THE INSTITUTE OF INTERNAL AUDITORS

The Unseen Employee

Practical Assurance in the AI Era

Presented By | Janine Koch – National Practice Lead, Governance, Risk & Compliance

APRIL 27, 2026

SOLOMONEDWARDS

The Unseen Employee

AI is already operating as an “unseen employee”.

- ☑ **Executing tasks**
- ☑ **Influencing decisions**
- ☑ **Interacting with ERP, finance, and operations**

Internal Audit must ensure:

- Visibility
- Governance
- Controlled access
- Clear accountability

AI is not just technology; it is a **new control actor** within the enterprise risk environment.

Learning Objectives

Today's Focus Areas

01 **Identify** where Unseen Employees operate across the enterprise

02 **Evaluate** the key risks of their access & decision authority

03 **Assess** their governance and control structures

04 **Apply** practical audit approaches within enterprise risk

Imagine an employee approving hundreds of expenses at 2 a.m.

No badge.

No oversight.

That "employee" already exists.

Why This Matters to Internal Audit Now

AI has authority and oversight must **catch up.**

Operational Authority

Unseen Employees already execute transactions inside core financial systems.

Regulatory Expectation

Regulatory bodies expect documented, auditable AI governance.

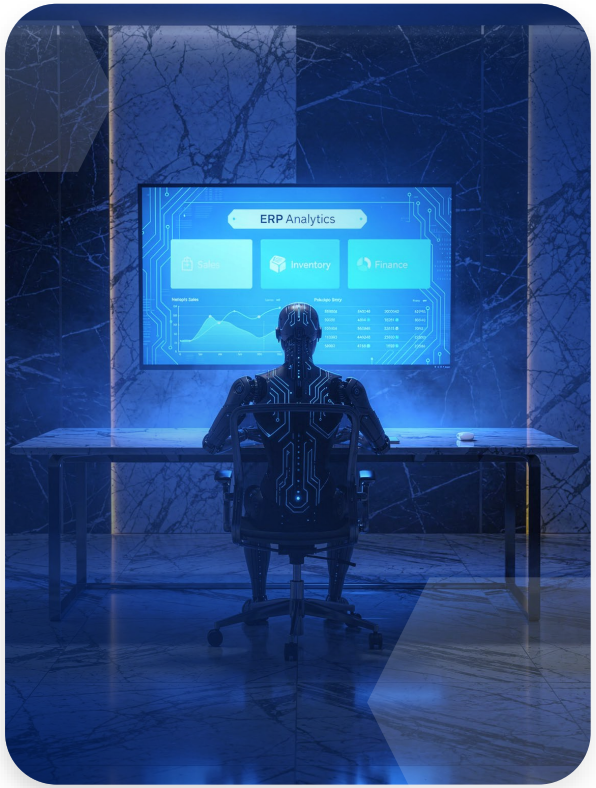
Board Scrutiny

Audit committees are demanding transparency into AI risk.

Internal Audit cannot wait for failure. oversight must be proactive.

Today’s Practical Outcomes

From AI visibility to executable audit procedures



AI Footprint Mapping

Understand where AI employees are operating inside your ERP and enterprise systems.

Governance Maturity Model

Apply the IIA AI Auditing Framework to assess governance maturity

Amplified Control Risks

Identify risks introduced when AI operates as an unsupervised "employee."

Executable Audit Steps

Translate high-risk AI use cases into practical audit procedures.

SECTION I

The Rise of the Unseen Employee

SOLOMONEDWARDS

Where the Unseen Employee is Working Today

They Already Have Authority

- Finance / Procure-to-Pay (P2P)
- Accounts Payable
- Human Resources
- Operations & Compliance
- Shadow / Citizen AI

Trained by business teams, integrated into ERP, often without central oversight.

