



## Asian Journal of Management and Commerce

E-ISSN: 2708-4523

P-ISSN: 2708-4515

Impact Factor (RJIF): 5.61

AJMC 2026; 7(2): 18-20

© 2026 AJMC

[www.allcommercejournal.com](http://www.allcommercejournal.com)

Received: 08-11-2025

Accepted: 11-12-2025

**Ansari Azharuddin Qamruddin**

Assistant Professor, Swayam

Siddhi Degree Night

Pipeline Road, Bhiwandi,

Maharashtra, India

# Hotel audit: transition from transactional assurance to AI governance

**Ansari Azharuddin Qamruddin**

**DOI:** <https://www.doi.org/10.22271/27084515.2026.v7.i2a.999>

### Abstract

The integration of Artificial Intelligence (AI) in the hospitality industry particularly in high-volume functions such as Revenue Management, Procurement, and Guest Services, is altering the old internal control environment. This study examines the key evolution of the Internal Audit (IA) function, arguing for a move from Transactional Assurance (periodic verification of specific controls and samples) to AI Governance and Continuous Monitoring (CM/CA). Based on professional experience and industry reports, the study identifies which routine audit tasks are most vulnerable to automation, examines the core risks of AI deployment (such as algorithmic bias and lack of explain ability in dynamic pricing models), and proposes a strategic re-skilling framework for hospitality auditors.

This study examines the up-gradation of the Internal Audit (IA) function, arguing for a move from Transactional Assurance to AI Governance, the research paper is based on industry reports and research papers.

**Keywords:** Internal Audit (IA), AI Governance, Transactional Assurance, Algorithmic bias, Hospitality Industry, Revenue Management

### Introduction

Internal audit (IA) tasks have traditionally been organized around the need to offer periodic assurance about the efficacy of internal controls, often by sampling and human verification of high-volume financial and operational transactions. In the hotel business, this includes daily cash reconciliations, food and beverage (F&B) expense checks, and payroll controls—all of which are high volume and high risk. The exponential growth of AI and automation tools—such as advanced algorithms for dynamic pricing, predictive maintenance, and RPA for back-office functions—is fast dismantling this traditional approach. The First Line of Defense (management and operations) is increasingly automating routine assurance tasks using Continuous Monitoring (CM). This technical progress poses a twin challenge to IA.

1. **Audit's Automation:** AI systems can automate data analysis and compliance checks faster and more precisely than human auditors, reducing the need for routine transactional audits.
2. **Automation's Audit:** AI systems pose unique risks like as algorithmic bias, poor data quality, and lack of transparency that typical internal auditing procedures cannot address.

This research aims to analyze the mandatory shift from Transactional Assurance (focused on outputs) to AI Governance.

### Objectives

- Analyzing the Impact of AI and Robotic Process Automation (RPA) on Manual Hospitality Auditing
- Understanding AI System's considered High Risk
- Evaluating Emerging Risks like as Algorithmic Bias, Data Integrity.
- Recommendations for Chief Audit Executives (CAEs) for strategies needed to implement this transition.

**Corresponding Author:**

**Ansari Azharuddin Qamruddin**

Assistant Professor, Swayam

Siddhi Degree Night

Pipeline Road, Bhiwandi,

Maharashtra, India

- **The Erosion of Transactional Assurance:** The Erosion of Transactional Assurance: Traditional auditing involves analyzing a sample of transactions (e.g., invoices, journal entries, room night records) at a specific time. Following audit areas are particularly vulnerable to automation via AI/RPA and Continuous Monitoring (CM):
- **Inventory Cut-off & Valuation in Food & Beverage (F&B), Stores:** Automated tracking of purchase-to-consumption ratios; real-time anomaly detection in high-cost item variances
- **Daily Revenue Reconciliation in Front Desk, Night Audit:** AI algorithms reconciling PMS data, POS systems, and payment gateway reports instantly; flagging discrepancies in real-time
- **Invoice-to-PO Matching in Procurement, Accounts Payable:** RPA bots validating purchase order (PO) details against vendor invoices and receipts, automating the three-way match and eliminating manual review.
- **Fixed Asset Verification:** Use of drone or image recognition AI for automated inventory and location verification

**Table 1:** AI Systems Considered High Risk

Area / Category	Description
Biometric identification and categorization of natural persons	AI systems intended to be used in remote biometric identification in real or delayed time of natural persons.
Management and exploitation of critical infrastructures	AI models linked to transport or other similar infrastructures may endanger the life and health of citizens.
Vocational education and training	AI systems that can determine access to a person's education and career.
Employment, worker management, and access to self-employment	AI systems for recruitment; for example, to advertise vacancies, select or filter applications, or evaluate candidates during interviews or tests, as well as to make decisions on promotion and termination of work-related contractual relationships, assigning tasks, and monitoring
Access and enjoyment of essential private services and public services and benefits	AI systems intended to be used by or on behalf of authorities to assess entitlement to public assistance benefits and services, as well as to grant, revoke, or claim such benefits and services.
Law enforcement matters	AI models intended to be used to make individual risk assessments or other predictions intended to be used as evidence, or to determine the reliability of information provided by a person to prevent, investigate, detect, or prosecute a crime.
Migration, asylum, and border control management	AI systems intended to be used to predict the occurrence of crimes or events of social unrest to allocate resources dedicated to patrol and surveillance of territories.
Migration, asylum, and border control management	AI systems intended to assist a judicial authority in the investigation and interpretation of facts and the law, as well as in its application to a specific set of facts.

