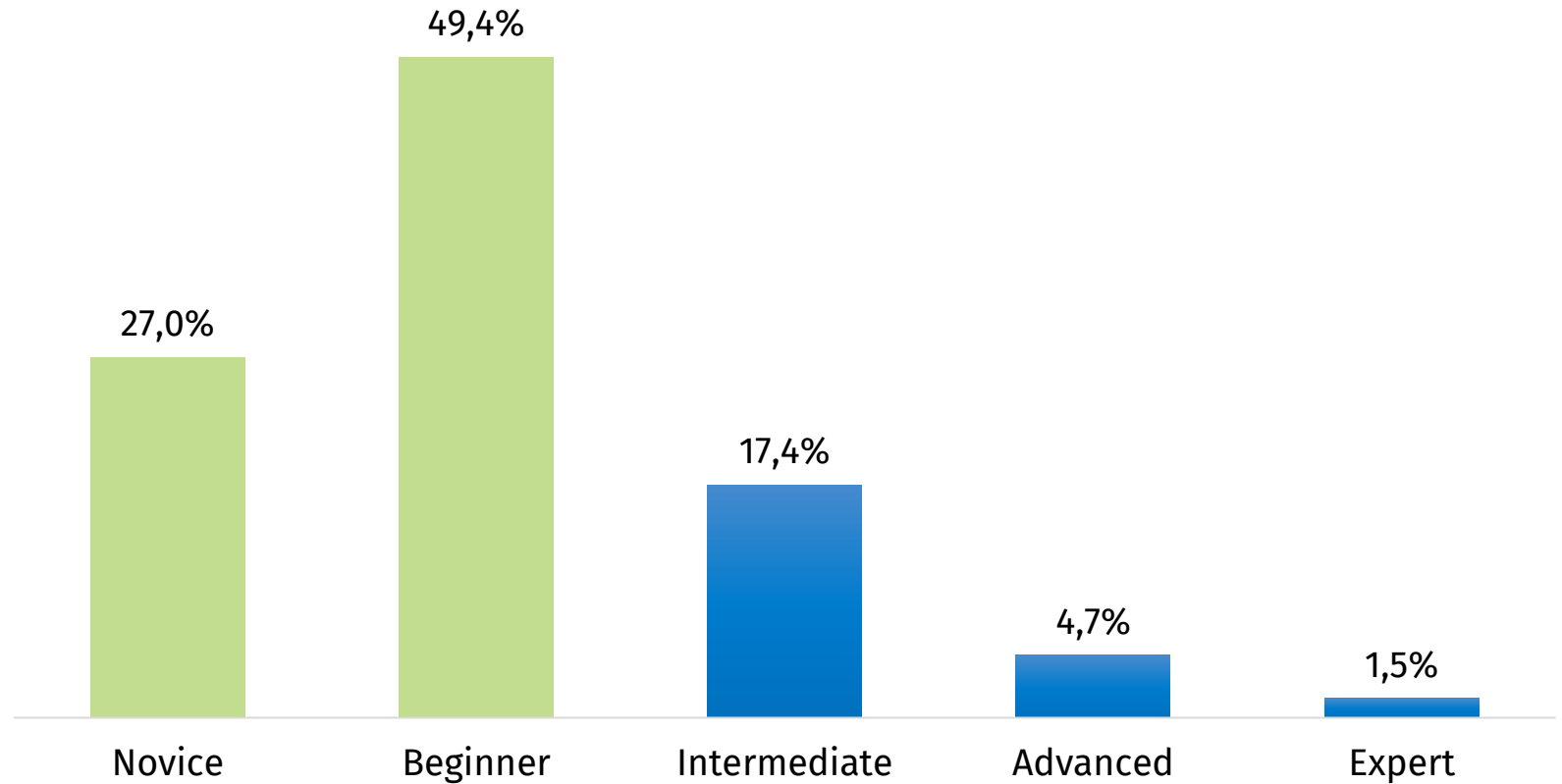
Ideas being built and integrated through APIs

- **Spot common patterns across hundreds of issues automatically.**
Let AI review large volumes of issues to identify recurring problems or themes, instead of doing it manually.
- **Get suggestions for resolving findings, based on what worked before.**
Use AI to match new issues with similar past cases and show which actions were effective.
- **Keep TeamMate and other systems like JIRA in sync.**
If you create an issue in TeamMate, it can show up automatically in JIRA (or the other way around), reducing double work.
- **Bulk edit audit data easily.**
Export issues from TeamMate to Excel, update them in bulk, and upload them back—no manual editing one by one.
- **Ask questions about company policies and get instant answers.**
Upload your policies and use an AI chatbot to answer questions, like “Can I expense this on my work trip?”

Individual Knowledge and Use of GenAI

76%
rate themselves
as novices or
beginners

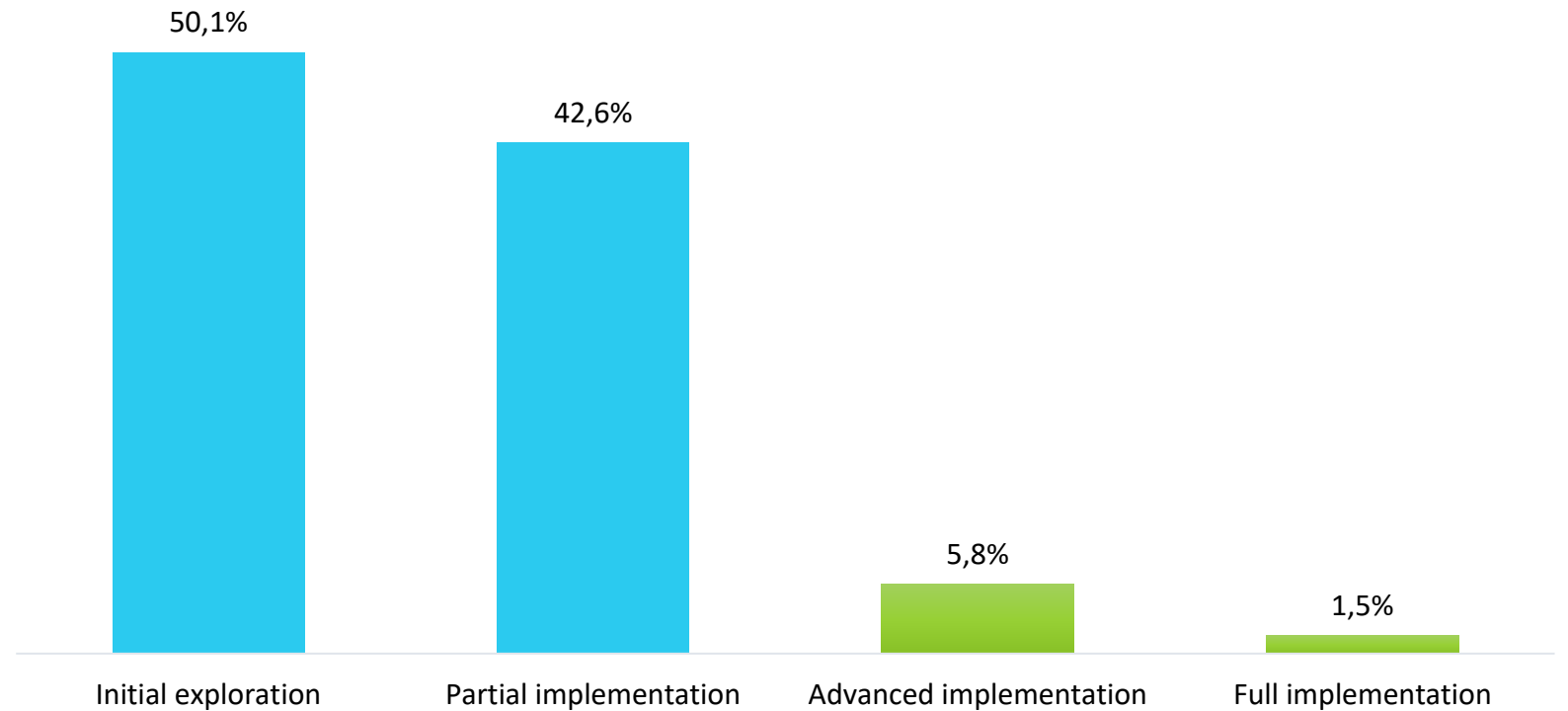
Proficiency and Personal Use of GenAI in Professional Role



