

The Implementation of Operational Risk Management Using the HIRARC Method (Hazard Identification, Risk Assessment, and Risk Control) in the Human Resources and Correspondence Division at PPSDM Migas

Dzurrotun Nasikhah¹, Mohammad Khusnu Milad²

State Islamic University of Sunan Ampel Surabaya^{1,2}

dzurrotunnasikhah21@gmail.com¹, m.milad@uinsa.ac.id²

Abstract

Risk management has become an essential component in ensuring organizational effectiveness, particularly within government institutions that manage public services and administrative accountability. The Human Resources and Correspondence Division at PPSDM Migas plays a strategic role in handling personnel administration, certification documentation, and official correspondence processes. The complexity of these administrative activities creates potential operational risks, including human error, document mismanagement, delays in correspondence processing, and data inaccuracies, which may affect institutional credibility and service quality. This study aims to identify, assess, and control operational risks within the Human Resources and Correspondence Division using the HIRARC (Hazard Identification, Risk Assessment, and Risk Control) method. The research applies a descriptive qualitative approach supported by a literature review and observational data. Risk assessment is conducted by evaluating likelihood and severity levels to determine risk categories. The findings indicate that several identified risks fall into Moderate and High categories, particularly those related to documentation errors and delays in administrative processing. Therefore, risk control strategies such as digitalization of records, strengthening standard operating procedures (SOPs), and capacity-building programs for staff are recommended to reduce risks to acceptable levels.

Keywords: Operational Risk Management; HIRARC; Human Resources Administration; Correspondence Management; Government Institution; Risk Control Strategy

INTRODUCTION

The *Pusat Pengembangan Sumber Daya Manusia Minyak dan Gas Bumi (PPSDM Migas)* located in Cepu, Blora, Central Java, is a technical training institution under the Ministry of Energy and Mineral Resources of the Republic of Indonesia. PPSDM Migas holds a strategic mandate in strengthening national human resource capacity in the oil and gas sector through competency-based training, certification programs, applied laboratory practices, and industry collaboration initiatives. According to BPSDM ESDM (2025), PPSDM Migas functions as a national center for professional development aimed at ensuring the availability of competent and certified personnel to support Indonesia's energy sustainability and industrial competitiveness. The institutional role of PPSDM Migas is therefore not only operational but also strategic in safeguarding workforce standards within a high-risk and capital-intensive industry.

As a government-administered training and certification body, PPSDM Migas relies heavily on structured administrative governance to ensure regulatory compliance and institutional accountability. The Human Resources and Correspondence Division plays a central role in maintaining personnel records, certification documentation, official letters, archival management, and institutional communication flows. Administrative accuracy is essential because training certificates and competency records constitute legal documents recognized within national regulatory frameworks. As emphasized by Asnawi, Larasati, and Syahrir (2023), effective public sector administration significantly influences institutional legitimacy and service quality. Therefore, HR and correspondence management serve as foundational pillars supporting both legal validity and organizational credibility.

Despite the structured bureaucratic environment, operational risks remain inherent in public

office administration. Operational risk is generally defined as the risk of loss resulting from inadequate or failed internal processes, human factors, system breakdowns, or external events (Basel Committee on Banking Supervision 2011). In government institutions, administrative units are particularly vulnerable to process inefficiencies and documentation errors due to procedural complexity and reliance on manual verification systems. According to Power (2007), modern organizations operate within what he describes as a “risk society,” where administrative systems must actively anticipate vulnerabilities rather than react to failures. This perspective underscores the necessity of embedding risk-based thinking into routine office functions.

One of the primary sources of operational risk in administrative divisions is human error. Errors in entering personnel data, issuing certificates, misnumbering official correspondence, or misfiling documents can create legal discrepancies and reputational consequences. Reason (1997) argues that human error is an inevitable element in complex organizational systems and must be managed through layered control mechanisms rather than individual blame. In addition, the risk of archival loss whether due to improper filing systems, environmental hazards, or digital system failure poses serious implications for public institutions whose accountability depends on documented evidence. Empirical findings by Ahmeti and Vladi (2017) indicate that public sector institutions frequently underestimate documentation risk despite its long-term impact on governance performance.

Another operational vulnerability involves service delays within correspondence processing and certification issuance. Delays may arise from administrative bottlenecks, incomplete documentation, or a lack of standardized procedures. OECD (2014) reports that inefficiencies in public service administration can erode public trust and reduce organizational performance outcomes. Furthermore, recurring administrative failures may escalate into reputational risk, which in government institutions is closely linked to transparency and public accountability obligations. According to Hood (2011), reputational risk in public organizations often results not from catastrophic failures but from cumulative minor administrative breakdowns that damage stakeholder confidence over time.

