**AI-Powered Smart Hospitality ERP: Risk management and AI governance considerations**

Akshara Kumari, Chelsea Anestal, Christian Abreu, Claudia Beatriz Saleh, and Vladomir Jungkman

Muma College of Business, University of South Florida

ISM 6155: Enterprise Information Systems Management

Dr. Samuel Conn

September 27, 2024

Executive Summary

## Project Objective

 This project’s primary objective is to define a comprehensive AI governance framework and risk management plan that aligns with Emerald Hotels and Resorts (Emarald H &R’s) strategic objectives of expansion, safety, and quality.

## Scope

 This project provides an overview of relevant key theories and frameworks in AI governance and risk management as well as how AI is revolutionizing the hospitality industry. It uses a scoping methodology to narrow down to specific frameworks that will be used and addresses the timeline, personnel, resources, and tools for implementation.

## Key Findings

Through a 9-month implementation process, the team at Emerald H&R will employ an AI governance framework that will address major components such as the governance process and roles/responsibility while using FASTEPS principles of fairness, accountability, safety, transparency, ethics, privacy, and security, and risk management plan addressing risk mitigation, owners, monitoring, and reporting.

## Recommendations

Recommendations include frequent updates to align with business practices and changes in AI technology, a council to provide direction and regular updates, adjustments to match organizational needs before employment by other organizations.

# Table of Contents

[Executive Summary 2](#_Toc178352810)

[Project Objective 2](#_Toc178352811)

[Scope 2](#_Toc178352812)

[Key Findings 2](#_Toc178352813)

[Recommendations 2](#_Toc178352814)

[Introduction 5](#_Toc178352816)

[Literature Review 7](#_Toc178352817)

[AI Governance Frameworks 7](#_Toc178352818)

[Risk Management 7](#_Toc178352819)

[AI in the Hospitality Industry 8](#_Toc178352820)

[Notable Research Gaps 9](#_Toc178352821)

[Methodology 10](#_Toc178352822)

[Tools, techniques, and frameworks used for risk analysis 10](#_Toc178352823)

[Sources of data and information 11](#_Toc178352824)

[AI Governance Framework 12](#_Toc178352825)

[Policies and Procedures Included in the Framework 12](#_Toc178352826)

[Roles and Responsibilities within the Governance Structure 13](#_Toc178352827)

[Continuous Monitoring and Feedback Mechanisms 14](#_Toc178352828)

[FASTEPS Principles in AI Governance 14](#_Toc178352829)

[Risk Management plan 15](#_Toc178352830)

[Risk Identification and Assessment: 15](#_Toc178352831)

[Risk Mitigation 16](#_Toc178352832)

[Risk Owners 17](#_Toc178352833)

[Implementation Plan 19](#_Toc178352834)

[Timeline for implementation 19](#_Toc178352835)

[Resources required (e.g. personnel, tools) 19](#_Toc178352836)

[Training and communication strategies 20](#_Toc178352837)

[Communication Strategies: 21](#_Toc178352838)

[Discussion 22](#_Toc178352839)

[Proposed framework and addressed risks 22](#_Toc178352840)

[Challenges 23](#_Toc178352841)

[Comparison to similar frameworks 23](#_Toc178352842)

[Conclusion 25](#_Toc178352843)

[Impact 25](#_Toc178352844)

[Final recommendations 25](#_Toc178352845)

[References 27](#_Toc178352846)

[Appendices 29](#_Toc178352847)

[Appendix A: Roles and Responsibilities in AI Governance 29](#_Toc178352848)

[Appendix B: FASTEPS 30](#_Toc178352849)

[Appendix C: AI Manifesto 31](#_Toc178352850)

[Appendix D: AI Principles 33](#_Toc178352851)

[Appendix E: Data Privacy Policy 35](#_Toc178352852)

[Appendix F: Ethical Use Guidelines 41](#_Toc178352853)

Introduction

A luxury hotel and resort chain, Emerald Hotels and Resorts (Emerald H&R), is contracting with Oracle for a new AI – enhanced ERP system. The AI-powered system is expected to improve operational efficiencies across various departments, including human capital management, customer relationship management (CRM), finance, supply chain, general IT, and operations. This implementation marks a significant step for Emerald H&R as it expands into international markets, requiring scalable solutions that can handle the complexity of a global hospitality business.

Oracle's new system leverages AI for tasks such as credit card transaction anomaly detection, product defect checking in supply chain operations, operational automation, and financial forecasting. While these features hold great potential for enhancing guest satisfaction and operational efficiency, the use of AI brings inherent risks, including concerns over data privacy, bias, discrimination, and compliance with international regulations like the GDPR.

Given these challenges, AI governance and risk management are critical components in ensuring the successful deployment and adoption of this system. The purpose of this document is to define a comprehensive AI Governance Framework and Risk Management Plan that aligns with Emerald H&R’s strategic objectives of expansion, safety, and quality. The framework incorporates trustworthy AI development principles, emphasizing fairness, transparency, and accountability, while embedding ethical considerations into every stage of the AI system lifecycle.

This governance approach will guide the organization in mitigating risks related to privacy, security, bias, and system errors while ensuring compliance with legal standards. By implementing a structured and responsible framework, Emerald H&R will set a strong foundation for utilizing AI technologies in a way that enhances guest experiences while maintaining the integrity of its operations.

Literature Review

## AI Governance Frameworks

Several AI research teams have developed governance and responsible AI frameworks to help organizations manage this emerging technology. In 2024, Lu, Zhu, Xu, Whittle, Zowghi, and Jacquet (2024) presented a comprehensive framework, “Responsible AI Pattern Catalogue (RAIPC),” to address AI system adoption and implementation challenges. This framework outlines multi-level governance patterns, trustworthy process patterns, and RAI-by-design product development (Lu et. al, 2024). The systematic literature review that underpins this framework highlights its robustness and practical applicability across diverse industry settings. The framework applies to all enterprises incorporating AI into their operations, providing guidelines for responsible development and deployment, which serves well for our group project. By adopting the RAIPC, our group can ensure a comprehensive approach to integrating responsible AI practices, thereby enhancing the credibility and sustainability of our project outcomes.