Finance / P2P > The Unseen Employee in Action

Autonomous Financial Posting with ***No Human Sign-off***

Expense Auto-Approval

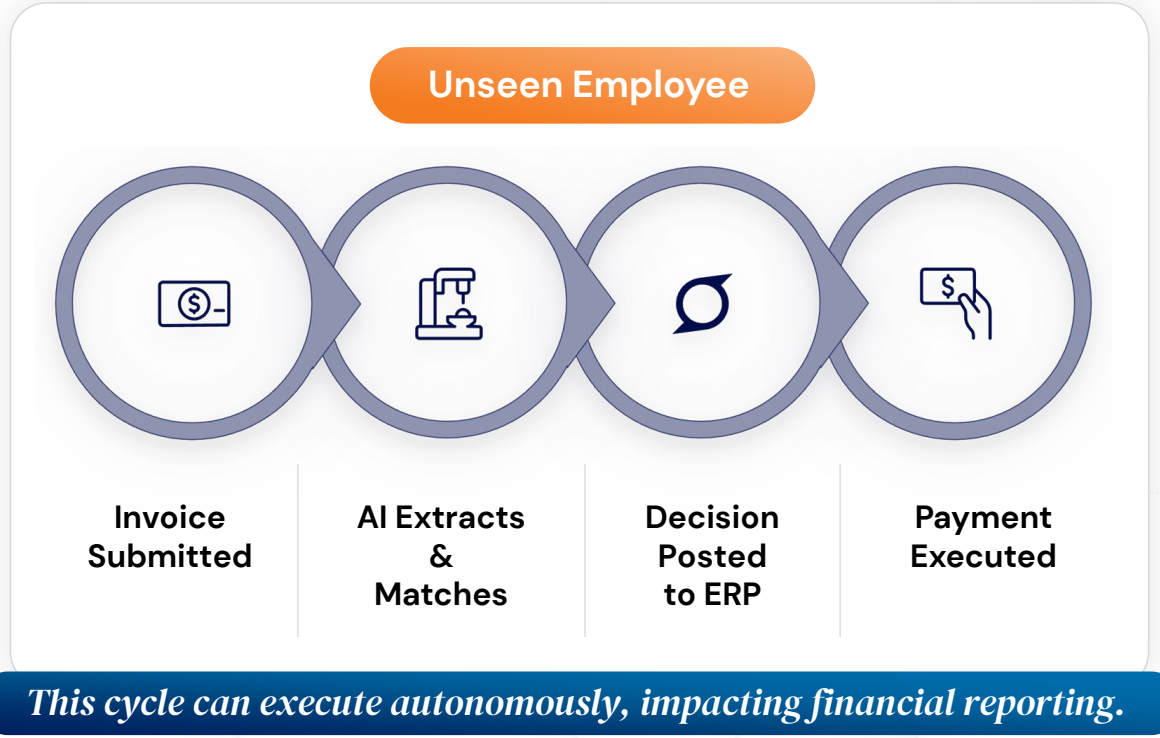
Threshold-based approvals ($5K–$10K) executed automatically

Agentic Processing

Extract → match → validate → decide → post inside ERP

No Human Signature

Transactions can complete end-to-end without manual review



This cycle can execute autonomously, impacting financial reporting.

Accounts Payable › The Unseen Employee in Action

Service Accounts with ***Create + Approve*** *access*

Automated Data Extraction

Optical Character Recognition (OCR) + Natural Language Processing (NLP) extract structured invoice data

Auto Exception Handling

Applies trained rules without human escalation

Autonomous GL Posting

Transactions post directly to the general ledger

Dual Authority Risk

Service accounts may both create and approve transactions

Segregation of duties

can be bypassed without a human in the loop.