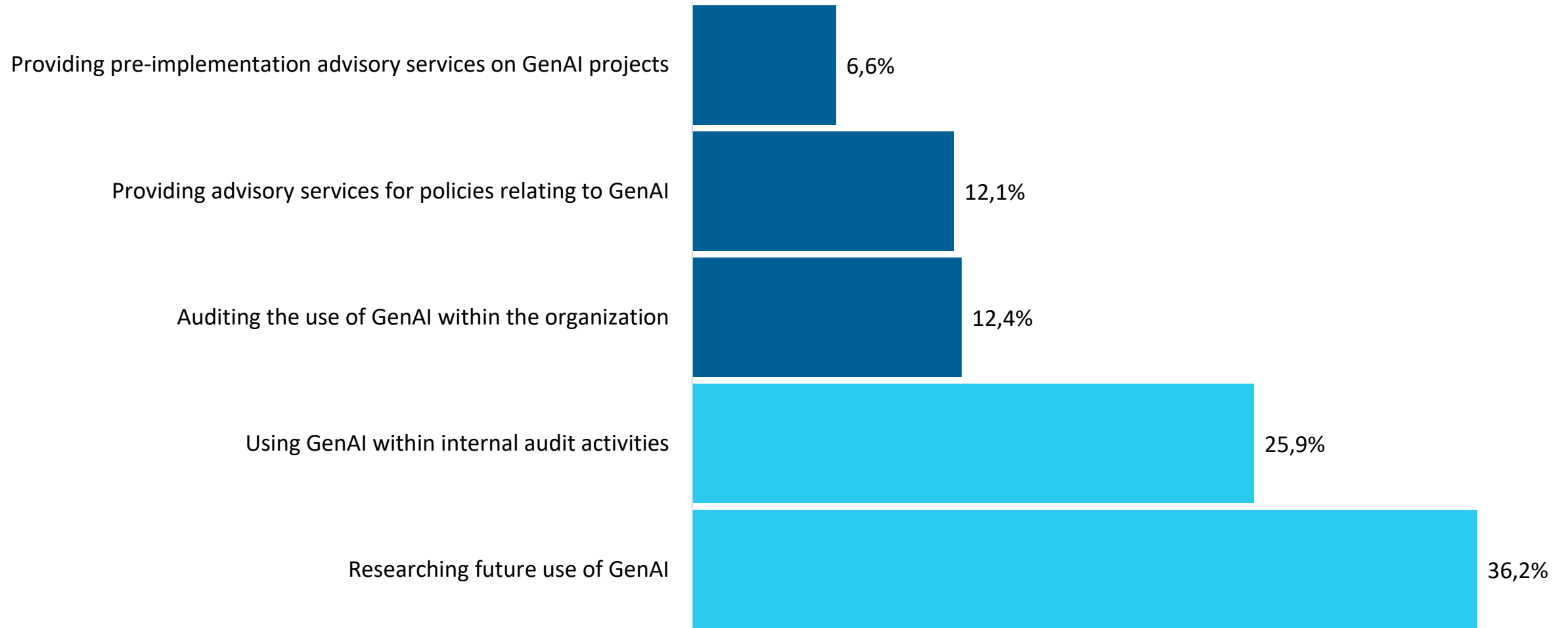
Adoption within the Organization

93%
adoption is in
initial exploration
or partial
implementation

Organization Maturity Level of GenAI Adoption

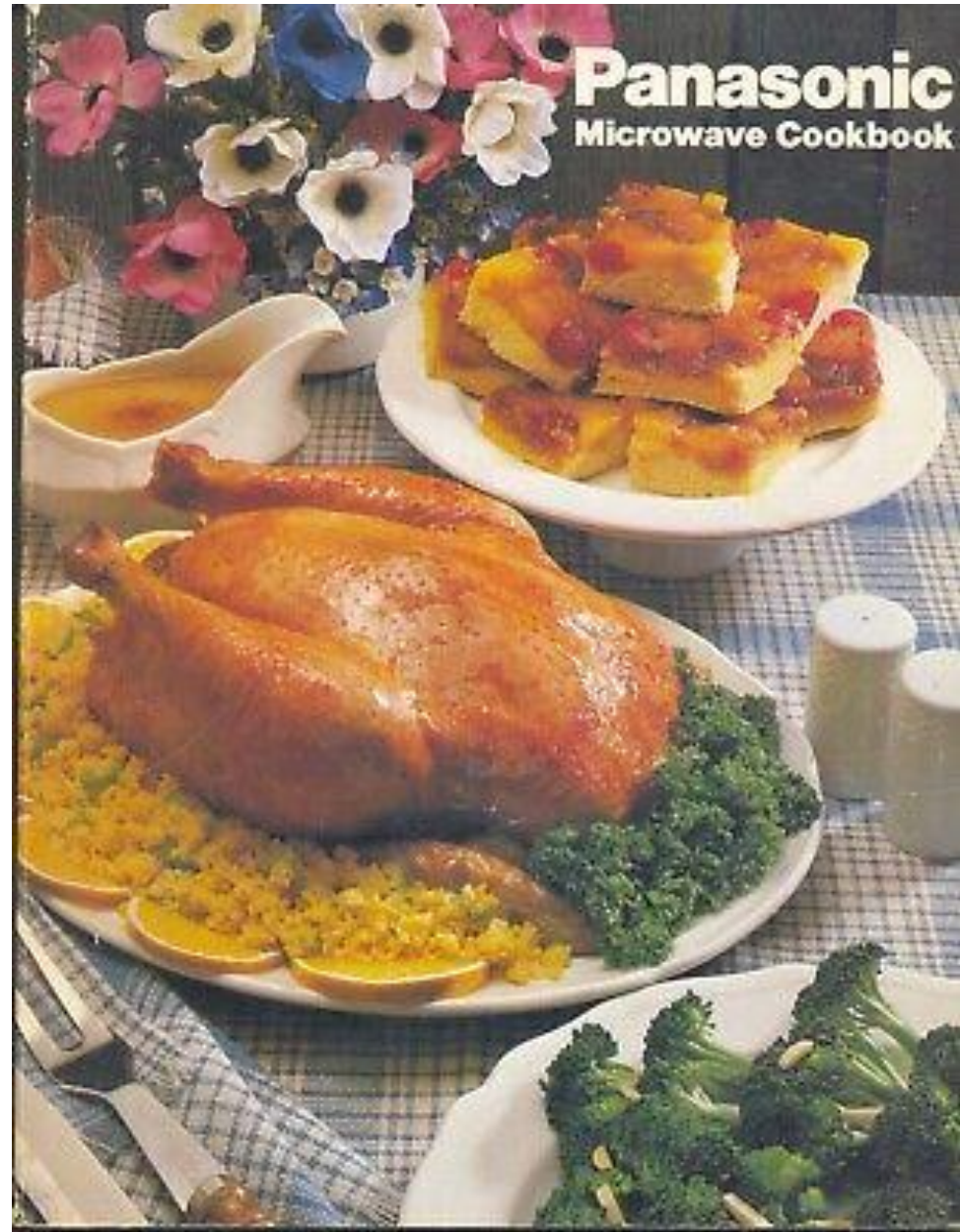


Internal Audit Involvement in GenAI Activities



Next steps: What
can I do?

Get to know its potential – and limitations



Embedding GenAI in TeamMate+

Use Cases Across All Phases of the Audit Cycle



Learning: GenAI can help practitioners learn about potential audit subjects and issues.