Another group of researchers, Boza and Evgeniou, address the integration of AI principles with existing governance framework (Boza & Evgeniou, 2021). They note an increased need to describe how to implement these AI principles. Through their review, they highlight the current state and possible gaps at the time including appropriate implementation processes. In this project, we hope to address this gap.

## Risk Management

In terms of risks associated with AI, several have been identified including the following: misinformation, prejudice, bias and discrimination, privacy concerns, job losses, and AI control once it surpasses human intelligence are impetuses for safeguards as noted in Camilleri’s 2024 article (Camilleri, 2024). Camilleri provides a broad perspective of risk based on a review of contemporary research for AI policies.

To identify risks for an organization, Hristov and his team developed a Key Risk Indicator (KRI) system that scores businesses on several factors including risk dimensions and drivers (Hristov, Camilli, Chirico, & Mechelli, 2022). The questionnaire helps organizations not only understand their current risks, but also their current processes and if adjustments need to be made.

AI systems should be valid, reliable, safe, secure, resilient, accountable, transparent, explainable, interpretable, privacy-enhanced, and fair with harmful bias managed as noted in Tabassi’s article (Tabassi, 2023). This article defines a risk management framework that addresses the core AI risks, safety, security, privacy accountability, and fairness. The specificity of this framework makes it very useful for the objectives of the project at hand.

From broad risk assessment to specific risks to detailed risk management frameworks, there are multiple key perspectives in the areas of AI and general risk management for enterprises.

## AI in the Hospitality Industry

The hospitality industry is seeing an increased usage of AI to enhance customer relationships and streamline processes in the hospitality industry. According to Jorgarao, AI has “the potential to revolutionize guest experience by increasing guest satisfaction, streamlining operations, and enhancing convenience and comfort” (Jorgarao, 2024, p.199). With this stated, there have been numerous case studies showcasing how AI can improve organizations in hospitality. Companies like Hilton Worldwide, Alibaba's Fly Zoo Hotel, and Marriott International have utilized AI to improve guest interaction such as making reservations, obtaining personalized reservations, and requesting services with AI-powered assistants. By being able to satisfy guest needs with AI, waiting times can be reduced for the customer which leads to better reviews for these organizations.

According to Zade, increased customer expectations along with health and safety concerns have been major shifts in customer behavior/sentiments since the end of COVID-19 (Zade, 2024). Safety and security concerns can be addressed through monitoring potential threats. AI has improved systems to detect malicious incidents such as identity theft or credit card fraud. To promote health, some hotels have keyless entry systems. These measures help avoid unnecessary contact to pathogens on surfaces within these hotels. AI can also help with back-office features and concerns such as supply chain management and staffing. Through using historical data, AI can predict the correct amount of inventory per quarter. AI can also create schedules for staff members based on trends throughout the period.

Overall, AI has been a significant factor in helping increase customer satisfaction and productivity in the hospitality industry.

## Notable Research Gaps

As Lu and team noted there are gaps in contemporary research on responsible AI “transparency, accountability, contestability, and human-centered values” from the perspective of the system (Lu et. al., 2024). Through our investigation and implementation of FASTEPS (see Appendix B), we aim to address some and potentially all of these. In terms of risk management, as Camilleri noted, future research should investigate the “what, how, when, and where protocols to protect and safeguard individuals and entities from possible risks and dangers of AI” (Camilleri, 2024). We aim to address this through our detailed risk management process and adopting strategies employed by Hristov and Tabassi.

Methodology

We are using a scope review methodology to conduct a summary and synthesis of existing AI Governance and Risk Management literature. After reviewing several key responsible AI frameworks and governance frameworks, we decided to adopt a structure that focuses on the main concepts from Zendata’s “AI Governance 101”article. The helpful information from this article allows us to get a base understanding on what needs to be focused on when creating this plan such as data policies and training programs. Our risk management plan is adopting one used by other prominent hospitality enterprises.

The Implementation Plan will consist of a three-phase process. These phases being planning and assessment, design and development, and finally implementation and monitoring. These phases will be completed withing a 9-month timeframe, with certain months being categorized to each phase. This three-phase process allows certain steps to be completed in an agile fashion to ensure the new system can be utilized correctly for business needs.

## Tools, techniques, and frameworks used for risk analysis

The hospitality industry faces multiple risks in terms of AI implementation, especially from the financial standpoint. All these risks should be evaluated and managed correctly for system efficiency in the hospitality industry. Ivo Hristov and his team identified a risk analysis process that we plan to implement in this project. It introduces a balanced scorecard that provides “a flexible approach that can be adapted to integrate RM in strategy execution” (Hristov, Camilli, Chirico, & Mechelli, 2022, p. 844).

 Once addressed, opinions on risk from all departments in the organization including, human capital management, customer relationship, finance, supply chain, general IT, and operations, should be deliberated. These opinions would focus on exactly which risk has the most importance that can reduce its effect on company performance. The proposed risk analysis process allows effective communication within each department to narrow what can be addressed and what can be a potential challenge when creating a new system. To understand these risk indicators, questions on the dimension of a risk indicator can be an issue. For example, the KRI of financial risk should be addressed because financial risk has dimensions of liquidity risk and credit risk. Once all information is obtained, decisions can be made on how to incorporate practices to reduce all risks with the integration of a new system.

Tabassi’s 2023 “AI Artificial Intelligence Risk Management Framework (AI RMF 1.0)” will also be incorporated. It allows risk measurement, prioritization based on impact to business, mapping based on the context of the risk, and governance by individuals. Also, it ensures the AI system is “valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed” (Tabassi, 2023, p. 12).

While incorporating both Hristov’s and Tabassi’s ideas with our IT and AI governance principles, the risks could be satisfied in an effective manner while lining up with the system’s properties to ensure a trustworthy AI System.