Human Resources > The Unseen Employee in Action

Influencing Regulated Employment Decisions *Before Human Review*

Automated Onboarding Documentation

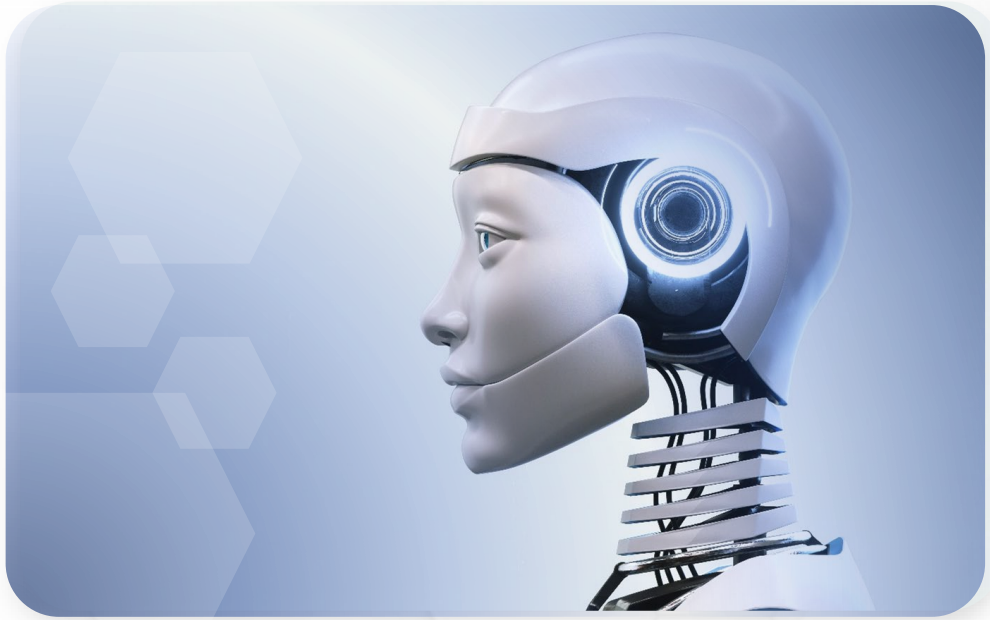
Auto-populates onboarding forms, access requests, and compliance acknowledgments

AI-Generated Performance Narratives

LLMs draft first-pass performance evaluations from structured inputs

Automated Candidate Filtering

Ranks and filters candidates before human recruiter review



Employment decisions may be shaped by AI without documented human judgment.

Operations & Compliance › The Unseen Employee in Action

Initiating Operational Approvals *Without Human Review*

Predictive Maintenance Approvals

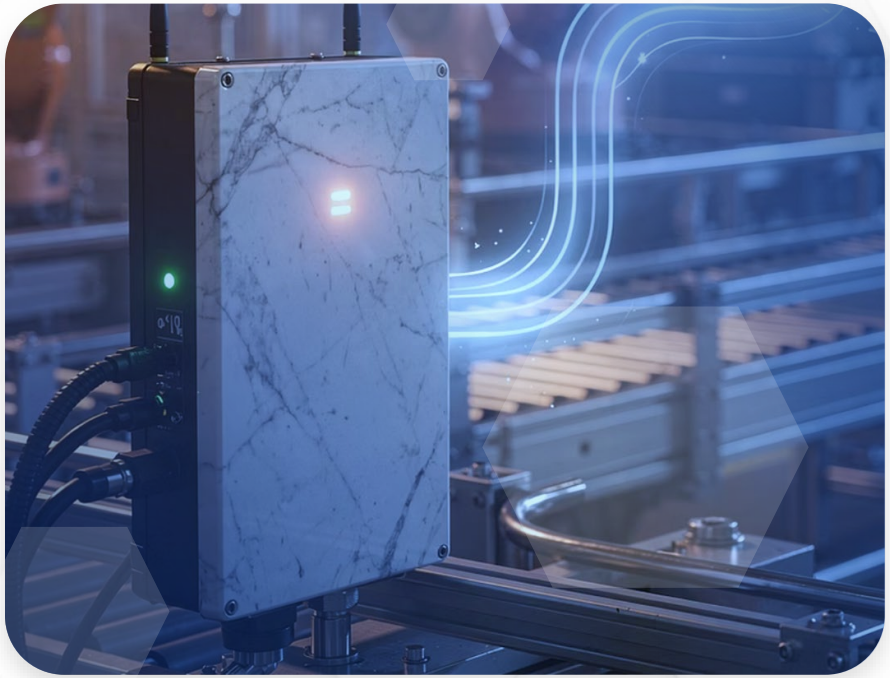
Autonomously approves maintenance work orders based on sensor data

Operational Safety Impact

AI-triggered approvals can directly affect asset valuation and safety

Regulatory Checklist Auto-Fill

Completes compliance checklists and regulatory filings with minimal human review



Operational approvals may execute without documented human oversight.