Considering these risk exposures, systematic risk management becomes a strategic necessity rather than a procedural formality. ISO 31000 (2018) defines risk management as a coordinated approach to directing and controlling an organization with regard to uncertainty, emphasizing structured identification, assessment, and treatment processes. In operational contexts, structured tools such as HIRARC (Hazard Identification, Risk Assessment, and Risk Control) have been widely used to categorize risk levels based on likelihood and severity (Alamsyah et al. 2021). Although traditionally applied in industrial safety environments, the HIRARC framework can be adapted to administrative systems to assess operational vulnerabilities in HR and correspondence divisions.

Based on the institutional context and risk exposures described above, this study formulates three primary research questions. First, what potential operational risks exist within the Human Resources and Correspondence Division at PPSDM Migas Cepu? Second, how are these risks categorized when assessed using the HIRARC method? Third, what appropriate risk control strategies can be implemented to reduce risk levels to acceptable thresholds? These questions aim to systematically examine administrative vulnerabilities through a structured analytical framework grounded in risk management theory. Accordingly, the objectives of this research are threefold: to identify potential operational risks within HR and correspondence functions; to analyze risk levels based on likelihood and severity assessments; and to formulate effective risk control strategies aligned with institutional conditions. Theoretically, this research contributes to the literature on public sector operational risk management by expanding the application of HIRARC beyond industrial safety contexts. Practically, the findings are expected to provide actionable recommendations for strengthening administrative systems within PPSDM Migas Cepu, enhancing service reliability, and reinforcing institutional credibility in Indonesia's oil and gas human resource development sector.

LITERATURE REVIEW

A. Concept of Risk Management

Risk management is a systematic approach used by organizations to identify, analyze, evaluate, and control uncertainties that may affect the achievement of objectives. According to ISO (2018), risk is defined as the “effect of uncertainty on objectives,” which may result in positive or negative consequences. ISO 31000 further explains that risk management is a coordinated set of activities designed to direct and control an organization with regard to risk. This definition emphasizes that risk management is not merely reactive but is embedded within governance, strategy, and operational processes. In public institutions, risk management serves as a mechanism to ensure accountability, transparency, and performance stability.

The primary objective of risk management is to minimize potential losses while maximizing organizational resilience and decision-making quality. As noted by Hopkin (2018), effective risk management improves institutional reliability, protects assets, enhances stakeholder trust, and supports sustainable performance. In the public sector context, risk management also aims to safeguard public value and prevent administrative failures that may damage institutional legitimacy (OECD 2014). Therefore, risk management should not be perceived solely as a compliance requirement but as a strategic governance instrument.

The process of risk management generally consists of four major components: risk identification, risk analysis, risk evaluation, and risk control. Risk identification involves recognizing potential events or conditions that could negatively affect organizational objectives (Hillson 2002). Risk analysis refers to assessing the likelihood and impact of identified risks to determine their severity. Risk evaluation is the stage where analyzed risks are compared against established criteria to determine acceptability levels (ISO 2018). Finally, risk control (or risk treatment) involves selecting and implementing appropriate measures to reduce risk to an acceptable level. These four components form a continuous cycle that supports organizational learning and improvement. In administrative environments such as HR and correspondence divisions, these components are highly relevant. Errors in documentation, delays in processing official letters, and mismanagement of personnel records can be systematically identified and assessed through structured risk management processes. According to Power (2007), organizations that institutionalize risk frameworks are better prepared to prevent systemic failures. Hence, integrating risk management principles into public office administration strengthens operational stability and service quality.

B. Operational Risk in Public Organizations

Operational risk is commonly defined as the risk of loss resulting from inadequate or failed internal processes, people, systems, or external events (Basel Committee on Banking Supervision 2011). While originally conceptualized within financial institutions, this definition has been widely adopted in public sector governance. In government offices, operational risks often emerge in the form of administrative errors, system failures, human resource limitations, and procedural non-compliance. Administrative risk refers to vulnerabilities arising from documentation errors, misfiling of archives, incomplete records, and procedural inconsistencies. Public institutions rely heavily on documentation as legal proof of accountability; therefore, administrative failures may create long-term legal and reputational consequences. According to Asnawi, Larasati, and Syahrir (2023), weak administrative controls in public organizations can directly affect service delivery effectiveness and governance performance.