## Sources of data and information

The primary sources of data and information include Zendata’s AI Governance, Tabassi’s risk management plan, and Hristov’s Risk Indicator process. These sources of data will be helpful pieces of information that allow certain frameworks to be structured in a correct and effective manner.

AI Governance Framework

The AI governance framework for Emerald H&R is designed to integrate ethical use, regulatory compliance, and risk management across its AI systems. This governance model aligns with the company’s strategic goals, which focus on expansion, safety, and quality, while fostering transparency, fairness, and security.

 As Emerald expands into international markets, the framework ensures that AI technologies can scale effectively. This involves adopting global standards and best practices for AI, enabling the seamless deployment of AI systems across various departments and regions. AI-enhanced customer interactions, such as language translation and personalized recommendations, are also part of this strategy to maintain service consistency.

The framework emphasizes data privacy and secure AI usage. By ensuring compliance with data protection laws and implementing rigorous monitoring of AI systems, Emerald can enhance guest safety and trust. Prioritizing the security of AI systems also reduces the risk of data breaches, thus preserving the integrity of customer data.

Quality service is central to guest satisfaction. The framework ensures that AI-powered services, such as customer service automation, room personalization, and guest feedback analysis, are held to high operational standards. Continuous monitoring of AI performance contributes to maintaining a high level of service quality, thereby enhancing guest experiences and promoting loyalty.

## Policies and Procedures Included in the Framework

The AI governance framework incorporates a range of policies and procedures to ensure responsible AI usage. As per (Z*endata, 2024*), key components of the framework include:

1. Data Privacy Policy: This policy outlines how personal data is collected, stored, processed, and shared, with a focus on complying with international regulations like GDPR and CCPA. Data privacy must be prioritized in AI systems to maintain guest trust and avoid legal penalties. (See Appendix E for the Data Privacy Policy)

2. Ethical Use Guidelines: These guidelines establish the principles of fairness, transparency, and accountability. AI systems must be designed to avoid bias and ensure equitable treatment of all guests, particularly in personalized services and guest feedback analysis.(See Appendix F for Ethical Use Guidelines)

3. Bias Mitigation Protocols: A procedure to identify, assess, and mitigate biases in AI algorithms is essential for fair AI operations. Continuous monitoring and feedback loops should be employed to adjust algorithms and reduce disparities.

4. Incident Response Plan: The framework includes a clear plan for responding to incidents such as data breaches, AI errors, or system failures. The incident response team must act quickly to resolve issues and prevent further harm to guests or operations.

5. Training and Awareness Programs: Staff training is critical for the effective governance of AI systems. Employees must be aware of AI capabilities, governance policies, and ethical considerations. These programs should also include awareness of potential AI system limitations and risks, empowering staff to make informed decisions.

## Roles and Responsibilities within the Governance Structure

A clear governance structure is crucial to managing AI responsibly (Sinkinson, 2024). At Emerald H&R, the following roles will be defined: The Chief AI Officer (CAIO) oversees AI initiatives, ensuring alignment with business goals and compliance with ethical standards, while the AI Ethics Officer focuses on fairness, transparency, and preventing bias. The Data Steward ensures data quality and legal compliance, managing the data lifecycle for unbiased AI training. The AI Risk Manager handles identifying and mitigating risks related to AI security and biases, and the IT Governance Committee provides oversight, approving AI deployments and monitoring their alignment with governance standards. (See Appendix A for description of the roles).

## Continuous Monitoring and Feedback Mechanisms

To maintain the effectiveness of the AI systems, the governance framework includes continuous monitoring and feedback processes. These mechanisms enable the early identification of issues such as algorithmic bias, data inaccuracies, and system vulnerabilities. Monitoring AI performance and collecting stakeholder feedback also allows for the ongoing refinement of AI applications to meet the evolving needs of guests and employees.

## FASTEPS Principles in AI Governance

The AI governance framework at Emerald H&R follows the FASTEPS principles: Fairness ensures unbiased guest interactions, Accountability assigns clear responsibility for AI decisions, and Safety guarantees rigorous testing to protect guests and operations. Transparency allows stakeholders to understand AI processes, while Engagement ensures guest and staff concerns are addressed. Privacy safeguards personal data, and Security protects sensitive information and AI systems from breaches. (See Appendix B for details about each principle).

The responsible deployment of AI systems at Emerald H&R is tightly integrated with the company's core strategic objectives of expansion, safety, and quality. By establishing clear policies, assigning specific roles and responsibilities, and following the FASTEPS principles, the organization can effectively use AI to enhance guest experiences while upholding ethical standards. Continuous monitoring of AI systems and active stakeholder engagement will ensure the company remains flexible in adapting to new technological advancements and regulatory requirements. This approach allows Emerald H&R to maintain the integrity of its AI operations and address challenges as they arise.

Risk Management plan

The purpose of the Risk Management Plan is to outline the risks and mitigation strategies associated with the implementation of an Oracle AI-enhanced ERP System spanning across several key business functions including human capital, customer relationship management, finance, supply chain, IT and operations. The new ERP system is a cloud-based solution that leverages artificial intelligence and natural language processing to drive capabilities like credit card transactions anomaly detection, product defect checking, operation automation, and financial forecasting. This document presents the findings of the Information Security Risk Assessment conducted by the Information Security team and proposes a risk plan to address the identified risks and align the service implementation with our company security policies and best practices. The risk management plan addresses core AI risks, including safety, security, privacy, accountability, and fairness. To identify key risks, we utilized Hristov’s Key Risk Indicator system that scores businesses on several risk factors as outlined in his study (Hristov et. al., 2022).

## Risk Identification and Assessment:

The Information Security Risk Assessment conducted a thorough risk assessment to identify operational, compliance, security, and AI-specific risks. The risk assessment identified several risk findings related to the ERP implementation and classified, as shown in the table below.