Shadow / Citizen AI > The Unseen Employee in Action

AI Built, Trained and *Deployed Outside Enterprise Governance*

Low-Code & Embedded AI Tools in Use

- Power Automate
- Vertex AI
- ChatGPT Enterprise

Business-Led Automation in Production

- Reconciliations
- Testing scripts
- Financial reporting support
- Operational dashboards

How it Happens

Citizen Developer

Business user builds AI-enabled workflow without formal IT or risk review

Custom AI

Operates without central governance or oversight

Unsecured Cloud / ERP

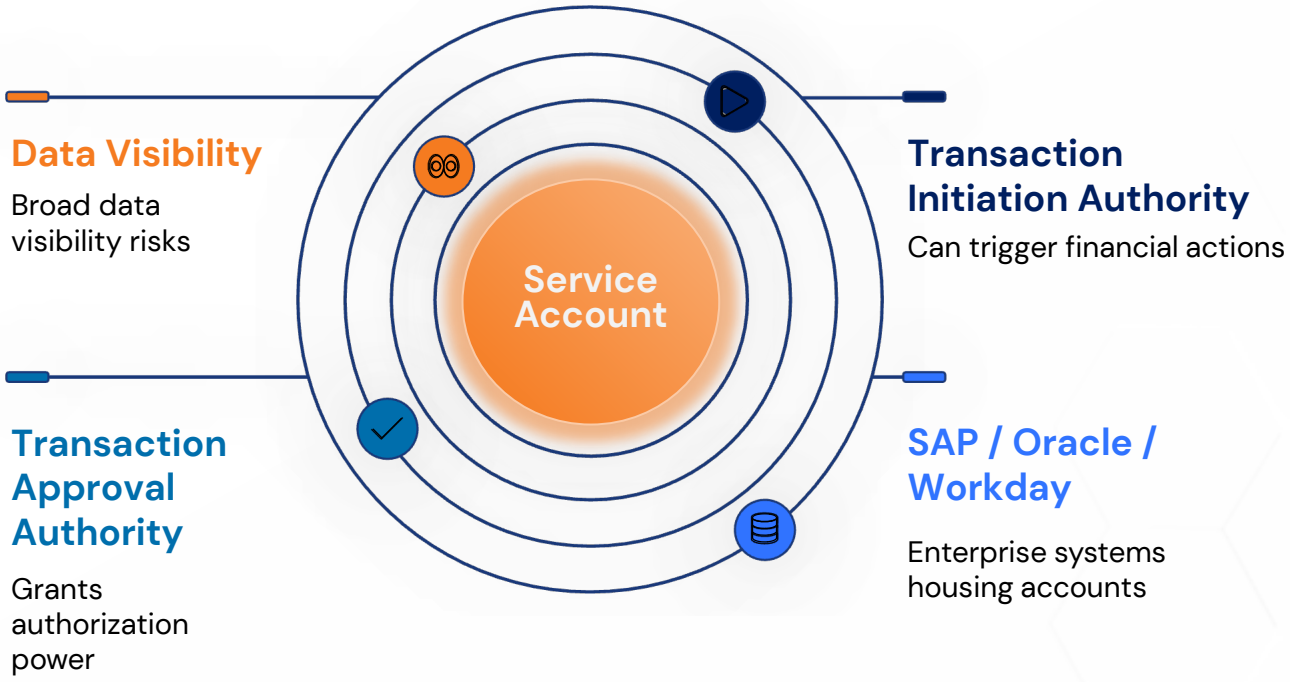
- No IAM review
- No SoD validation
- No formal owner

Direct system access with limited or no audit trail and no defined control owner

AI systems may be operating in production without formal governance, ownership, or audit visibility.

Common Thread Across All Examples

Your audit starting point



The Pattern

Across every use case—finance, AP, HR, operations and citizen —the same structural control weakness emerges:

- No centralized onboarding, vetting, or governance approval
- Service accounts embedded within SAP, Oracle, and Workday
- Broad authority to read, initiate, and approve transactions

The common risk driver is uncontrolled authority within enterprise systems.

SECTION II

Key Risks When Unsupervised

The 8 Amplified Control Risks

SolomonEdwards

8 Amplified Risks of the Unseen Employee

Key Risks When AI Operates Without Supervised

These eight risks cluster into three control areas:

Governance Risks

1. Bias & Unfairness
2. Opacity & Explainability
3. Accountability Gaps

Control Environment Risks

4. Access & Decision Rights
5. Integration Risks
6. Drift & Hallucinations

Oversight & Strategic Risks

7. Regulatory Exposure
8. Over-Reliance & Deskilling

Internal Audit cannot wait for failure. Oversight must be proactive.