Human resource risk involves issues related to employee competence, workload imbalance, lack of training, and human error. Reason (1997) argues that human error is inevitable in complex systems and must be mitigated through structured organizational controls rather than individual blame. In the context of HR divisions, incorrect data entry, delays in updating employee records, or miscommunication between departments may disrupt institutional processes. Reputational risk is another critical dimension of operational risk in public organizations. Hood (2011) explains that

public institutions are highly vulnerable to reputational damage because they operate under public scrutiny and political accountability. Even minor administrative failures can reduce public trust. Additionally, compliance risk defined as the risk of legal or regulatory sanctions resulting from non-adherence to laws and regulations poses significant consequences in government institutions (Hopkin 2018). Non-compliance in certification documentation or archival management may result in legal disputes and institutional sanctions. Therefore, operational risk management in public organizations must integrate administrative, human resource, reputational, and compliance dimensions into a unified risk framework. This integrated perspective ensures that institutional governance remains aligned with legal mandates and service expectations.

C. HIRARC Method

The HIRARC (Hazard Identification, Risk Assessment, and Risk Control) method is a structured risk assessment tool widely applied in occupational health and safety management systems. However, its systematic framework can also be adapted for administrative risk assessment. According to Ramli (2010), HIRARC provides a practical mechanism to identify hazards, measure risk levels, and determine appropriate control measures in a structured manner. Hazard identification is the first stage in the HIRARC process. It involves identifying potential sources of risk within work activities, processes, or systems. In industrial contexts, hazards may include physical or chemical dangers. In administrative environments, hazards can include documentation errors, data loss, system failure, service delays, or miscommunication. According to ISO (2018), risk identification must be comprehensive and consider both internal and external factors influencing organizational objectives.

Risk assessment involves evaluating the level of risk based on two primary variables: likelihood and severity. Likelihood represents the probability of a risk occurring, while severity reflects the magnitude of impact if the risk materializes (Hopkin 2018). In the HIRARC model, each variable is typically measured using a 1–5 scale:

Likelihood (1–5)

Severity (1–5)

Risk Score is calculated as:

$\text{Risk Score} = \text{Likelihood} \times \text{Severity}$

The risk categories are generally classified as follows:

1–4 = Low

5–8 = Moderate

9–15 = High

16–25 = Very High

This scoring system enables organizations to prioritize risk treatment strategies based on quantitative evaluation. According to Alamsyah et al. (2021), structured risk scoring enhances decision-making consistency and facilitates resource allocation efficiency.

The final stage of HIRARC is risk control. Risk control strategies are determined based on the hierarchy of control, which prioritizes the most effective measures. The hierarchy consists of:

1. Elimination – Removing the source of risk entirely.
2. Substitution – Replacing the risk source with a safer alternative.
3. Engineering Control – Designing systems or technologies to reduce exposure.
4. Administrative Control – Establishing procedures, training, and supervision.
5. Personal Protective Equipment (PPE) – Providing protective equipment (adjusted to office context, such as data security protocols or ergonomic protection).

According to Reason (1997), effective risk control should emphasize systemic safeguards rather than relying solely on individual vigilance. In office environments such as HR and correspondence divisions, engineering controls may include digital archiving systems, while administrative controls may involve standardized operating procedures (SOPs) and periodic audits. Thus, the HIRARC method provides a structured and measurable framework for assessing and controlling operational risks in public administrative settings. When integrated with broader risk

management principles, HIRARC can serve as an effective analytical tool for strengthening governance and operational resilience.

METHODS

This study employs a descriptive qualitative research design combined with a literature study approach and direct observation conducted during the internship (PKL) period at PPSDM Migas. Descriptive qualitative research aims to systematically describe phenomena, processes, and risk conditions as they occur in their natural setting without manipulating variables (Creswell and Creswell 2018). The literature study was conducted to build a theoretical foundation related to risk management, operational risk in public organizations, and the HIRARC method. Meanwhile, field observation allowed the researcher to directly examine administrative workflows, documentation systems, and correspondence procedures within the Human Resources and Correspondence Division. This combined approach ensures that theoretical concepts are aligned with actual operational practices in the institutional environment.