**Table 1**

*Risk Identification & Assessment*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | Findings ID # | Impact Score  | Likelihood  | Risk Description  |
| Regulatory & Compliance  | FIND-10613 | High | Medium | Due to the highly sensitive nature of customer data, including credit card information and personal preferences, there are additional regulatory challenges. |
| Data Privacy  | FIND-10614 | High | Medium | The AI system processes sensitive guest data (such as preferences, room choices, and financial transactions), making data privacy critical. Compliance with international data protection regulations like GDPR is essential. |
| AI Bias | FIND-10615 | Medium | Medium | There is concern about AI bias, especially in automated pricing models and guest service personalization. AI might unintentionally favor certain groups, leading to customer dissatisfaction or legal issues. |
| Security Risk | FIND-10616 | High | Medium | With AI integrated into the operations, the attack surface for cybersecurity threats increases. Protecting sensitive guest data and preventing unauthorized access is a top priority. |
| Operational Errors | FIND-10618 | High | Medium | The reliance on AI for real-time decision-making, such as dynamic pricing and predictive maintenance, introduces the risk of system errors that could disrupt operations or lead to revenue losses. |
| System Down Time | FIND-10619 | High | Medium | Unplanned system outages can severely impact business operations, customer service & financial reporting. |

## Risk Mitigation

The risk mitigation provides the recommended actions to reduce or eliminate the risks identified by the risk assessment. The mitigation actions are aligned with the applicable security policies and controls.

**Table 2**
*Risk Mitigation Descriptions*

|  |  |  |
| --- | --- | --- |
| Risk | Findings ID # | Mitigation Description  |
| Regulatory & Compliance  | FIND-10613 | * Regularly Audit ERP system to ensure compliance with local & internation regulations
* Utilize Oracle’s built in compliance tools and regular update them based on regulatory changes
* Utilize legal experts to interpret regulatory requirements
 |
| Data Privacy  | FIND-10614 | * Encrypt sensitive data both in transit and at rest
* Implement strict access controls based on roles
* Develop & enforce comprehensive data privacy policies & procedures
 |
| AI Bias | FIND-10615 | * Regularly audit & test AI algorithms to detect & address bias
* Use diverse and representative datasets to train models to minimize bias
* Implement human oversight for critical AI-driven decisions
 |
| Security Risk | FIND-10616 | * Strategically implement Multi Factor Authentication
* Deploy advanced measures including firewalls, intrusion detection systems and regularly conduct vulnerability assessments
 |
| Operational Errors | FIND-10618 | * Phased rollout of AI systems will allow for Realtime human oversight during the initial implementation phase
* Conduct thorough training for all users on the new ERP system including AI features
* Establish QA processes to review audit AI driven tasks
 |
| System Down Time | FIND-10619 | * Develop & test a business continuity plan to ensure operations can continue during disruptions
* Implement redundant systems and failover solutions to maintain operational continuity
* Review and update operation procedures to address potential risk
 |

## Risk Owners

The system will be subject to ongoing risk monitoring, ensuring that any potential issues related to AI bias, security vulnerabilities, or data breaches are addressed immediately. A dedicated team will oversee these activities to ensure the AI tools perform effectively and safely across all hotel locations and report to the Information Security Team.

* Compliance Team: Manages regulatory & compliance risk.
* Data Privacy team: Oversees data privacy and security risk.
* AI/Data Science Team: Handles algorithm bias and operational errors.
* IT Team: Responsible for scalability, operational risk & system downtown.

Implementation Plan

## Timeline for implementation

Due to the scale and complexity of this implementation, we predict that the AI governance and risk management implementation timeline will last at least 9 months but may encompass several years to achieve a comprehensive governance approach when considering our multiple global headquarters and the various local regulations we need to account for.

**Table 3**
*Implementation Plan*

|  |  |  |
| --- | --- | --- |
| Phase 1: Planning & Assessment | Month 1 | Define AI principles and AI manifesto (See Appendix A and B), establish AI Governance Council, conduct initial quality assessment, form Risk Management Team |
| Month 2 | Develop AI governance framework, identify potential risks, conduct risk identification workshops, perform AI product intake |
| Perform cross-functional workshops, finalize project timeline and milestones, develop quality metrics |
| Month 3 | Finalize project timeline, develop quality metrics, prioritize tasks, develop monitoring process |
| Phase 2: Design & Development | Month 4 | Develop AI governance tools and solutions, design risk identification tools, develop user guidelines |
| Risk assessment using Oracle tools, finalize risk management strategies |
| Month 5 | Create training collateral, hold stakeholder training, establish communication processes |
| Month 6 | Scalability tests with Oracle, finalize risk management plan, apply adjustments |
| Phase 3: Implementation & Monitoring | Month 7 | Start data migration, perform testing, implement real-time monitoring and incident protocols |
| Month 8 | Feedback sessions, evaluate effectiveness of AI governance, continue risk mitigation |
| Month 9 | Full integration into business operations, final compliance assessments, conduct training, risk monitoring summaries |

## Resources required (e.g. personnel, tools)

Emerald H&R’s AI governance and risk management implementation team along with the AI council will be needed. An ERP implementation team would also be required, in which they would communicate with Oracle representatives about the system. This team would also have to create an ERP implementation plan and follow the system development life cycle (SDLC) steps. Additional personnel would be a team to discuss best practices while using this new AI system. Active involvement in all departments allows for potential future issues to be addressed. Overall, these will foster safe and effective AI use at Emerald H&R.

## Training and communication strategies

To effectively implement AI within Emerald H&R while mitigating risks such as privacy concerns, bias, and system errors, it is crucial to develop comprehensive training and communication strategies. This involves equipping employees with the knowledge and skills to utilize AI tools responsibly and ethically, ensuring they are aware of the governance framework in place and their roles within it (Karagiannis, 2024).