Brainstorming: With effective prompting, GenAI can deliver impressive ideation for audit work in all engagement phases.



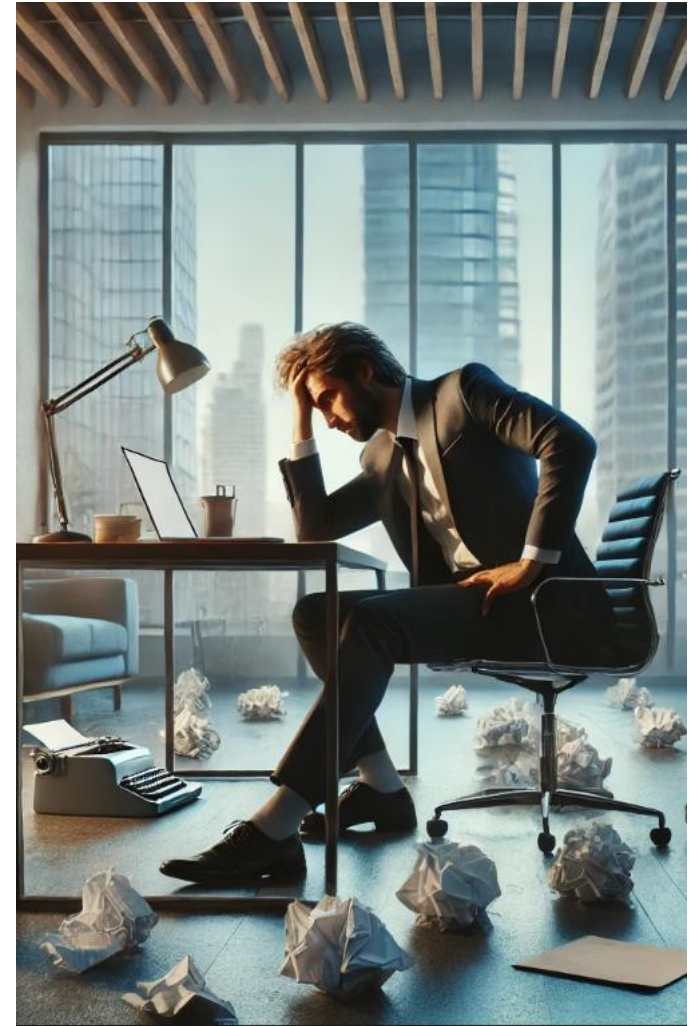
Building: GenAI can help build frameworks, questionnaires, and other commonly used tools.



Writing: GenAI can readily improve communications of issues and recommendations by assuring emails, information requests, reports, follow-ups and other communications are concise, accurate and relay the proper tone.