The research location focuses specifically on the Human Resources and Correspondence Division of PPSDM Migas, which plays a crucial role in managing personnel data, certification records, official letters, and document archiving systems. Data collection techniques consisted of three primary methods: literature review, direct observation of administrative activities, and documentation analysis of Standard Operating Procedures (SOPs). The literature review provided theoretical references regarding risk identification and assessment frameworks (ISO 2018; Hopkin 2018). Observation was used to identify potential operational risks such as documentation errors, processing delays, and archival vulnerabilities. Documentation analysis was conducted by reviewing internal SOPs to understand formal control mechanisms and compliance structures, which are essential components in evaluating administrative risk exposure (OECD 2014). Data analysis was conducted using the HIRARC (Hazard Identification, Risk Assessment, and Risk Control) framework. The analysis began with identifying key work activities within the HR and correspondence units, followed by identifying potential hazards or operational risks associated with each activity. The next stage involved risk assessment using a risk matrix based on Likelihood (1–5) and Severity (1–5), where $\text{Risk Score} = \text{Likelihood} \times \text{Severity}$ (Alamsyah et al. 2021). Risks were then classified into four categories: Low (1–4), Moderate (5–8), High (9–15), and Very High (16–25). The final stage involved formulating risk control recommendations based on the hierarchy of control principles, emphasizing elimination, substitution, engineering controls, administrative controls, and contextual office-based protective measures (Reason 1997). This structured analytical process ensures that risk evaluation remains systematic, measurable, and aligned with established risk management standards.

RESULTS AND DISCUSSION

A. Identification of Work Activities

Based on field observations conducted during the internship period at PPSDM Migas, the Human Resources and Correspondence Division performs several core administrative activities that directly influence institutional effectiveness and legal accountability. The first major activity is employee data entry and updating. This process includes recording personal information, employment status, training history, certification records, and performance documentation into administrative databases. Accurate data entry is critical because personnel information forms the basis for official certification issuance and institutional reporting. According to ISO (2018), reliable information systems are fundamental in risk management because inaccurate data may generate operational disruptions and compliance issues. Errors in data input, duplication, or delayed updates may result in administrative discrepancies and reputational consequences. The second key activity involves archiving certification documents, both in physical and digital formats. Certification documents issued by PPSDM Migas serve as formal evidence of professional competency in the oil and gas sector. Therefore,

document archiving must follow structured procedures to ensure traceability, authenticity, and security. According to Asnawi, Larasati, and Syahrir (2023), public sector documentation systems are highly sensitive to procedural weaknesses that may compromise institutional legitimacy. Improper filing, misclassification, or loss of certification records may lead to compliance risk and legal disputes. Additionally, Reason (1997) explains that documentation systems in complex organizations are vulnerable to latent errors if control mechanisms are not regularly evaluated. The third primary activity is the management of incoming correspondence (surat masuk). This includes receiving official letters, registering them in logbooks or digital systems, verifying sender information, and forwarding documents to relevant units. Effective correspondence management ensures timely decision-making and coordinated communication within the institution. According to OECD (2014), delays in administrative processing can reduce organizational performance and weaken public trust. Risks in managing incoming correspondence may include misplacement, delayed recording, or incorrect internal distribution, which can disrupt operational workflow and institutional responsiveness.

The fourth activity involves the distribution of outgoing correspondence (surat keluar). This includes drafting official letters, assigning reference numbers, obtaining authorization signatures, recording documentation, and dispatching letters to external stakeholders. The accuracy and timeliness of outgoing correspondence are essential because official letters often represent formal institutional commitments. Hopkin (2018) emphasizes that communication risk is a significant component of operational risk, particularly when formal documentation reflects legal and organizational responsibility. Errors such as incorrect numbering, incomplete attachments, or delayed dispatch may expose the institution to reputational and compliance risks. The fifth activity concerns physical archive storage management. Physical documents are stored in filing cabinets and archival rooms according to classification systems. Risks associated with physical archiving include environmental damage (humidity, fire, pests), misfiling, and limited retrieval efficiency. Basel Committee on Banking Supervision (2011) defines operational risk as including system and process failures, which can also encompass documentation storage systems. Without structured archival control, institutions may face difficulties in retrieving historical records for audits or verification processes. The sixth activity is document digitization, which involves scanning physical documents and integrating them into digital storage systems to improve efficiency and data security. Digitalization aims to reduce dependency on physical archives and enhance accessibility. However, digital systems also introduce new risks such as data corruption, cybersecurity threats, and system downtime. According to Power (2007), modernization through digital systems requires parallel strengthening of risk control mechanisms to avoid shifting vulnerabilities from physical to technological domains. Therefore, each of these six work activities presents identifiable operational risks that must be assessed systematically through the HIRARC framework in the next stage of analysis.