**Table 4**

*Training Modules and Expected Outcomes*

|  |  |  |  |
| --- | --- | --- | --- |
| MODULE | DESCRIPTION | TRAINING METHOD | EXPECTED OUTCOME |
| Data Privacy | Understanding data privacy laws (e.g., GDPR, CCPA), and how AI systems should handle personal data. | Interactive workshop, case studies | Employees understand key data privacy requirements and how AI systems should be compliant. |
| Ethical AI Use | Principles of ethical AI, including fairness, transparency, and avoiding bias in AI models. | Scenario-based discussions, role-playing | Participants grasp how to design, develop, and deploy ethical AI solutions while mitigating biases. |
| Risk Management | Identifying and managing risks associated with AI, including technical, legal, and reputational risks. | Simulations, risk analysis workshops | Employees are trained to identify and mitigate risks in AI development and deployment. |
| Compliance with Regulations | Understanding industry-specific regulations and compliance requirements for AI applications. | Seminars, regulatory deep dives | Employees are equipped to ensure AI systems comply with relevant industry regulations. |
| Bias and Discrimination | Detecting and mitigating bias in AI algorithms to prevent unfair treatment. | Real-world case discussions, tools demo | Employees understand how to recognize bias in AI and take steps to reduce or eliminate it in AI models. |
| Simulations and Scenario Planning | Engaging employees in operational simulations where they face real-life scenarios involving AI. | Simulators and scenario planning | Participants develop decision-making skills and understand impact on business operations and customers. |

## Communication Strategies:

**Table 5**
*AI Communication Strategy*

|  |  |
| --- | --- |
| Section | Description |
| Establish an AI Governance Communication Plan | Ensure all employees are familiar with AI governance policies and their role in the framework. |
| Clear Policies Document | Develop a comprehensive document outlining AI policies, ethical guidelines, data privacy standards, and incident response protocols. |
| Regular Updates and Announcements | Use internal channels (newsletters, intranet) to share updates on AI initiatives and policy changes. |
| Raise Awareness of AI Governance Framework | Foster a culture of ethical AI use through kick-off meetings, workshops, poster campaigns, and digital tools (videos, infographics). |
| Encourage Two-Way Communication | Establish feedback channels and hold open Q&A sessions to discuss AI governance and address concerns. |
| Alignment with Strategic Objectives | Align AI governance with Emerald Hotels' goals (expansion, safety, quality), preparing employees for scalable AI systems. |

These strategies help ensure that employees are well-informed, feel involved, and are ready to work with AI in the line with the company’s goal.

Discussion

Proposed framework and addressed risks

Our proposed AI governance framework for Emerald H&R will integrate ethical use, regulatory compliance, and risk management across our organization’s global AI systems. The strategic goals of our company focus on the following:

* Expansion – we aspire to expand in the international market by becoming a top choice for guests when they choose a location to stay at,
* Safety - we aspire to provide secure transactions and psychologically and physically safe hotel and resort accommodations when guests stay at any of our locations, and
* Quality – we aspire to provide the highest level of quality for all interactions, rooms, and amenities used.

The AI governance framework proposed addresses these key objectives by fostering scalability for expansion, safety in the design of our solution that prevents data breaches while providing peace of mind and embedding efficiency in the key principles which will help to enhance quality of delivery of hospitality services.

The proposed AI governance framework will address risks identified earlier regarding privacy, security, bias/discrimination, and system errors. This will be accomplished through fostering

 Transparency – the guidelines will be clearly outlined and available for all members of the organization along with embedded in our marketing to future and recurring customers,

Fairness – prevent discrimination and bias through ensuring equitable access to features and thorough investigation of any ethical misconduct or lack of compliance to the governance and enforcement will be expected at all levels of the organization, and

Security – embedded in the design of the framework and the AI-enhanced products.

The framework emphasizes data privacy and secure AI usage. By ensuring compliance with data protection laws and implementing rigorous monitoring of AI systems, Emerald can enhance guest safety and trust. Prioritizing the security of AI systems also reduces the risk of data breaches, thus preserving the integrity of customer data.

## Challenges

The major challenges our organization may face while implementing this framework is ensuring compliance at all levels of the organization, identifying and making necessary adjustments, and the ever-evolving nature of AI technologies.

To navigate the challenge of ensuring compliance at all levels of the organization. Our team clearly defines roles and responsibilities as seen in our risk management plan and will have training for all staff members and enlist champions for ethical practice in each department. There will be a clear communication process and investigation protocol for any breaches or deviations.

In terms of identifying and making necessary adjustments, our council will facilitate continuous monitoring of AI governance practices and performance. We will hold regular focus groups and surveys to determine what is working and what can be adjusted.

The ever-evolving nature of AI technologies is a challenge for our team. We and other leaders in the organization will need to stay current on trends, updated training, and continuously evaluate whether our current policies will need to be re-evaluated. We will remain true to the primary goals of this organization and employ FASTEPS principles of fairness, accountability, safety, transparency, engagement, privacy, and security.

## Comparison to similar frameworks

Compared to other frameworks and plans discussed in the literature the one developed for Emerald H&R is more comprehensive. The RAIPC had primarily focused on Responsible AI, but did not address the “human-centered values” as Lu and team noted in their analysis of limitations (Lu et. al, 2024) We were able to address this through the FASTEPS principles (see Appendix B). There was also a gap in the “what, how, when, and where” (Camilleri, 2024). We addressed this through very a detailed governance framework, risk management plan, and implementation plan. Though each framework holds much merit. We wanted to use a framework that addresses all the areas of our organization and would have the scale to work with a global organization.

Despite potential challenges, we may have with the size of our organization, reviewing for adjustments, and ever-evolving nature of AI technologies, we are confident in the organizations ability to implement and adapt the proposed method as it is well-researched and established.

Conclusion

As Emerald H&R implements this new AI-enhanced ERP system, we aim to stay true to our strategic objectives of expansion, safety, and quality. After reviewing key literature and theories through a scoping methodology we have narrowed down to the AI Governance framework and risk management plan that will work best for our organization. The AI Governance Framework authored by (Zendata, 2024), addresses concepts such as the model governance process, policies/procedures/standards, risk, security, and compliance, operating model, organizational roles and responsibilities, monitoring, tools and technologies while employing FASTEPS principles of fairness, accountability, safety, transparency, ethics, privacy, and security. The risk management plan we formulated addresses the pattern we will use to identify and assess, risk mitigation, risk owners, and monitoring and reporting processes. The 9-month implementation plan undergoes a three-phase process including planning and assessment, design and development, implementation and monitoring which is the longest phase.