Governance Risks

Bias & Unfairness | Opacity & Explainability | Accountability Gaps

01. Bias & Unfairness

AI replicates historical past discrimination.

Example: Expense approvals skewed by vendor patterns

Audit Questions
- Is bias testing documented and reviewed?
- Are business users trained to identify potential bias in outputs?
- Who approved the fairness thresholds?

02. Opacity & Explainability

Decision logic is not explainable.

Example: No one can explain why a vendor was rejected

Audit Questions
- Can management explain how decisions are made?
- Has management defined what constitutes a “defensible explanation”?
- Can a historical decision be reconstructed six months later?

03. Accountability Gaps

No formally assigned decision owner.

Example: An error is posted; no one is responsible

Audit Questions
- Who is formally accountable for decisions AI makes?
- Who signs off on AI-generated financial postings?
- What happens when the original developer leaves?

Control Environment Risks

Access & Decision Rights | Integration Risks | Drift & Hallucinations

04. Access & Decision Rights

AI Accounts Can Create, Approve, and Post Transactions

Example: The Unseen Employee creates, approves and pays in SAP

Audit Questions
- Does this AI violate segregation of duties?
- Is there independent review of AI activity?
- Does the AI operate under a service account?

05. Integration Risks

AI Spans Multiple Systems with No Unified Control

Example: Workflow touches Workday, Oracle, and payment platform

Audit Questions
- Who monitors cross-system activity?
- Is version history maintained?
- Are integrations tested in UAT before productions deployment?

06. Drift & Hallucinations

Model Behavior Shifts Over Time.

Example: Approval thresholds creep upward unnoticed

Audit Questions
- How is model drift detected and monitored?
- What drift indicators are defined (data, concept & performance drift)?
- Have hallucination incidents been documented and analyzed?

Oversight & Strategic Risks

Regulatory Exposure | Over-Reliance & Deskilling

07. Regulatory Exposure

Automated Decisions May Breach Regulated Oversight Requirements.

Example: AI-generated HR decision without human review

Audit Questions

- Is there required human oversight documented?
- Are impact assessments performed?
- Has management defined regulatory accountability?