B. Hazard Identification

Hazard identification is the first stage in the HIRARC method, aiming to systematically recognize potential sources of operational risk within work activities. According to ISO (2018), risk identification must be comprehensive and consider human factors, system weaknesses, procedural gaps, and environmental threats. In administrative environments, hazards are not limited to physical dangers but also include process failures, documentation errors, and communication breakdowns (Hopkin 2018). Based on field observation and documentation review, the following hazards were identified within the HR and Correspondence Division.

Table 1 Hazard Identification in HR and Correspondence Division

No	Work Activity	Potential Hazard	Identified Risk
I	Certificate data entry	Human error (mis-typing, incomplete verification)	Incorrect participant name or certification details

2	Manual document archiving	Documents not digitized / improper filing	Loss or misplacement of certification archives
3	Incoming correspondence management	Delay in internal disposition process	Administrative process bottlenecks
4	Outgoing correspondence distribution	Incorrect recipient address or incomplete attachments	Reputational loss and communication failure
5	Physical archive storage	Fire, humidity, pests, or environmental hazards	Permanent loss of institutional documents
6	Document digitization	System failure or data corruption	Inaccessibility or damage to digital records
7	Employee data updating	Delayed updating of personnel records	Inaccurate HR database and reporting discrepancies
8	Document numbering system	Duplicate or incorrect reference numbers	Administrative inconsistency and compliance risk

The table above demonstrates that most hazards originate from human factors, procedural weaknesses, and system limitations. As explained by Reason (1997), organizational accidents often result from accumulated minor failures within administrative systems. Similarly, Basel Committee on Banking Supervision (2011) categorizes such process failures and human errors as core components of operational risk. Therefore, each identified hazard requires further assessment using likelihood and severity analysis to determine its risk level classification.

C. Risk Assessment

Risk assessment in this study was conducted using the HIRARC method by evaluating each identified hazard based on two parameters: Likelihood and Severity. Likelihood measures the probability of occurrence, while Severity evaluates the potential impact if the risk materializes. According to ISO (2018), risk level determination should be based on structured criteria to ensure consistency and objectivity. Similarly, Hopkin (2018) emphasizes that risk quantification through scoring matrices improves prioritization and decision-making in operational risk management.

Tabel 2 Likelihood Scale

Score	Category	Description
1	Rare	Very unlikely to occur
2	Unlikely	Could occur but infrequent
3	Possible	Might occur under certain conditions
4	Likely	Expected to occur periodically
5	Almost Certain	Occurs frequently or repeatedly

Tabel 3 Severity Scale

Score	Category	Description
1	Insignificant	Minimal impact, easily corrected
2	Minor	Small operational disruption
3	Moderate	Noticeable disruption requiring corrective action
4	Major	Significant administrative/legal impact
5	Extreme	Severe institutional or reputational damage

Risk Score is calculated using the formula:

Risk Score = Likelihood ×

Severity Risk Classification:

1–4 = Low

5–8 = Moderate

9–15 = High

16–25 = Very High

Table 4 Risk Assessment Results – HR and Correspondence Division

No	Identified Risk	Likelihood	Severity	Risk Score	Classification
1	Incorrect participant name in certificate	4	3	12	High
2	Loss of manual certification archive	3	4	12	High
3	Delay in incoming letter disposition	3	3	9	High
4	Incorrect recipient address in outgoing letter	2	3	6	Moderate
5	Permanent loss of physical archive due to fire	1	5	5	Moderate
6	Data entry delay in employee database	2	2	4	Low

Risk Classification Summary

Based on the assessment results:

3 risks categorized as High

2 risks categorized as Moderate

1 risk categorized as Low

The High-category risks are primarily related to human error in certificate data entry and the potential loss of certification archives. These risks pose serious administrative and reputational consequences because certification documents serve as formal proof of professional competence. As stated by Basel Committee on Banking Supervision (2011), operational risks arising from process failures and human error can significantly impact institutional credibility. The Moderate risks are associated with correspondence inaccuracies and physical archive vulnerability, while the Low risk relates to routine database delays with limited institutional impact.

According to Reason (1997), high-risk conditions in administrative systems typically result from repeated minor process weaknesses that accumulate over time. Therefore, priority risk control measures must focus on strengthening verification mechanisms, improving digital archiving systems, and enhancing procedural supervision. The next section will discuss appropriate risk control strategies based on the hierarchy of control principles.

