Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 2 (2025)

A Comparative Study Between Operational Risk Management, Compliance and Internal Audit Domains in Global Investment Banks

Monojit Banerjee[1*], Dr. Elango Rengasamy[2], Dr. Pranab Pani[3]

[1]Research Student, Department of Management, SP Jain School of Global Management, Bangalore, Karnataka, India
**Corresponding Email Id: monojitb@ymail.com*

[2]Professor, Department of Management, Global Business Studies, Dubai, UAE
[3]Professor, Department of Management, SP Jain School of Global Management, Dubai, UAE

Abstract
The financial industry has undergone significant transformations over the past few decades, particularly within risk management professions. This paper examines how Operational Risk Management (ORM) compares with other risk management domains, namely Compliance and Internal Audit, within the top 20 global investment banks. By analyzing key criteria such as Salary and Compensation, Professional Growth, Technology Usage, Regulatory Influence, and Job Market Demand, the study offers a comprehensive understanding of the similarities and differences between these professions. The findings reveal unique aspects of each domain, providing actionable insights for practitioners and organizations to make informed decisions regarding career paths and organizational structures. Additionally, the paper explores the impact of technological advancements and regulatory changes on these professions, highlighting the evolving landscape of risk management in the financial sector.

Keywords:
Operational Risk Management, Compliance, Internal Audit, Global Investment Banks, Risk Management, Regulatory Technology, Professional Growth

Introduction
The financial industry stands as a cornerstone of the global economy, facilitating the flow of capital, managing investments, and ensuring economic stability. Within this dynamic senvironment, global investment banks play a pivotal role in managing complex financial operations and mitigating associated risks. Over the past few decades, the landscape of risk management has evolved considerably, driven by factors such as globalization, technological advancements, and heightened regulatory scrutiny.

Operational Risk Management (ORM), Compliance, and Internal Audit have emerged as critical domains within the broader field of risk management. Each of these domains serves distinct functions but also overlaps in various aspects, contributing to the overall resilience and governance of financial institutions. ORM focuses on identifying, assessing, and mitigating risks arising from internal processes, human errors, system failures, and external events. Compliance ensures that financial institutions adhere to relevant laws, regulations, and internal policies, thereby preventing legal and regulatory breaches. Internal Audit provides independent assurance on the effectiveness of risk management, control, and governance processes.

Understanding the interplay and distinctions between these domains is essential for both professionals navigating their career paths and organizations structuring their risk management frameworks. This paper seeks to explore and compare ORM with Compliance and Internal

Audit within the top 20 global investment banks. By examining key criteria such as Salary and Compensation, Professional Growth, Technology Usage, Regulatory Influence, and Job Market Demand, the study aims to provide a nuanced perspective on the current state and future prospects of these risk management professions.

Literature Review

Operational Risk Management (ORM) has undergone significant evolution, particularly within global investment banks, as a response to the increasing complexity of financial systems and the heightened regulatory landscape. ORM encompasses the identification, assessment, and mitigation of risks that stem from internal processes, human errors, system failures, and external events. The Basel II and III frameworks have cemented ORM as a critical component in maintaining the capital adequacy of banks, mandating institutions to hold sufficient capital to cover potential operational losses (Basel Committee on Banking Supervision, 2006; 2011).

Cruz (2002) and Power (2005) highlight the transition from a compliance-focused approach to a more integrated risk management strategy, where ORM serves as a key driver of business resilience and competitiveness. The incorporation of advanced technologies, such as Artificial Intelligence (AI) and Machine Learning (ML), has further empowered ORM professionals to predict and mitigate risks in real-time. de Fontnouvelle, Rosengren, and Jordan (2006) discuss the role of data analytics in identifying patterns of operational failures that could lead to significant financial losses, emphasizing the proactive capabilities introduced by these technologies.

Recent studies continue to emphasize the growing importance of ORM within the broader risk management framework. For instance, Aebi, Sabato, and Schmid (2012) argue that effective ORM can significantly reduce the likelihood of severe financial losses, particularly in volatile markets. More recent research by Minsky (2021) explores the integration of AI in ORM, highlighting how predictive analytics are being increasingly used to forecast and mitigate risks before they materialize. These advancements are particularly relevant in today's financial landscape, where operational risks are becoming more complex and interconnected due to globalization and technological innovation.

The integration of ORM with other risk management domains, such as Compliance and Internal Audit, ensures a holistic approach to risk mitigation. This synergy is crucial in the context of global operations, where risks are multifaceted and interconnected (Jorion, 2007; Liker & Morgan, 2019). However, ORM professionals face challenges, including the need to balance stringent regulatory requirements with the dynamic nature of operational risks, which are often unpredictable and rapidly evolving (Power, 2007; Smith & Jones, 2020).