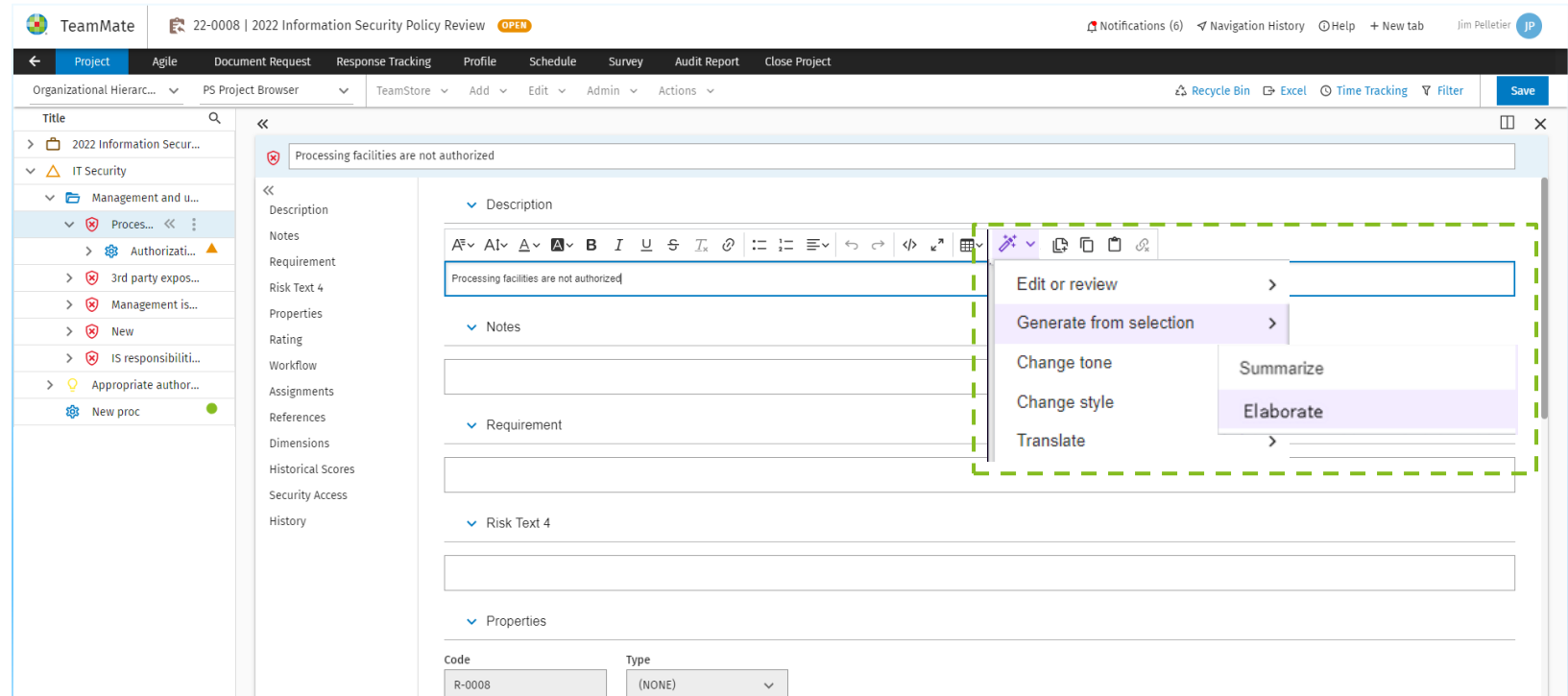
TeamMate+ Generative AI: Writing Engine

- Auditors often waste valuable time writing, editing, and rewriting workpapers and audit findings, leading to unnecessary effort and causing audits to exceed deadlines
- Consistency of writing varies across teams impacting quality and stakeholder satisfaction



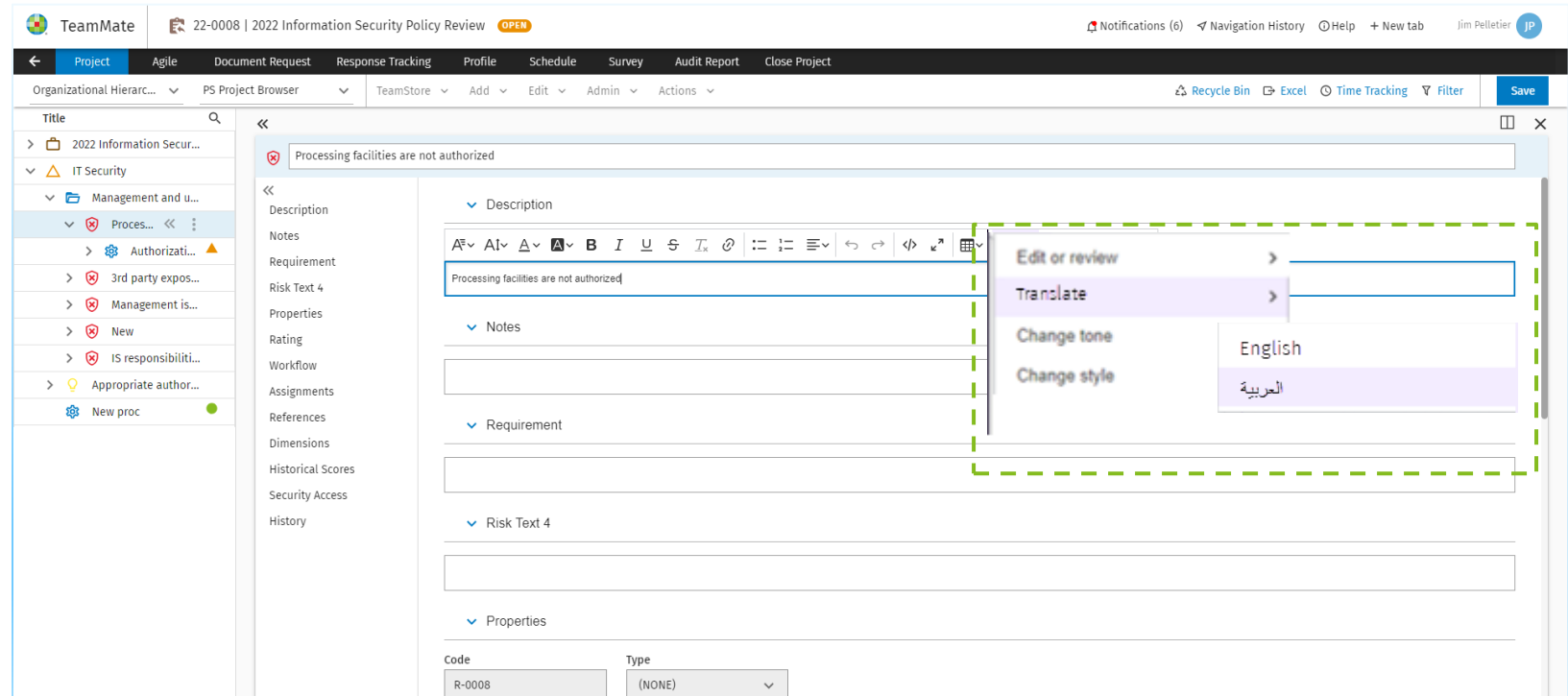
ChatGPT DALL E

TeamMate+ Generative AI: Writing Engine



- Leverage GenAI to draft narratives, improve writing, summarize or expand existing content, support consistency across teams
- Incremental time savings and improved quality at the individual auditor level will quickly translate into a significant productivity boost for the team

TeamMate+ Generative AI: Writing Engine



- Leverage GenAI to translate text reducing time when working on audits over entities which operate in different languages
- Organisational data remains isolated so is not available to 3rd parties or used to train the model reducing risk

Use case 1: Summarize text

TeamMate

WK 099 | Satinalma Auditi

Open

Notifications (2)

Recent Activity

Help

New tab

Michal Dutkiewicz

Project

Profile

Schedule

Audit Report

Close Project

Organization Hierarchy

Project Browser

TeamStore

Add

Edit

Admin

Actions

Excel

Filter

Title

Satinalma Auditi

IT Security

Control 1

Conflict of Interest

Improper segregation of duties

Conflict of Interest

Exec Summary

Finding

Exec Summary

Condition

Cause

Consequence

Workflow

Assignments

References

Dimensions

Security Access

History

Role and Functions of Financial Internal Audit

Risk Management

A core function of internal audit is the identification and management of financial risks. This includes assessing risks related to inaccurate financial reporting, fraud, non-compliance with laws and regulations, and operational inefficiencies. Auditors review the financial practices of the organization to identify areas of potential risk and ensure that effective mitigation strategies are in place.

Internal Controls Evaluation

Internal controls are policies and procedures established by an organization to ensure the accuracy and integrity of its financial reporting and safeguard assets. Internal auditors evaluate these controls to ensure they are functioning as intended and that they are adequate to prevent errors, fraud, and operational inefficiencies. For instance, an audit might focus on the segregation of duties, ensuring that no individual has control over all aspects of a financial transaction, which helps prevent fraudulent activities.

Compliance Assurance

An essential part of financial internal auditing is ensuring that the organization complies with relevant laws, regulations, and internal policies. This includes adherence to financial reporting standards (such as IFRS or GAAP), tax laws, and other industry-specific regulations. Auditors may check for compliance with anti-money laundering regulations, the Foreign Corrupt Practices Act, or other relevant legal frameworks.