D. Risk Control Based on Hierarchy of Control

Based on the field observations conducted by the researcher during the internship period at PPSPDM Migas Cepu, operational risks identified in the Human Resources and Correspondence Division require structured mitigation strategies aligned with the hierarchy of control principles. The hierarchy of control emphasizes prioritizing the most effective risk reduction measures, starting from elimination to personal protective equipment (PPE) (ISO 2018). Although originally developed for occupational safety contexts, this hierarchy can be adapted to administrative and office-based environments. As explained by Reason (1997), systemic control mechanisms are more effective than relying solely on individual vigilance; therefore, risk mitigation in administrative settings should prioritize system improvement.

The first level, Elimination, involves completely removing the source of risk. Based on observation, one of the significant vulnerabilities identified was the continued reliance on partial manual archiving systems. To eliminate the risk of document misplacement and duplication, it is

recommended to gradually remove manual archival systems and transition toward fully integrated digital documentation. Eliminating manual duplication reduces exposure to archive loss and retrieval inefficiencies. According to Hopkin (2018), elimination is the most effective control strategy because it removes uncertainty at its source rather than managing its consequences.

The second level, Substitution, refers to replacing risky processes with safer alternatives. In the context of PPSDM Migas, substitution can be implemented by replacing physical correspondence distribution with an electronic office (e-office) system. During field observation, several administrative processes were still conducted through printed documentation before digital recording. By substituting paper-based communication with secure digital correspondence platforms, risks related to delayed delivery, incorrect addresses, and document damage can be significantly reduced. OECD (2014) highlights that digital governance systems enhance efficiency and reduce procedural vulnerability in public sector institutions.

The third level, Engineering Control, focuses on designing technological safeguards to reduce risk exposure. Based on observed archival practices, digital records require stronger backup mechanisms to prevent data corruption or system failure. Therefore, implementing automatic server backups and secure cloud storage systems is recommended. Engineering controls may also include access restrictions, user authentication systems, and data encryption protocols. According to Basel Committee on Banking Supervision (2011), technological control systems are essential in minimizing operational risk arising from system failures and information processing errors.

The fourth level, Administrative Control, is considered the most applicable and dominant risk control strategy within office-based environments. Based on field findings, administrative reinforcement can be implemented through a two-step verification SOP for certificate data entry, periodic internal audits of document management, and structured employee training programs. A dual verification system (double-check mechanism) can significantly reduce human error in participant name input and certificate numbering. Internal audits ensure compliance with archival standards, while training programs strengthen employee competence and awareness of procedural risks. As noted by Asnawi, Larasati, and Syahrir (2023), strengthening administrative governance mechanisms directly improves public service reliability and institutional accountability.

The final level, Personal Protective Equipment (PPE), has limited relevance in administrative office contexts compared to industrial settings. However, in this study, PPE can be interpreted in a broader sense as individual protective measures such as data access passwords, secure login credentials, and ergonomic work arrangements to prevent fatigue-related errors. While PPE does not eliminate systemic risk, it supports individual-level protection. Nevertheless, consistent with risk management theory, PPE should not be the primary control mechanism but rather a complementary safeguard (ISO 2018). Overall, based on the researcher's field observation at PPSDM Migas Cepu, the most effective mitigation strategy combines elimination of manual duplication, substitution through digital systems, engineering reinforcement via automated backups, and strengthened administrative controls such as SOP verification and routine audits. This integrated approach ensures that high and moderate risks identified in Section 5.3 can be systematically reduced to acceptable levels while maintaining institutional accountability and service quality.

E. Managerial Implications

Based on the findings of this study, the managerial implications emphasize strengthening existing systems rather than correcting fundamental weaknesses. Observations conducted during the internship period indicate that the administrative governance at PPSDM Migas has already been structured, procedurally guided, and aligned with public sector accountability standards. However, in the perspective of management science, continuous improvement remains essential to ensure sustainability, efficiency, and strategic risk mitigation. As ISO (2018) states, risk management is not a one-time corrective mechanism but a continuous improvement process embedded within organizational governance.

The first managerial implication concerns the importance of administrative digitalization.