08. Over-reliance & Deskilling

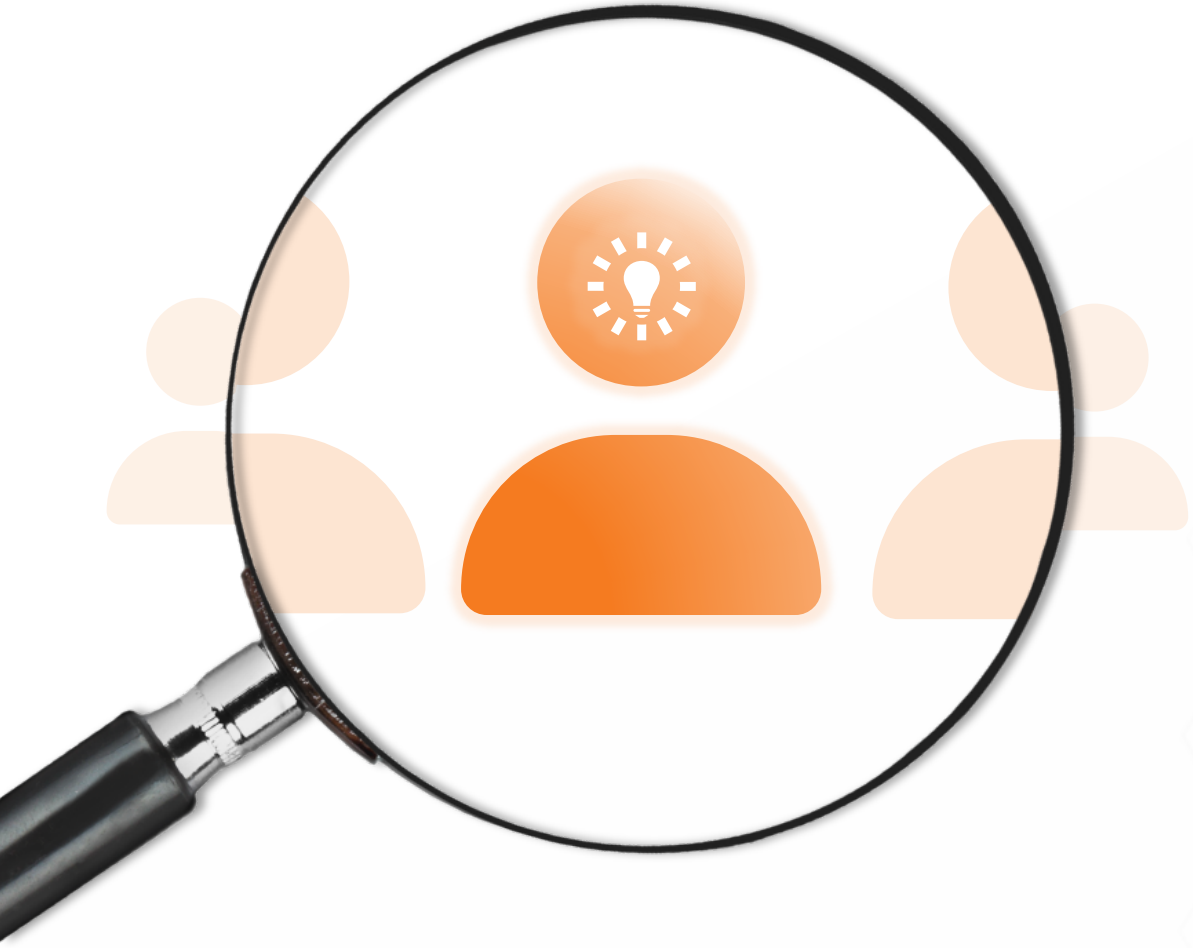
Staff Defer To AI without Independent Validation.

Example: AP can no longer manually verify invoices

Audit Questions

- If AI failed tomorrow, could operations continue?
- Are staff trained to understand AI logic?
- How often do humans challenge AI recommendations?

Reflection for Internal Audit Leaders



How many “Unseen Employees” are already inside your audit universe?

Think about the Unseen Employees and automated workflows operating in your ERP today.

- Which of the 8 risks are already present?
- Which are simply undiscovered?

SECTION III

The IIA Roadmap

Turning Unseen Employee Risk Into Structured Oversight

SolomonEdwards

IIA Artificial Intelligence Auditing Framework

The Three Domains of AI Oversight

DOMAIN 1

Governance

Setting Direction & Risk Appetite

- AI Strategy + Ethics
- AI Inventory
- Board Oversight

Governance sets direction.

DOMAIN 2

Management Controls

Operating Within Guardrails

- Data & Model Integrity
- Operational Guardrails
- Decision Rights & Access Governance

Management operates AI.

DOMAIN 3

Internal Audit

Independent Validation & Continuous Assurance

- Advisory: Early engagement
- Assurance on Maturity
- Framework-based audits

Audit validates trust.

Governance

Domain 1 of 3: Setting Direction & Risk Appetite

Strategy & Ethics

- **Defined AI** risk appetite
- **Executive ownership** of material AI
- **Escalation** for incidents & model failure

Inventory

- **Risk-classified** AI inventory
- **Purpose, data & decision authority** documented
- **Third-party** & shadow AI identified

Board Oversight *Tone at the Top*

- **AI risk** dashboard review
- **Incident oversight** & remediation tracking
- **Review** of independent assurance

Without governance, AI multiplies without oversight.

The board cannot oversee what it cannot see.

Management Controls

Domain 2 of 3: Operating Within Guardrails

Data & Model Integrity

- **Data quality** controls
- **Bias testing** across key groups
- **Controlled model** changes

Decision Rights & Access Governance

- **Defined AI roles** & permissions
- **Approval thresholds** enforced
- **Segregation of duties**
- **Access monitoring** & recertification

Operational Guardrails

- **Human oversight** requirements
- **Escalation** for high-value decisions
- **Third-party AI** vendor oversight

Most operational AI risk lives here.