Fraud Detection and Prevention

Internal auditors are trained to detect irregularities and discrepancies in financial data that may indicate fraudulent activities, such as financial manipulation, embezzlement, or misuse of funds. Through thorough examination of financial records, transaction trails, and operational practices, auditors are able to identify potential fraudulent activities. Furthermore, internal auditors recommend measures to prevent future fraud, such as the implementation of stronger access controls or more frequent audits.

Use case 1: Summarize text

TeamMate

WK 099 | Satinalma Auditi

Open

Notifications (2)

Recent Activity

Help

+ New tab

Michal Dutkiewicz

Project

Profile

Schedule

Audit Report

Close Project

Last Saved: 3:00

Organization Hierarchy

Project Browser

TeamStore

Add

Edit

Admin

Actions

Excel

Filter

Title

Satinalma Auditi

IT Security

Control 1

Conflict of Interest

Improper segregation of duties

Conflict of Interest

Exec Summary

Findings

Exec Summary

Condition

Cause

Consequence

Workflow

Assignments

References

Dimensions

Security Access

History

Internal Audit

Summarize

Continue

Internal risk and ensure that effective mitigation strategies are in place.

Internal Controls Evaluation

Internal controls are policies and procedures established by an organization to ensure the accuracy and integrity of its financial reporting and safeguard assets. Internal auditors evaluate these controls to ensure they are functioning as intended and that they are adequate to prevent errors, fraud, and operational inefficiencies. For instance, an audit might focus on the segregation of duties, ensuring that no individual has control over all aspects of a financial transaction, which helps prevent fraudulent activities.

Compliance Assurance

An essential part of financial internal auditing is ensuring that the organization complies with relevant laws, regulations, and internal policies. This includes adherence to financial reporting standards (such as IFRS or GAAP), tax laws, and other industry-specific regulations. Auditors may check for compliance with anti-money laundering regulations, the Foreign Corrupt Practices Act, or other relevant legal frameworks.

Fraud Detection and Prevention

Internal auditors are trained to detect irregularities and discrepancies in financial data that may indicate fraudulent activities, such as financial manipulation, embezzlement, or misuse of funds. Through thorough examination of financial records, transaction trails, and operational practices, auditors are able to identify potential fraudulent activities. Furthermore, internal auditors recommend measures to prevent future fraud, such as the implementation of stronger access controls or more frequent audits.

Use case 1: Summarize text

TeamMate

WK 099 | Satinalma Auditi

Open

Notifications (2)

Recent Activity

Help

+ New tab

Michał Dutkiewicz

Project

Profile

Schedule

Audit Report

Close Project

Organization Hierarchy

Project Browser

TeamStore

Add

Edit

Admin

Actions

Excel

Filter

Title

Satinalma Auditi

IT Security

Control 1

Conflict of Interest

Improper segregation of duties

Conflict of Interest

Exec Summary

Condition

Cause

Consequence

Workflow

Assignments

References

Dimensions

Security Access

History

Role and Functions of Financial Internal Audit

Risk Management

A core function of internal audit is the identification of financial reporting, fraud, non-compliance with laws and regulations, and operational inefficiencies. Auditors assess the organization's financial practices to pinpoint potential risks and ensure effective mitigation strategies are implemented.

Internal Controls Evaluation

Internal controls are policies and procedures established to safeguard assets. Internal auditors evaluate these controls for effectiveness. For instance, internal auditors may check for compliance with anti-money laundering controls over all aspects of a financial transaction, fraud, and operational inefficiencies. Furthermore, internal auditors recommend measures to prevent future fraud, such as the implementation of stronger access controls or more frequent audits.

Compliance Assurance

An essential part of financial internal auditing is ensuring compliance with applicable laws and regulations. This includes adherence to financial reporting standards and internal policies. Internal auditors may check for compliance with anti-money laundering controls over all aspects of a financial transaction, fraud, and operational inefficiencies. Furthermore, internal auditors recommend measures to prevent future fraud, such as the implementation of stronger access controls or more frequent audits.

Fraud Detection and Prevention

Internal auditors are trained to detect irregularities, manipulation, embezzlement, or misuse of funds. Through thorough examination of financial records, transaction trails, and operational practices, auditors are able to identify potential fraudulent activities. Furthermore, internal auditors recommend measures to prevent future fraud, such as the implementation of stronger access controls or more frequent audits.

AI Editor

Role and Functions of Financial Internal Audit

Risk Management

The primary role of internal audit involves identifying and managing financial risks, including those associated with inaccurate financial reporting, fraud, non-compliance with laws and regulations, and operational inefficiencies. Auditors assess the organization's financial practices to pinpoint potential risks and ensure effective mitigation strategies are implemented.

Replace

Insert below

Try again

Stop

AI-generated content may be incorrect.

Any Personally Identifiable Information (PII) will be anonymized before sending to the AI.

Use case 1: Summarize text

TeamMate

WK 099 | Satinalma Auditi

Open

Notifications (2)

Recent Activity

Help

+ New tab

Michal Dutkiewicz

MD

←

Project

Profile

Schedule

Audit Report

Close Project

Organization Hierarchy

Project Browser

TeamStore

Add

Edit

Admin

Actions

Excel

Filter

Save

Title

Search

Satinalma Auditi

IT Security

Control 1

Conflict of Interest

Improper segregation of duties

Conflict of Interest

Finding

Exec Summary

Condition

Cause

Consequence

Workflow

Assignments

References

Dimensions

Security Access

History

Exec Summary

Aspect

Description

| | |
|--------------------------------|--|
| Risk Management | Identification and management of financial risks related to reporting inaccuracies, fraud, and compliance. |
| Internal Controls Evaluation | Assessment of policies ensuring accuracy in financial reporting and asset safeguarding. |
| Compliance Assurance | Verification of adherence to laws, regulations, and internal policies. |
| Fraud Detection and Prevention | Identification of discrepancies indicating fraud and recommendations for preventive measures. |

Use case 2: Change tone of a finding description

<<

⚠

Inadequate Data Backup Process

<<

Issue

Issue Reporting Categories

Workflow

Assignments

References

Dimensions

History

▼ Issue *

during our audit we realized that data backups are rubbish. Backups don't work the way they should. IT staff should retain all these backups for at least 3 years – everyone who reads the Backup Policy should know this! Certain backups are gone, nobody knows where they are. What the hell is going on in this company, somebody should lose their job!