## Impact

The governance framework will ensure that we meet our strategic objectives, but also mitigate risks in our implementation of the new Oracle AI-enhanced ERP software. The risk management plans outline clear instructions to identify risks, mitigate risks, recognize owners, and monitor and report risks. This process will be useful for our organization as we seek to establish a manner to closely monitor and address any identified risks.

## Final recommendations

We recommend our team continuously make updates to the AI governance and risk management plan as we learn more about AI and increasingly integrate it into our business practices. We will keep the AI Council as a standing body to provide direction and regular updates on changes to the governance model and expectations. We recommend other organizations consider our approach and make regular adjustments.

References

Boza, P., & Evgeniou, T. (2021). Implementing AI principles: frameworks, processes, and tools.

SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.3783124>

Camilleri, M. A. (2023). Artificial Intelligence Governance: Ethical Considerations and

implications for social responsibility. *Expert Systems*, *41*(7). [https://doi.org/https://doi.org/10.1111/exsy.13406](https://doi.org/https%3A/doi.org/10.1111/exsy.13406)

Hristov, I., Camilli, R., Chirico, A., & Mechelli, A. (2022). . *Production Planning &amp; Control*, *35*(8), 842–855.
 <https://doi.org/10.1080/09537287.2022.2140086>

Jogarao ,M.(2024). AI in the Hospitality Industry Revolutionizing Guest Experience. *Technology and Luxury Hospitality*,1,199-210. <https://www.taylorfrancis.com/chapters/edit/10.4324/9781003488248-14/ai-hospitality-industry-malla-jogarao>

Karagiannis, M. (2024, February 12). AI and Ethics: What Hoteliers Need to Know - Hotel Tech - Medium. Medium. https://medium.com/hotel-tech/ai-and-ethics-what-hoteliers-need-to-know-69b4b73c6922

Lu, Q., Zhu, L., Xu, X., Whittle, J., Zowghi, D., & Jacquet, A. (2024)*. Responsible AI pattern*

*catalogue: A collection of best practices for AI Governance and Engineering. ACM Computing Surveys,* 56(7), 1–35.

<https://doi.org/10.1145/3626234>

Sinkinson, T. (2024, September 5). Who is responsible for artificial intelligence governance? Trilateral Research. https://trilateralresearch.com/artificial-intelligence/who-is-responsible-for-artificial-intelligence-governance

Tabassi, E. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. <https://doi.org/10.6028/nist.ai.100-1>

Zade, Aarohi. (2024). TRANSFORMING HOSPITALITY THE DIGITAL REVOLUTION IN

POST-PANDEMIC, *International Journal of Cultural Studies and Social Sciences* 20. 42. https://www.researchgate.net/publication/383154895

Zendata*. (2024). AI Governance 101: Understanding the Basics and Best Practices. Zendata.*

[*https://www.zendata.dev/post/ai-governance-101-understanding-the-basics-and-best-practices*](https://www.zendata.dev/post/ai-governance-101-understanding-the-basics-and-best-practices)

# Appendices

## Appendix A: Roles and Responsibilities in AI Governance

1. Chief AI Officer (CAIO): The CAIO oversees all AI-related initiatives and ensures alignment with business objectives and ethical standards. They are responsible for integrating AI systems across various hotel departments and ensuring compliance with AI governance policies.

2. AI Ethics Officer: This role focuses on safeguarding ethical practices in AI implementation, including fairness, transparency, and accountability. The AI Ethics Officer must regularly assess AI systems to ensure they do not perpetuate discrimination or bias, and that they align with the company’s values.

3. Data Steward: The Data Steward ensures data integrity and quality, focusing on compliance with data protection laws and regulations. This role also involves managing the data lifecycle and ensuring that AI models are trained on diverse, unbiased datasets.

4. AI Risk Manager: This individual is responsible for identifying, assessing, and mitigating risks associated with AI systems. Their primary focus includes the security of AI systems, mitigating algorithmic biases, and ensuring compliance with data protection standards.

5. IT Governance Committee: The IT Governance Committee provides oversight for all technology systems, including AI developments. This committee evaluates AI use cases, approves AI system deployments, and monitors ongoing AI performance to ensure alignment with governance standards.

## Appendix B: FASTEPS

1. Fairness: AI algorithms must promote equitable treatment of all guests, avoiding biases that could harm customer interactions.

2. Accountability: The governance structure ensures that all AI outcomes are traceable, with clear responsibility assigned to individuals or teams for decision-making.

3. Safety: AI systems undergo rigorous testing to ensure guest safety and prevent operational failures.

4. Transparency: The company remains open about how AI systems operate, ensuring that stakeholders understand the decisions informed by AI.

5. Engagement: Stakeholder engagement is key to AI governance, ensuring that concerns from guests and staff are addressed.