If management fails to control data, access, and oversight, the "unseen employee" can quietly create financial, regulatory, and reputational harm.

Internal Audit

Domain 3 of 3: Independent Validation & Continuous Assurance

Advisory: Early Engagement

- **Review** controls pre-deployment
- **Advise** on oversight thresholds
- **Assess** implementation readiness

Assurance on Maturity

- **Test** bias controls
- **Validate** model change controls
- **Assess** AI segregation of duties

Practitioner's Guide checklists

- **Apply** IIA AI Auditing Framework
- **Risk based** AI scoping
- **Test** explainability & traceability

Internal Audit validates that AI governance is effective and defensible.

SECTION IV

Practical Audit Examples

SolomonEdwards

Five High-Impact AI Audit Domains

Expense-Approval

Review permissions, thresholds & GL posting

Accounts Payable

Test extraction accuracy & autonomous posting

HR Pre-Screening

Assess bias risk & human override

Predictive Maintenance

Evaluate autonomous approvals & escalation triggers

Citizen AI / Shadow AI

Inventory automations & ERP access

Risk-rotate: 1 high-impact AI Internal Audit per quarter.

Embed AI into your annual audit plan.

Your 12 Month Roadmap to Lead on AI Auditing

Start one step this month, most begin with the inventory for fast visibility.

Start This Quarter

Three Commitments

COMMITMENT 1

Establish Visibility

Inventory all AI agents, models and service accounts within 90 days.

COMMITMENT 2

Deliver One Audit

Conduct and complete at least one full-scope AI Internal Audit after the inventory.

COMMITMENT 3

Institutionalize Oversight

Adopt a quarterly AI risk rotation schedule.

We don't slow innovation.
We make it trustworthy and sustainable.

The “Unseen Employee”

Must be governed

Q&A:

Questions?
Experiences and stories?

Thank you & Contact Info

Thank You

The work of making Unseen Employees trustworthy and auditable starts with practitioners like you asking the right questions.

The AI era requires stronger audit leadership; and that starts with you.

"We don't slow innovation; we make it trustworthy and sustainable."

Janine Koch
National Practice Lead, Governance, Risk & Compliance
832.465.9019
jkoch@solomonedwards.com | LINKEDIN

IIA Resources

IIA Artificial Intelligence Auditing Framework (Sept 2024) — available at theiia.org

Where AI Control Failures Are Discovered

ERP Access Review

Sample Table: Non-Human Accounts, Permissions, Red Flags

Use this table structure to document and assess AI service accounts identified during your audit inventory phase. This is often where the most significant AI control failures are discovered.

Account Name	System	Permissions	Business Owner	⚠️ Red Flags
AP_BOT_PROD_01	SAP S/4HANA	Read / Post / Approve	Unassigned	No owner; **Create + Approve combined** (SoD breach)
HR_SCREEN_BOT	Workday	Read / Score / Recommend	HR Technology	No bias testing documented; no human override log maintained
CITIZEN_BOT_FIN	Power Automate → Oracle	Read / Extract / Post	Unknown	Shadow deployment; no IT review; broad ERP write access granted

Immediate Audit Action:

- Pull all non-human ERP accounts.
- Treat combined create + approve as automatic SoD findings.

What a Real AI Audit Looks Like: Expense Approval

Audit Procedures in Table Format

One detailed example — Expense-Approval AI — showing how to structure a practical audit program for a high-impact AI use case.

This is how AI risk becomes an audit finding.

#	Audit Procedure	Evidence to Obtain	⚠️ Red Flag / Finding Indicator
1	Obtain and review the AI service account profile in SAP/Oracle	User admin extract; permission role assignments	**Account holds create + approve roles simultaneously (SoD violation)**
2	Review auto-approval threshold configuration and change history	System configuration log; change tickets	Threshold increased without documented approval
3	Test exception escalation: submit out-of-policy expense and observe AI behavior	Test transaction results; escalation log	AI approves out-of-policy item or fails to escalate to human reviewer
4	Review model monitoring and drift detection documentation	Model performance reports; monitoring schedule	No monitoring in place; last model review >12 months ago
5	Confirm business owner and formal accountability assignment	RACI or ownership documentation	No named owner; IT and Finance both disclaim responsibility