▼ Issue Reporting Categories

Issue Type *

(NONE) ▼

Report Levels

Root Cause

(NONE) ▼

Required

39

TeamMate Audit Insights | Bahrain, May 2025

Use case 2: Change tone of a finding description

<<

⚠

Inadequate Data Backup Process

<<

Issue

Issue Reporting Categories

Workflow

Assignments

References

Dimensions

History

▼ Issue *

✎ ▼

A ▼

A↑ ▼

A ▼

A ▼

B

I

U

Ⓢ

T_x

🔗

:=

½= ▼

≡ ▼

↶

↷

</>

:

Edit or review

Generate from selection

Change tone

Translate

Professional

Direct

Confident

Friendly

▼ Issue Reporting Categories

Issue Type *

Report Levels

Root Cause

Backups are rubbish. Backups don't work the way they should. IT staff

at least 3 years – everyone who reads the Backup Policy should know this!

is going on in this company, somebody

40

TeamMate Audit Insights | Bahrain, May 2025

Use case 2: Change tone of a finding description

The screenshot displays the TeamMate Audit Insights interface. At the top, a red warning icon is next to the title "Inadequate Data Backup Process". On the left, a sidebar contains navigation links: "Issue", "Issue Reporting Categories", "Workflow", "Assignments", "References", "Dimensions", and "History". The main area shows the "Issue" section with a dropdown menu for "Issue Reporting Categories" and a text input field for the issue description. The text in the input field is: "during our audit we should retain all the Certain backups are should lose their job". Below this, the "Issue Type" dropdown is set to "(NONE)" and is marked as "Required". The "System" dropdown is also set to "(NONE)". An "AI Editor" overlay is open, showing a text area with the following text: "During our audit, we identified significant deficiencies in the data backup processes. The current backups do not function as intended. It is imperative that IT personnel retain all backups for a minimum duration of three years, as stipulated in the Backup Policy, which should be well understood by all relevant stakeholders. Notably, some backups are missing, and there is a lack of clarity regarding their whereabouts. This situation raises serious concerns about the management of data integrity within the organization, and appropriate actions must be taken to address these issues." Below the text area, there are buttons for "Replace", "Insert below", "Try again", and "Stop". At the bottom of the overlay, a disclaimer states: "AI-generated content may be inaccurate and incorrect - always review and verify before use."

Issue

Issue Reporting Categories

Workflow

Assignments

References

Dimensions

History

Issue *

Issue Report

Issue Type *

(NONE)

Required

System

(NONE)


AI Editor

During our audit, we identified significant deficiencies in the data backup processes. The current backups do not function as intended. It is imperative that IT personnel retain all backups for a minimum duration of three years, as stipulated in the Backup Policy, which should be well understood by all relevant stakeholders. Notably, some backups are missing, and there is a lack of clarity regarding their whereabouts. This situation raises serious concerns about the management of data integrity within the organization, and appropriate actions must be taken to address these issues.

Replace Insert below Try again Stop

AI-generated content may be inaccurate and incorrect - always review and verify before use.

Use case 2: Change tone of a finding description

 Inadequate Data Backup Process

<<

Issue

Issue Reporting Categories

Workflow










Assignments

References

Dimensions

History

▼ Issue *

 ▼ | **A** ▼ | A ▼ | A ▼ | **A** ▼ | **B** | *I* | U | ~~S~~ | I |  |  |  ▼ |  ▼ |  |  |  | 

during our audit we realized that data backups are rubbish. Backups don't work the way they should. IT staff should retain all these backups for at least 3 years – everyone who reads the Backup Policy should know this! Certain backups are gone, nobody knows where they are. What the hell is going on in this company, somebody should lose their job!

During our audit, we identified significant deficiencies in the data backup processes. The current backups do not function as intended. It is imperative that IT personnel retain all backups for a minimum duration of three years, as stipulated in the Backup Policy, which should be well understood by all relevant stakeholders. Notably, some backups are missing, and there is a lack of clarity regarding their whereabouts. This situation raises serious concerns about the management of data integrity within the organization, and appropriate actions must be taken to address these issues.

Use case 3: Continue writing a finding

⚠

Critical Applications are not timely patched

⏪

Issue

Issue Reporting Categories

Workflow

Assignments

References

Dimensions

History

▼

Issue *

During the course of the IT audit, it was observed that the patch management process for a critical business application is not functioning in alignment with the organization's established corporate policy.

▼

Issue Reporting Categories

Issue Type *

(NONE) ▼

Required

Report Levels

▼

Root Cause

(NONE) ▼

43

TeamMate Audit Insights | Bahrain, May 2025

Use case 3: Continue writing a finding

Critical Applications are not timely patched

<<

Issue

Issue Reporting Categories

Workflow

Assignments

References

Dimensions

History

▼ Issue *

Edit or review

Generate from selection

Change tone

Translate

Observed that the patch management process for a critical business application is not

Summarize

Continue

Issue Type *

(NONE) ▼

Report Levels

Root Cause

(NONE) ▼

Required

Use case 3: Continue writing a finding

Critical Applications are not timely patched

<<

Issue

Issue Reporting Categories

Workflow

Assignments

References

Dimensions

History

▼ Issue *

✎

⌵

⌵

⌵

⌵

B

I

U

~~S~~

TX

🔗

⋮

⋮

⋮

⋮

↶

↷

</>

⋮

During the course of the IT audit, it was observed that the patch management process for a critical business application is not functioning in alignment with the organization's established corporate policy.

During the course of the IT audit, it was observed that the patch management process for a critical business application is not functioning in alignment with the organization's established corporate policy. This misalignment raises significant concerns regarding the overall security posture of the application and the potential risks associated with unpatched vulnerabilities. Effective patch management is essential for mitigating risks related to security breaches and ensuring compliance with regulatory requirements. The audit findings indicate that there may be gaps in the processes for identifying, testing, and deploying patches in a timely manner. It is crucial for the organization to review and enhance its patch management procedures to ensure they are consistent with the corporate policy and best practices in the industry. Furthermore, it is recommended that the organization implement regular monitoring and reporting mechanisms to track the status of patch deployments and to ensure that any deviations from the policy are promptly addressed. This will not only help in maintaining compliance but also in safeguarding the integrity and availability of critical business applications.

45

TeamMate Audit Insights | Bahrain, May 2025

Use case 4: PII masking

⚠

PII Data Leakage

⏪

Issue

Issue Reporting Categories

Workflow

Assignments

References

Dimensions

History

▼

Issue *

During the audit of the organization's data storage and handling practices, it was identified that personally identifiable information (PII) of employees and customers is being stored in an unencrypted format on several internal servers. One of them is VIP client Arthur Smith, phone number 00446771234, email address: smitha@hotmail.com.