6. Privacy: Robust data privacy measures ensure that personal data is handled securely and transparently.

7. Security: Advanced security protocols protect sensitive data and AI systems from breaches or misuse.

## Appendix C: AI Manifesto

|  |  |
| --- | --- |
| **DO’s** | **DON’Ts** |
| **AI + human cooperation:** AI should augment and complement human intelligence, creativity, and decision-making, not replace or undermine them, and respect human autonomy, agency, diversity, flourishing, and well-being. | **No Malicious Use**: AI should not be used for harmful, unlawful, or unethical purposes. |
| **Data driven culture:** AI should use high-quality, reliable, and relevant data that reflects the reality and diversity of the world and the people, and be transparent and explainable about data collection, analysis, and use, while respecting the rights, interests, consent, privacy, and security of data subjects and providers. | **Respect Human Dignity**: AI should not violate or undermine human dignity, rights, or values. |
| **Unbiased data-driven outcomes:** AI should be fair and inclusive, and avoid or mitigate any harmful biases, discrimination, or injustice, and respect and promote the principles of equality, diversity, non-discrimination, human dignity, and human rights, and provide human oversight, review, feedback, correction, and redress mechanisms. | **No Deception**: AI should not spread or create misinformation, disinformation, or propaganda. |
| **Transparency in products:** AI should be clear and understandable about its capabilities, limitations, and impacts, and communicate them truthfully, accurately, and accessibly, and disclose its purpose, functionality, and intended use, and provide relevant information about its performance, reliability, and risks, and enable users and stakeholders to make informed choices, and exercise control and responsibility over AI. | **Avoid Manipulation**: AI should not be used for manipulation, deception, coercion, or exploitation. |
| **Critical thinking:** AI should encourage and enable critical and ethical reflection, questioning, and challenge, and foster a culture of curiosity, creativity, innovation, and learning. AI should be open to scrutiny and evaluation, and support the development of ethical and responsible standards, norms, and best practices. | **No Recklessness**: AI should not be used in a reckless, irresponsible, or negligent manner. |
| **Sustainable AI:** AI should be aligned with and contribute to the sustainable development and well-being of humanity and the planet, and respect and protect the natural resources, ecosystems, and biodiversity that sustain life on Earth. AI should minimize its negative environmental impacts, and support the transition to a low-carbon, circular, and green economy, and enhance resilience and adaptation to global challenges. | **Legal and Ethical Compliance**: AI should not be used to evade or contradict laws or ethical standards. |
|  | **No Abuse or Violence**: AI should not be used to cause abuse, harm, violence, conflict, or instability. |

## Appendix D: AI Principles

1. **Human-Centric Augmentation**:
2. **Complement, Don’t Replace**: AI should enhance human intelligence and decision-making without undermining human autonomy.
3. **Respect for Human Values**: AI should respect and promote human autonomy, agency, diversity, and well-being.
4. **Transparency**:
	1. **Clear Communication**: AI should clearly communicate its capabilities, limitations, and impacts truthfully and accurately.
	2. **Disclosure**: AI should disclose its purpose, functionality, and intended use.
	3. **Performance Information**: Provide relevant information about AI's performance, reliability, and risks.
	4. **Informed Choices**: Enable users and stakeholders to make informed decisions and exercise control over AI.
5. **Data Integrity**:
	1. **High-Quality Data**: AI should use reliable and relevant data that reflects the diversity of the world.
	2. **Transparent Data Practices**: Be clear about data collection, analysis, and use.
	3. **Respect Privacy**: Respect the rights, interests, consent, privacy, and security of data subjects and providers.
6. **Encouraging Critical Thinking**:
	1. **Promote Inquiry**: AI should encourage critical and ethical reflection and questioning.
	2. **Support Innovation**: Foster a culture of curiosity, creativity, and learning.
	3. **Openness to Scrutiny**: Be open to evaluation and support ethical standards and best practices.
7. **Fairness and Inclusivity**:
	1. **Avoid Bias**: AI should avoid or mitigate harmful biases and discrimination.
	2. **Promote Equality**: Respect and promote principles of equality, diversity, and non-discrimination.
	3. **Human Rights**: Uphold human dignity and human rights.
	4. **Oversight and Redress**: Provide mechanisms for human oversight, review, feedback, correction, and redress.
8. **Sustainability**:
	1. **Environmental Responsibility**: Align AI with sustainable development and the well-being of humanity and the planet.
	2. **Minimize Environmental Impact**: Reduce negative environmental impacts and support a low-carbon, circular economy.
	3. **Enhance Resilience**: Contribute to resilience and adaptation to global challenges.

## Appendix E: Data Privacy Policy

**Data Privacy Policy for Emerald Hotels & Resorts**

Effective Date: September 27, 2024

Policy Owner: Chief Data Officer (CDO)

Reviewed by: Legal & Compliance Department

Next Review Date: September 27, 2025

**1. Purpose**

This Data Privacy Policy outlines how Emerald Hotels & Resorts ("Emerald H&R") collects, stores, processes, and shares personal data in compliance with applicable international regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other relevant data protection laws. Our goal is to ensure that personal data is handled securely, ethically, and transparently, respecting the privacy of our guests, employees, and partners.

**2. Scope**

This policy applies to all personal data processed by Emerald H&R, including data collected through our hotel operations, websites, mobile applications, guest services, AI-powered systems, and other communication channels. It applies to all employees, contractors, and third-party service providers who handle personal data on behalf of Emerald H&R.

**3. Key Definitions**

* Personal Data: Any information related to an identified or identifiable natural person. This includes data such as names, email addresses, phone numbers, billing details, guest preferences, and any other information that can be linked to a specific individual.
* Processing: Any operation or set of operations performed on personal data, including collection, recording, storage, modification, retrieval, transmission, and deletion.
* Data Subject: An individual whose personal data is being processed by Emerald H&R.

**4. Principles of Data Processing**

Emerald H&R adheres to the following principles when processing personal data:

* Lawfulness, Fairness, and Transparency: Personal data shall be processed lawfully, fairly, and in a transparent manner.
* Purpose Limitation: Personal data shall be collected for specified, explicit, and legitimate purposes, and not processed in a manner that is incompatible with those purposes.
* Data Minimization: Personal data collected shall be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
* Accuracy: Personal data shall be accurate and kept up to date. Inaccurate data shall be corrected or deleted without delay.
* Storage Limitation: Personal data shall be kept in a form that permits identification of data subjects only for as long as necessary for the purposes for which it is processed.
* Integrity and Confidentiality: Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage, using appropriate technical and organizational measures.