Although PPSDM Migas has implemented structured documentation procedures, strengthening digital integration would further enhance efficiency and minimize operational risk exposure. Digital systems reduce dependency on manual processes, improve document traceability, and accelerate service responsiveness. According to OECD (2014), digital governance significantly improves public sector transparency and operational reliability. From a management perspective, digital transformation aligns with strategic management principles that emphasize innovation, process optimization, and competitive institutional positioning (Hill, Schilling, and Jones 2020). Therefore, digitalization is not merely a technical upgrade but a strategic organizational investment. The second implication highlights the necessity of a structured double-verification system in critical administrative processes such as certificate issuance and official correspondence. The study identified that human error constitutes one of the most significant operational risks. Implementing a two-step verification mechanism strengthens internal control and reduces documentation inaccuracies. Hopkin (2018) explains that internal control mechanisms are central to operational risk mitigation, especially in documentation-sensitive institutions. In management theory, this aligns with control function principles, where supervision and verification ensure goal congruence and performance accuracy (Robbins and Coulter 2022). Thus, double verification should be institutionalized within administrative SOPs to reinforce reliability. The third implication concerns competency-based human resource development, particularly in digital administrative skills. As a student of Management within the Faculty of Islamic Economics and Business, this finding reinforces the importance of aligning HR management practices with technological transformation. Digital competence enhances employee productivity and reduces system-based errors. According to Asnawi, Larasati, and Syahrir (2023), risk-aware organizational culture can only be developed when employees possess adequate knowledge and technical capability. Continuous training programs in digital documentation systems, data security, and administrative risk awareness would strengthen institutional resilience while supporting strategic HR management objectives. The fourth implication emphasizes the integration of risk management principles directly into Standard Operating Procedures (SOPs). Rather than treating risk assessment as a separate evaluation tool, embedding risk-based thinking into daily administrative workflows ensures proactive governance. ISO (2018) underscores that risk management should be integrated into organizational processes and decision-making structures. From a strategic management standpoint, embedding risk management into SOPs supports long-term sustainability and performance stability (Hill, Schilling, and Jones 2020). This integration ensures that operational risk mitigation becomes part of routine practice rather than reactive response. Overall, the managerial implications of this research demonstrate that PPSDM Migas Cepu already possesses a solid administrative foundation. The recommended improvements focus on strengthening digital infrastructure, enhancing internal control systems, upgrading HR digital competencies, and integrating systematic risk management into SOP frameworks. From a management science perspective, these strategies reflect the core managerial functions of planning, organizing, leading, and controlling. Thus, this study not only contributes practically to PPSDM Migas but also aligns theoretically with the broader discipline of strategic and operational management.

CONCLUSION

This study aimed to analyze the implementation of operational risk management within the Human Resources and Correspondence Division at PPSDM Migas Cepu using the HIRARC (Hazard Identification, Risk Assessment, and Risk Control) framework. Based on systematic observation during the internship period and supported by relevant literature, it can be concluded that administrative activities within the institution are generally structured and procedurally regulated. However, like all public administrative systems, these activities inherently contain operational risks that require structured identification and mitigation.

The hazard identification stage revealed that key administrative processes such as employee data entry, certification archiving, incoming and outgoing correspondence management, physical

archive storage, and document digitization present measurable risk exposure. These risks are primarily associated with human error, documentation inconsistencies, procedural delays, environmental threats to physical archives, and system-based vulnerabilities in digital records. Importantly, the findings do not indicate systemic weaknesses but rather reflect typical operational risks inherent in documentation-intensive public institutions. The risk assessment results demonstrated that among the identified risks, two were categorized as High, three as Moderate, and one as Low. High-level risks were mainly linked to inaccuracies in certification data entry and potential loss of certification archives, both of which directly affect institutional credibility and compliance integrity. Moderate risks were related to correspondence inaccuracies and physical archive vulnerability, while low-level risk concerned routine delays in employee database updates. These classifications confirm that while most risks remain manageable, structured mitigation strategies are necessary to prevent accumulation of minor errors into larger institutional disruptions. The application of the HIRARC method proved to be effective in translating qualitative administrative observations into measurable risk categories. The use of likelihood and severity scales enabled objective prioritization of risks, ensuring that mitigation strategies focus on the most impactful areas. Furthermore, the hierarchy of control framework demonstrated that the most sustainable risk mitigation efforts in office-based settings lie in system improvement, digital integration, procedural reinforcement, and competency development rather than relying solely on individual caution. From a managerial perspective, this study highlights that PPSDM Migas Cepu already possesses a strong administrative foundation supported by standard operating procedures and structured documentation processes. The recommended improvements such as strengthening digital archiving systems, implementing double-verification mechanisms, enhancing competency-based digital training, and integrating risk management into SOPs are positioned as strategic enhancements rather than corrective measures. These improvements align with core management principles of planning, organizing, controlling, and continuous improvement, which are central to modern public sector governance.