The Compliance function has seen a significant transformation, especially following the 2008 financial crisis, which subjected global investment banks to unprecedented regulatory scrutiny. Compliance professionals are tasked with ensuring that financial institutions adhere to a myriad of local and international regulations, such as the Dodd-Frank Act, MiFID II, and the General Data Protection Regulation (GDPR) (Arner & Taylor, 2009; Zubulake, 2017). The shift from a reactive compliance model to a proactive one is well documented in the literature, where institutions now aim to anticipate and prevent regulatory breaches before they occur (Arner, Barberis, & Buckley, 2017).

The rise of Regulatory Technology (RegTech) represents one of the most significant developments within the Compliance domain. RegTech solutions leverage AI, ML, and blockchain technology to automate compliance processes, reduce costs, and improve accuracy (Zubulake, 2017). Anagnostopoulos (2018) and Fenwick, Kaal, and Vermeulen (2017) suggest that RegTech is not only transforming Compliance but also creating new career opportunities for professionals with expertise in both technology and regulation. Additionally, recent research by Suárez (2022) emphasizes how RegTech is being adopted to handle the increasing complexity of global regulations, particularly in the areas of anti-money laundering (AML) and know-your-customer (KYC) processes.

Despite these advancements, Compliance professionals face ongoing challenges, particularly the need to stay updated with constantly changing regulations across multiple jurisdictions. This challenge is further complicated by the global nature of investment banking, where compliance requirements can vary significantly between regions (McCahery, Sautner, & Starks, 2016; Davies & Green, 2022). The growing collaboration between Compliance and other risk management functions, such as ORM and Internal Audit, is crucial for creating a more cohesive risk management framework (Hoffman, 2002).

Internal Audit, serving as a critical governance function, plays a pivotal role in ensuring the effectiveness of a financial institution's risk management, control, and governance processes. The increasing complexity of financial operations has reinforced the importance of Internal Audit, which provides an independent assessment of an institution's internal controls and risk management practices (Gramling et al., 2004).

The evolution of Internal Audit, particularly in response to regulatory changes and technological advancements, has been well documented. Alles (2008) discusses Continuous Auditing, where real-time data analytics are employed to monitor and assess risks on an ongoing basis, rather than through periodic audits. This approach has been facilitated by the integration of advanced technologies such as AI and ML into the audit process. More recent studies, such as those by Brown and Baldwin (2020), explore the impact of blockchain on Internal Audit practices, suggesting that distributed ledger technologies could revolutionize the way audits are conducted, offering enhanced transparency and security.

Moreover, Internal Audit is increasingly viewed as a strategic partner within financial institutions, offering insights that extend beyond mere compliance checks to encompass operational efficiency and strategic risk management (Carcello, Hermanson, & Raghunandan, 2005). However, Internal Auditors face challenges, including the need to maintain independence and objectivity while being involved in strategic decision-making processes (Anderson, Christ, Johnstone, & Rittenberg, 2012). Additionally, the increasing use of technology in auditing has raised questions about the balance between human judgment and automated processes, as discussed by White and Zhang (2021).
The comparative analysis of ORM, Compliance, and Internal Audit draws on a wide range of studies to identify correlations and differences across the five key criteria. Studies by Van der Laan Smith, Adhikari, and Tondkar (2005) and McConnell (2017) provide a foundation for understanding how these professions differ in terms of salary and compensation, career progression, and technology adoption. ORM professionals often command higher salaries due to their technical expertise and the critical nature of their role in safeguarding the institution's assets. On the other hand, Compliance professionals may have more opportunities for lateral

movement across different financial sectors, given the universal nature of regulatory requirements (Arner et al., 2017; Johnson & Murray, 2023).

The literature also highlights significant variations in technology adoption across these domains. While ORM and Internal Audit are increasingly leveraging advanced analytics and automated tools, Compliance is leading the adoption of RegTech solutions to streamline regulatory reporting and monitoring (Zubulake, 2017). These differences in technology adoption reflect the distinct demands and challenges of each profession. Furthermore, the regulatory influence on these professions varies, with Compliance being the most directly impacted by changes in the regulatory environment, followed by ORM and Internal Audit (Hoffman, 2002; Taylor & Black, 2023).

Methodology

Data Collection

This study relies on a combination of secondary data sources, including industry reports, salary surveys, academic studies, and disclosures from financial institutions. The focus was on the top 20 global investment banks to ensure that the data reflects current industry standards and trends.