**5. Data Collection**

Emerald H&R collects personal data through various channels, including but not limited to:

* Hotel bookings and reservations
* Customer interactions with AI-powered services (e.g., virtual concierge, personalized recommendations)
* Website and mobile app forms
* Guest feedback surveys and reviews
* On-property services such as check-ins, dining, and spa treatments

The types of personal data collected include:

* Contact details (name, phone number, email address)
* Financial information (payment details, billing information)
* Guest preferences (room preferences, dietary restrictions, service requests)
* Transaction data (booking history, spending behavior)
* Technical data (IP addresses, device information)

**6. Legal Basis for Processing**

Emerald H&R processes personal data based on the following legal grounds:

* Consent: Where data subjects have provided explicit consent (e.g., marketing communications).
* Contractual Obligation: Processing is necessary for the performance of a contract (e.g., fulfilling hotel reservations).
* Legal Obligation: Processing is required to comply with legal obligations (e.g., tax, accounting, and compliance reporting).
* Legitimate Interests: Processing is necessary for Emerald H&R's legitimate business interests, provided those interests do not override the fundamental rights of the data subjects (e.g., fraud prevention, improving guest experience).

**7. Data Subject Rights**

Emerald H&R is committed to ensuring that data subjects can exercise their rights under applicable data protection laws. These rights include:

* Right to Access: Data subjects may request access to the personal data we hold about them.
* Right to Rectification: Data subjects may request correction of inaccurate or incomplete personal data.
* Right to Erasure: Data subjects may request the deletion of their personal data in certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected.
* Right to Restrict Processing: Data subjects may request to limit the processing of their personal data under certain conditions.
* Right to Data Portability: Data subjects may request to receive their personal data in a structured, commonly used format and have it transmitted to another controller.
* Right to Object: Data subjects may object to the processing of their personal data, including for direct marketing purposes.
* Right to Withdraw Consent: Data subjects have the right to withdraw consent to the processing of their data at any time.

Requests to exercise these rights should be submitted to privacy@emeraldHR.com, and will be responded to within one month.

**8. Data Sharing and Third Parties**

Emerald H&R may share personal data with the following categories of recipients:

* Service Providers: Third-party vendors who assist us with hotel operations, AI service providers, payment processing, marketing, and customer relationship management.
* Legal Authorities: In cases where disclosure is required by law or to protect the rights, property, or safety of Emerald H&R or others.
* Affiliates and Business Partners: For the purposes of improving service delivery, guest experience, and operational efficiency.

All third parties who receive personal data from Emerald H&R are required to sign a Data Processing Agreement (DPA), ensuring that they adhere to the same standards of privacy and security.

**9. Data Security**

Emerald H&R implements a range of technical and organizational measures to safeguard personal data against unauthorized access, loss, and misuse. These measures include:

* Encryption: Personal data is encrypted both in transit and at rest using industry-standard encryption technologies.
* Access Controls: Access to personal data is restricted to authorized personnel who require it for the purposes of performing their job functions.
* Regular Audits: Regular security audits and vulnerability assessments are conducted to ensure the effectiveness of our security measures.
* Incident Response Plan: In the event of a data breach, Emerald H&R will notify affected data subjects and relevant authorities within 72 hours, as required by law.

**10. Data Retention**

Emerald H&R retains personal data only for as long as necessary to fulfill the purposes for which it was collected or to comply with legal, accounting, or reporting requirements. Personal data that is no longer required will be securely deleted or anonymized.

* Guest data: Retained for 7 years following the conclusion of the guest’s stay, unless a longer retention period is required by law.
* Financial data: Retained for 10 years in accordance with accounting regulations.

**11. International Data Transfers**

Emerald H&R operates globally, and personal data may be transferred to and processed in countries outside the European Economic Area (EEA). When transferring data internationally, Emerald H&R ensures that appropriate safeguards are in place to protect the data, such as Standard Contractual Clauses (SCCs), or by ensuring the recipient is part of the EU-US Privacy Shield Framework or equivalent.

**12. Employee Training and Awareness**

All employees and contractors who handle personal data are required to undergo mandatory data privacy training. Regular refresher courses and updates on data protection laws are provided to ensure continued compliance and awareness.

**13. Policy Review**

This Data Privacy Policy is reviewed and updated annually or as required to reflect changes in data protection laws, business practices, or new technologies. Any substantial changes to the policy will be communicated to data subjects via our website and other appropriate channels.

**14. Contact Information**

If you have any questions about this policy or would like to exercise your rights as a data subject, please contact us:

* Email: privacy@emeraldHR.com
* Mailing Address: Emerald Hotels & Resorts Data Privacy Department
* 123 Emerald Street, Suite 456 Orlando, FL 32801, USA

## Appendix F: Ethical Use Guidelines

**Ethical Use Guidelines for Employees Using AI Systems**

These guidelines are for employees who interact with AI systems, particularly in providing personalized services and analyzing guest feedback. By following these principles, you help ensure that our AI systems remain fair, transparent, and accountable.

1. Ensure Fairness

- When using AI systems, make sure that decisions are unbiased and equitable. The system should never discriminate based on race, gender, age, or any other protected characteristic.

- Regularly review the AI outputs to ensure fairness and report any potential biases or issues.

2. Be Transparent with Guests

- Always inform guests when AI is involved in their personalized service or feedback analysis. Be ready to explain how AI affects their experience and answer any questions they may have.

3. Be Accountable

- Take responsibility for AI-driven decisions. If a guest feels that a decision was unfair or incorrect, escalate the issue for human review and make any necessary adjustments.

- Follow the established process for addressing guest concerns and ensure issues are resolved promptly and fairly.

4. Protect Guest Privacy

- Handle guest data responsibly. Ensure that any data used by AI systems is secure and used only for its intended purpose.

- Respect guests' choices if they opt out of AI-driven services, and make sure their experience remains consistent.

5. Watch for Bias

- Regularly monitor the AI systems you work with to detect any potential biases. If you notice anything that could lead to unfair treatment, report it to the appropriate team.

- Use diverse and representative data when feeding AI systems to reduce the risk of bias.

6. Continuously Improve

- Stay informed about updates and improvements to the AI systems you use. Your feedback and insights help keep the system fair and effective.

- Participate in training and discussions on ethical AI use to ensure you’re up to date with best practices.

By following these guidelines, you help maintain the integrity of our AI systems, ensuring they are used responsibly and that all guests are treated fairly and equitably.