Theoretically, this research contributes to the literature by extending the application of the HIRARC method beyond industrial safety contexts into public administrative environments. This demonstrates that risk assessment frameworks traditionally used in occupational safety can be effectively adapted to evaluate operational risks in documentation-based institutions. Practically, the findings provide structured and implementable recommendations that can support the long-term resilience, transparency, and accountability of PPSDM Migas Cepu and similar public training institutions. In conclusion, operational risk within public administrative systems is inevitable, but when managed systematically through structured frameworks such as HIRARC, it becomes measurable, controllable, and strategically manageable. By embedding risk management into daily administrative practices, PPSDM Migas Cepu can further strengthen its role as a professional and accountable national human resource development institution in the oil and gas sector.

SUGGESTIONS AND ACKNOWLEDGMENTS

Based on the findings of this study, it is suggested that future research may expand the scope of operational risk analysis by incorporating quantitative data, structured interviews, or comparative studies across multiple public training institutions to enhance generalizability and empirical robustness. Further studies could also explore the integration of digital governance systems with enterprise risk management frameworks to strengthen administrative resilience in public sector organizations. In practical terms, continuous digital transformation, periodic risk reassessment, and structured competency-based training programs are recommended to support sustainable administrative excellence. The author would like to express sincere gratitude to the management and staff of PPSDM Migas for providing the opportunity to conduct field observations during the internship period, as well as for their professionalism, cooperation, and institutional openness that made this research possible. Appreciation is also extended to academic supervisors and lecturers in the Management Program, Faculty of Islamic Economics and Business, State Islamic University of Sunan Ampel Surabaya for their

guidance and constructive feedback throughout the completion of this research.

REFERENCES

- Ahmeti, Remzi, and Besarta Vladi. 2017. "Risk Management in Public Sector: A Literature Review." *European Journal of Multidisciplinary Studies* 5 (1): 323–329.
- Alamsyah, A., R. Setiawan, and D. Nugroho. 2021. "Application of HIRARC Method in Occupational Risk Assessment." *International Journal of Engineering Research and Technology* 10 (3): 112–118.
- Asnawi, Meinarni, Rudiawie Larasati, and Azhar Syahrir. 2023. "Risk Management and Public Service: Integrated Analysis at Public Sector Organizations." *Jurnal Riset Akuntansi dan Keuangan* 11 (3): 525–540.
- Basel Committee on Banking Supervision. 2011. *Principles for the Sound Management of Operational Risk*. Basel: Bank for International Settlements.
- BPSDM ESDM. 2025. "Strengthening National Oil and Gas Human Resources through PPSDM Migas." Ministry of Energy and Mineral Resources, Indonesia.
- Creswell, John W., and J. David Creswell. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. Thousand Oaks, CA: SAGE Publications.
- Hill, Charles W. L., Melissa A. Schilling, and Gareth R. Jones. 2020. *Strategic Management: Theory and Cases*. 13th ed. Boston: Cengage Learning.
- Hillson, David. 2002. "Extending the Risk Process to Manage Opportunities." *International Journal of Project Management* 20 (3): 235–240.
- Hood, Christopher. 2011. *The Blame Game: Spin, Bureaucracy, and Self-Preservation in Government*. Princeton: Princeton University Press.
- Hopkin, Paul. 2018. *Fundamentals of Risk Management*. 5th ed. London: Kogan Page.
- International Organization for Standardization (ISO). 2018. *ISO 31000: Risk Management – Guidelines*. Geneva: ISO.
- OECD. 2014. *Risk Management and Public Governance*. Paris: OECD Publishing.
- Power, Michael. 2007. *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.
- Ramli, Soehatman. 2010. *Sistem Manajemen Keselamatan dan Kesehatan Kerja OHSAS 18001*. Jakarta: Dian Rakyat.
- Reason, James. 1997. *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate Publishing.
- Robbins, Stephen P., and Mary Coulter. 2022. *Management*. 15th ed. Harlow: Pearson Education.
- Peneliti. 2025. "Hasil Analisis dan Observasi Lapangan pada Unit Administrasi dan Pelayanan Diklat." *Laporan Internal Praktik Kerja Lapangan di PPSDM Migas, Cepu*