The thought factory institute of internal auditors of Spain: <https://www.theiia.org/globalassets/site/content/articles/affiliate-content/2025/ia-of-ai-applied-to-business-processes-iaa-spain.pdf>

### Challenges in implementing AI governance in hospitality

AI-driven Revenue Management Systems (RMS) are perhaps the highest-risk application in hotels. They are complex, opaque, and directly impact financial performance and brand reputation. Core governance risks include:

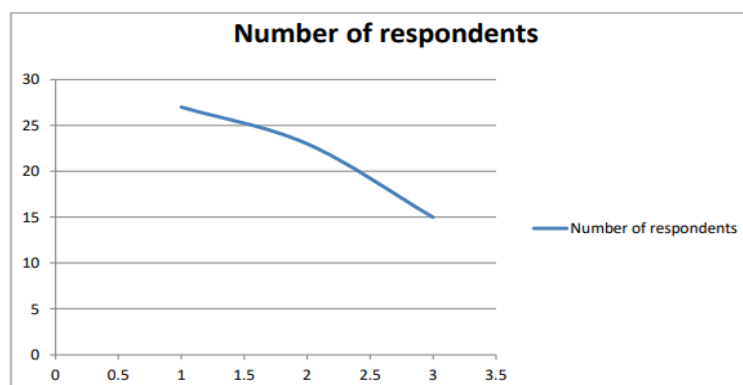
- **Ethical Issues:** The effects of AI on employment and society, the possibility of abuse, and the requirement for accountability and openness in AI systems are all ethical issues.
- **Algorithmic Bias:** RMS models may be trained on biased historical data, which could result in discriminatory pricing against specific customer segments (e.g., depending on device, location, or anticipated affluence), raising moral and legal issues (GDPR, consumer protection).
- **Data Integrity Risk:** The AI depends on large, real-time data streams (weather, airline information, rival pricing). The quality, applicability, and security of the data used to train and operate the RMS must be audited by IA.
- **Lack of Human Judgment:** Because AI lacks human judgment, it may not always be able to comprehend

the context of audit results or analyze complex circumstances.

- **Absence of Human Insight:** AI does not possess human intuition and might struggle to understand intricate situations or accurately interpret the context of audit results.
- **Concerns regarding Data Privacy:** AI technologies could handle sensitive data, which brings up issues related to data privacy and security; therefore, it is essential to establish strong data protection protocols.
- **Complexity of AI Systems:** AI technologies can be intricate and necessitate specialized expertise for their development, implementation, and maintenance, which can pose difficulties for certain organizations.
- **Dependence on AI Systems:** Relying too much on AI can result in laziness among auditors, who may not thoroughly examine audit results or apply critical analysis.
- **Regulatory Issues:** The application of AI in auditing might present regulatory obstacles since authorities may demand transparency and accountability in AI functionalities.

**Question 1**:-Do you think AI can effectively detect unusual working patterns and behaviors for auditors?

Question	Number of respondents	% of the respondents
Strongly Agree	27	27%
Agree	23	23%
Neutral	15	15%
Disagree	20	20%
Strongly Disagree	15	15%
TOTAL	100	100



**Interpretation:-** In simple terms, 50% of respondents either agree or strongly agree with the statement, while 35% disagree or strongly disagree. The remaining 15% are neutral. This indicates a somewhat positive leaning towards the statement among the respondents.

**Fig 1:** Below survey has been taken from <https://www.ijnrd.org/papers/IJNRDTH00148.pdf> with the interpretation as copied below:  
Question; Do you think AI can effectively detect unusual working patterns and behaviors for auditors?

### Recommendations for Chief Audit Executives (CAEs)

Hotel CAEs must implement a clear talent strategy to manage this transition:

1. **Talent Acquisition:** Prioritize hiring professionals with data science, cyber security, and cloud expertise, embedding them into audit teams.
2. **Targeted Up-skilling:** Shift Continuing Professional Education (CPE) focus away from core accounting compliance toward AI assurance, cloud auditing, and CM methodologies.
3. **Methodology Revision:** Mandate the development of specific AI Audit Playbooks (e.g., a "Revenue Management AI Audit") that standardize the testing of algorithmic controls and governance.

### Conclusion

Internal Audit (IA) in the hotel industry must transition from Transactional Assurance to AI Governance as a result of AI/Robotic Process Automation (RPA) integration.

- **Transactional Audits are no longer useful:** The Company is automating routine, sample-based audits (Continuous Monitoring), rendering traditional IA obsolete if it doesn't change.
- **Algorithmic Risk is the New Focus:** IA must shift from transaction verification to intelligent system governance, addressing high-impact risks such as algorithmic bias and data integrity.
- **Auditor's New Role:** Rather than serving as the last check on manual procedures, the auditor now serves as the governance guardian over intelligent systems. The AI development lifecycle has to be closely integrated with assurance.
- **Mandate for CAEs:** Immediate Talent Transformation (hiring data/cyber specialists) and Methodology Revision (developing specialized AI Audit Playbooks) are necessary for success.

### References

1. Institute of Internal Auditors Spain. Internal audit of artificial intelligence applied to business processes. Madrid: IIA Spain; year not specified.
2. Suyono WP, Puspa ES. Artificial intelligence in auditing: A systematic review of tools, applications, and challenges. Int J Audit Technol. 2015 Jun; volume (issue): page-page.
3. Srinivas H. The role of artificial intelligence in auditing: Current applications and future prospects. Int J Audit Account Res. 2024 May; volume (issue): page-page.
4. Wu DD. AI governance and auditing: Transformations, challenges, and adaptations. J AI Gov Audit. 2025 Apr; volume (issue): page-page.
5. Nguyen TTB. Transforming auditing in the AI era: A comprehensive review. Int J Audit Digit Technol. 2025 May; volume (issue): page-page.