▼

Issue Reporting Categories

Issue Type *

(NONE) ▼

Required

Report Levels

▼

Root Cause

(NONE) ▼

📌

46

TeamMate Audit Insights | Bahrain, May 2025

Use case 4: PII masking

⚠

PII Data Leakage

⏪

Issue

Issue Reporting Categories

Workflow

Assignments

References

Dimensions

History

▼ Issue *

✎ ▼

⌵

A ▼

A ▼

A ▼

A ▼

B

I

U

S

T_x

🔗

⋮

⌵

⌵

⌵

↶

↷

⌂

⋮

Edit or review

Generate from selection

Change tone

Translate

storage and handling practices, it was identified that personally identifiable information

Summarize

Continue

eral internal servers. One of them is VIP client

Issue Type *

Report Levels

Root Cause

47

TeamMate Audit Insights | Bahrain, May 2025

Use case 4: PII masking

⚠️

PII Data Leakage

<<

Issue

Issue Reporting Categories

Workflow

Assignments

References

Dimensions

History

▼ Issue *

✎ ▼

A ▼

A ▼

A ▼

A ▼

B

I

U

S

T_x

@

:

:

:

≡ ▼

↶

↷

</>

:

During the audit of the

(PII) of employees and

Arthur Smith, phone

▼ Issue Report

Issue Type *

(NONE)

Required

System

(NONE)

AI Editor

During the audit of the organization's data storage and handling practices, it was identified that personally identifiable information (PII) of employees and customers is being stored in an unencrypted format on several internal servers. This poses a significant risk to the confidentiality and integrity of sensitive information. One of the instances noted during the audit involved a VIP client, whose details include the name **PERSON**, phone number **PHONENUMBER**, and email address: **EMAIL**. The storage of such sensitive data in an unencrypted format not only violates best practices for data protection but also exposes the

Replace

Insert below

Try again


Stop

AI-generated content may be inaccurate and incorrect - always review and verify before use.

48

TeamMate Audit Insights | Bahrain, May 2025

Use case 5: Write a narrative from messy meeting notes

 Correct processing in applications

<<

Checklist Description

Test Steps

Record of Work Done


Test Conclusion

Recommendation

▼ Record of Work Done

- met our CISO to discuss IT security cntrols
- MFA in critical apps, not HR systems yet
- SOC centre understaffed
- patch mgmt working fine

Use case 5: Write a narrative from messy meeting notes

 Correct processing in applications

<<

Checklist Description

Test Steps

Record of Work Done

Test Conclusion


Properties

Workflow

Assignments

References

Record of Work Done



▼

Edit or review

>

Generate from selection

>

Change tone

>

Translate

>

Professional

Direct

Confident

Friendly

Test Conclusion

Click to edit

Use case 5: Write a narrative from messy meeting notes

Correct processing in applications

<<

Checklist Description

Test Steps

Record of Work Done

Test Conclusion

Properties

Workflow

Assignments

References

History

Record of Work Done

Click to edit

AI Editor

Engaged with our Chief Information Security Officer (CISO) to discuss information technology security controls.

Multi-Factor Authentication (MFA) has been implemented in critical applications; however, it has not yet been extended to Human Resources systems.

The ORGANIZATION (ORGANIZATION) is currently experiencing understaffing issues.

Patch management processes are functioning effectively.


Replace


Insert below

Try again


Stop

Use case 5: Write a narrative from messy meeting notes

 Correct processing in applications



- Checklist Description
- Test Steps
- Record of Work Done
- Test Conclusion
- Properties
- Workflow
- Assignments
- References
- History

 Record of Work Done

- met our firm's CISO to discuss IT security cntrols
- MFA in critical apps, not HR systems yet
- SOC centre understaffed
- patch mgmt working fine
- Engaged with our firm's Chief Information Security Officer (CISO) to discuss information technology security controls.
- Multi-Factor Authentication (MFA) has been implemented in critical applications; however, it has not yet been extended to Human Resources systems.
- The ORGANIZATION (SOC) is currently understaffed.
- Patch management processes are functioning effectively.

Use case 5: Write a narrative from messy meeting notes

Correct processing in applications

<<

Checklist Description

Test Steps

Record of Work Done

Test Conclusion

Properties

Workflow

Assignments

References

History

▼ Record of Work Done

▼

A[≡] ▼ A^I ▼ A ▼ **A** ▼ **B** *I* U ~~S~~ *T_x* @ | :: ½= ▼ ≡ ▼ ↶ ↷ </> ⋮

Edit or review >

Generate from selection >

Summarize

Continue

Change tone >

Translate >

...tion Security Officer (CISO) to discuss information technology security controls.

- Multi-Factor Authentication (MFA) has been implemented in critical applications; however, it has not yet been extended to Human Resources systems.
- The ORGANIZATION (SOC) is currently understaffed.
- Patch management processes are functioning effectively.

Use case 5: Write a narrative from messy meeting notes

Correct processing in applications

<<

Checklist Description

Test Steps

Record of Work Done

Test Conclusion

Properties

Workflow

Assignments

References

History

▼ Record of Work Done

▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼

- met our firm's CIS
- MFA in critical app
- SOC centre under
- patch mgmt worki
- Engaged with our
- Multi-Factor Auth
- Human Resources
- The ORGANIZATI
- Patch manage

AI Editor

Engaged with our firm's Chief Information Security Officer (CISO) to discuss the current state of information technology security controls. This engagement aimed to assess the effectiveness of existing measures and identify areas for improvement.


Multi-Factor Authentication (MFA) has been successfully implemented in critical applications to enhance security; however, it has not yet been extended to Human Resources systems, which poses a potential risk that needs to be addressed promptly.

The ORGANIZATION (SOC) is currently experiencing understaffing issues, which may

Replace Insert below Try again Stop

AI-generated content may be inaccurate and incorrect - always review and verify before use.

Use case 5: Write a narrative from messy meeting notes

 Correct processing in applications

<<

Checklist Description

Test Steps

Record of Work Done

Test Conclusion

Properties

















Workflow

Assignments

References

History

▼ Record of Work Done

 ▼  ▼  ▼  ▼        ▼  ▼    

- met our firm's CISO to discuss IT security cntrols
- MFA in critical apps, not HR systems yet
- SOC centre understaffed
- patch mgmt working fine
- Engaged with our firm's Chief Information Security Officer (CISO) to discuss information technology security controls.
- Multi-Factor Authentication (MFA) has been implemented in critical applications; however, it has not yet been extended to Human Resources systems.
- The ORGANIZATION (SOC) is currently understaffed.
- Patch management processes are functioning effectively.
- Engaged with our firm's Chief Information Security Officer (CISO) to discuss the current state of information technology security controls. This engagement aimed to assess the effectiveness of existing measures and identify areas for improvement.
- Multi-Factor Authentication (MFA) has been successfully implemented in critical applications to enhance security; however, it has not yet been extended to Human Resources systems, which poses a potential risk that needs to be addressed promptly.
- The ORGANIZATION (SOC) is currently experiencing understaffing issues, which may impact its ability to effectively manage security operations and respond to incidents in a timely manner.
- Patch management processes are functioning effectively, ensuring that systems are regularly updated to mitigate vulnerabilities and enhance overall security posture.

Use case 6: Write a control testing guidance

✓

Access Management

<<

Control Objective

Control Activity Description

Control Attributes

Rating

Assignments

▼ Control Activity Description

✎

▼

A[≡] ▼

A[↑] ▼

A ▼

A ▼

B

I

U

~~S~~

T_x

🔗

⋮

⋮

⋮

↶

↷

</>

↗

⋮

Edit or review

Generate from selection

Change tone

Translate

effectiveness of access management control. Auditors will validate both design and

Summarize

Continue

Use case 6: Write a control testing guidance

Access Management

<<

Control Objective

Control Activity Description

Control Attributes

Rating

Assignments

References

Dimensions

Historical Procedures

Historical Ratings

▼ Control Activity Description

A^B

A^I

A

A

B

B

~~C~~

T_x

@

::=

i=

≡

↶

↷

</>

↗

:

Internal audit team is assessing the effectiveness of access management control. Auditors will validate both design and operating effectiveness of access controls.

The ORGANIZATION team is currently undertaking a comprehensive assessment of the effectiveness of access management controls within the organization. This evaluation is crucial to ensure that access controls are not only designed appropriately but also function effectively in practice. The auditors will validate both the design and operating effectiveness of these access controls, which involves examining the policies, procedures, and technical measures in place to safeguard sensitive information and resources. This assessment will help identify any potential weaknesses or gaps in the access management framework, thereby enabling the organization to enhance its security posture and mitigate risks associated with unauthorized access.

Use case 7: Translating control description for a Spanish control owner

Access Management

<<

Control Objective

Control Activity Description

Control Attributes

Rating

Assignments

References

Dimensions

▼ Control Activity Description

A[≡]

A^I

A

A

I

U

~~S~~

T_x

[@](#)

:

=

≡

↶

↷

</>

↗

:

Auditors are currently undertaking a comprehensive assessment of the effectiveness of access management controls within the organization. This evaluation is crucial to ensure that access controls are not only designed appropriately but also function effectively in practice. The auditors will validate both the design and operating effectiveness of these access controls, which involves examining the policies, procedures, and technical measures in place to safeguard sensitive information and resources. This assessment will help identify any potential weaknesses or gaps in the access management framework, thereby enabling the organization to enhance its security posture and mitigate risks associated with unauthorized access.

Graphic control number

Access Management

<<

Control Objective

Control Activity Description

Control Attributes

Rating

Assignments

References

Dimensions

Historical Procedures

Historical Ratings

▼ Control Activity Description

✎ ▼

A ▼ A ▼ A ▼ B I U S Tx @ := != ≡ ▼ ↶ ↷ </> ↗ ⋮

Edit or review

Generate from selection

Change tone

Translate

English

Spanish

Portuguese

German

French

Simplified Chinese

Hindi

Arabic

comprehensive assessment of the effectiveness of access management controls
ion is crucial to ensure that access controls are not only designed appropriately but
The auditors will validate both the design and operating effectiveness of these
mining the policies, procedures, and technical measures in place to safeguard
any potential weaknesses or gaps in the access
management framework, thereby e
its security posture and mitigate risks
associated with unauthorized acces

▼ Control Attributes

Control Category

(NONE) ▼

Frequency

(NONE) ▼

Use case 7: Translating control description for a

Access Management

<<

Control Objective

Control Activity Description

Control Attributes

Rating

Assignments

References

Dimensions

Historical Procedures

Historical Ratings

▼ Control Activity Description

A[≡]

A^I

A

A

B

I

U

~~S~~

T_x

@

:

=

:=

≡

↶

↷

</>

↗

:

Auditors are currently undertaking a comprehensive assessment of the effectiveness of access management controls within the organization. This evaluation is crucial to ensure that access controls are not only designed appropriately but also function effectively in practice. The auditors will validate both the design and operating effectiveness of these access controls, which involves examining the policies, procedures, and technical measures in place to safeguard sensitive information and resources. This assessment will help identify any potential weaknesses or gaps in the access management framework, thereby enabling the organization to enhance its security posture and mitigate risks associated with unauthorized access.

Los auditores están llevando a cabo actualmente una evaluación integral de la efectividad de los controles de gestión de acceso dentro de la organización. Esta evaluación es crucial para garantizar que los controles de acceso no solo estén diseñados adecuadamente, sino que también funcionen de manera efectiva en la práctica. Los auditores validarán tanto el diseño como la efectividad operativa de estos controles de acceso, lo que implica examinar las políticas, procedimientos y medidas técnicas implementadas para salvaguardar la información y los recursos sensibles. Esta evaluación ayudará a identificar cualquier debilidad o brecha potencial en el marco de gestión de acceso, lo que permitirá a la organización mejorar su postura de seguridad y mitigar los riesgos asociados con el acceso no autorizado.

What is coming
around the
corner?

Do you want
support?

Do you have an
idea?

Questions about
technology?

Code examples from the
presentation:
https://github.com/future-audit-examples/oslo_2025



Geert-Jan Claassen

Regional Manager
Wolters Kluwer

Geert-Jan.Claassen@wolterskluwer.eu



Linda Nyvelius

Director Nordics
BR1GHT

Linda.Nyvelius@br1ght.eu



Thank you



Appendices

Responsible AI: How are We Addressing Data Security Concerns?

Response Safeguards

Designed to prevent inappropriate, inaccurate, or biased replies and PII blocker

Data Isolation

The AI will not use the content an auditor inputs to further train the model so information remains secure within the audit process and will not be accessible to external parties, nor will it be used for any model improvements

No Data Retention

Once the AI provides suggestions or generates text, the data is immediately discarded. There is no retention of user inputs for future processing

End-to-End Encryption

All data transmitted to and from the AI is encrypted

Wolters Kluwer Assurance Framework for Responsible AI Development

Privacy and Security

Wolters Kluwer focuses on privacy and security as part of the design, development and deployment of AI in our products and services. We promote the creation of AI systems that are safe, secure and reliable through our processes and procedures.

Transparency and Explainability

Wolters Kluwer aims to design and develop AI systems with sufficient transparency and explainability to enable users to understand and use the system appropriately.

Governance and Accountability

Wolters Kluwer adheres to development standards and processes that promote responsibility and accountability for AI systems and their outcomes. We address risk management and issue remediation during design and development, as well as after deployment.

Fairness

Wolters Kluwer recognizes the importance of treating people fairly and without discrimination in the design and development of AI products and services.

Human Focused

Wolters Kluwer strives to create AI systems that are human-centric, focused on solving business problems and benefiting our customers; while also considering the potential impact they may have on society and our environment.

Linda Nyvelius

Linda Nyvelius began her internal audit career at the Institute of Internal Auditors (IIA) Sweden, where she became CEO in 2015. She contributed to national, European, and global initiatives to advance the profession through advocacy, policy, training, and guidance.

Over time, she recognised that for internal audit to remain relevant, it must fully embrace new technology—not as an add-on, but as a core enabler of quality, efficiency, and strategic value. With growing stakeholder demands, a rapidly evolving risk landscape, and increasing competition for talent, technology a crucial enabler for the long-term success of the profession.

In 2020, she joined BR1GHT in Amsterdam to support internal audit teams more hands-on. As Director Nordics and Head of Internal Audit Services, she combines leading technology with expert practitioners to ensure every engagement integrates strategy, structure, processes, and people—unlocking the full potential of the audit function in a digital age.



Linda Nyvelius

Director Nordics
BR1GHT

Linda.Nyvelius@br1ght.eu