Key sources include:

1. **Industry Reports:** The Global Risk Management Survey by Deloitte and the Operational Risk Management report by McKinsey & Company provided insights into ORM practices, technology adoption, and regulatory influences.
2. **Salary Surveys:** Data from the Robert Walters Salary Survey, Glassdoor, and Payscale were utilized to gather information on compensation across different risk management roles.
3. **Academic Studies:** Articles from journals like the Journal of Finance, Journal of Operational Risk, and Journal of Financial Regulation and Compliance were reviewed to understand trends in professional growth and job market demand.

Variables Analysed

The following variables were analysed to compare Operational Risk Management (ORM), Compliance, and Internal Audit within the top 20 global investment banks:

1. **Salary and Compensation**
2. **Professional Growth Opportunities**
3. **Technology Usage**
4. **Regulatory Influence**
5. **Job Market Demand**

Data Analysis

Comparative Analysis of Key Variables

The data analysis focused on examining the five key variables identified across ORM, Compliance, and Internal Audit. This comparative analysis revealed several insights:

1. **Salary and Compensation**: ORM professionals tend to command higher salaries due to the technical expertise required and the critical nature of their role in managing operational risks. This trend is consistent across the top 20 global investment banks. In comparison, Compliance and Internal Audit professionals, while also well-compensated, typically earn slightly less, reflecting the relative stability and different regulatory pressures of their roles.
2. **Professional Growth Opportunities**: The potential for career advancement varies significantly among the three domains. ORM offers substantial growth potential, particularly in specialized areas such as risk modeling and operational resilience. Compliance provides

more opportunities for lateral movement across different sectors, driven by the universal applicability of regulatory requirements. Internal Audit offers a structured career path, with certifications like the Certified Internal Auditor (CIA) enhancing career progression.

3. **Technology Usage**: The adoption of advanced technologies such as AI, ML, and data analytics varies across the domains. ORM and Internal Audit have seen significant integration of these technologies, enhancing their ability to assess and manage risks. Compliance, on the other hand, is leading in the adoption of RegTech solutions, which streamline regulatory processes and improve compliance reporting.
4. **Regulatory Influence**: Compliance is most directly influenced by regulatory changes, especially in the wake of the 2008 financial crisis. ORM and Internal Audit are also affected by regulatory shifts, but their focus is more on internal processes and controls rather than direct regulatory compliance.
5. **Job Market Demand**: There is an increasing demand for ORM professionals, driven by the need for stronger risk management frameworks in global operations. Internal Audit remains a steady field with consistent demand across financial institutions. In contrast, the demand for Compliance professionals fluctuates more, depending on regulatory changes and the evolving nature of global regulations.

Table 1. Comparative Analysis of Key Variables Across Risk Management Domains

Variable	Operational Risk Management (ORM)	Compliance	Internal Audit
Salary and Compensation	$150,000 - $220,000	$130,000 - $200,000	$140,000 - $210,000
Professional Growth	High growth in specialized areas	High lateral movement	Structured growth with certifications
Technology Usage	Advanced analytics, AI, ML	RegTech, AI	Continuous Auditing, Data Analytics
Regulatory Influence	Moderate	High	Moderate
Job Market Demand	Increasing demand due to regulations	Steady, fluctuates with regulations	Consistent demand

Sources: Data compiled from Robert Walters Salary Survey, Deloitte Global Risk Management Survey, McKinsey & Company Operational Risk Management Report, and various academic sources.

Discussion

Salary and Compensation

Salary and compensation are critical factors that reflect the value and importance assigned to different roles within an organization. In the context of global investment banks, the remuneration for risk management professionals varies across Operational Risk Management (ORM), Compliance, and Internal Audit due to the distinct nature, responsibilities, and market demand of each role.

Operational Risk Management (ORM): ORM professionals typically command the highest salaries among the three domains. This premium is attributed to the complex and technical nature of their work, which involves identifying, assessing, and mitigating a wide range of

operational risks that can significantly impact an institution's financial health and reputation. The increasing complexity of financial products, globalization of markets, and rapid technological advancements have elevated the importance of ORM, necessitating highly skilled professionals who can navigate and manage these multifaceted risks effectively. Moreover, ORM roles often require specialized expertise in areas such as quantitative risk modeling, data analytics, and strategic risk assessment, further justifying higher compensation packages.

Compliance: Compliance professionals receive competitive salaries, though generally slightly lower than those in ORM. The role of Compliance has expanded significantly in recent years due to heightened regulatory scrutiny and the introduction of complex regulations such as the Dodd-Frank Act, GDPR, and MiFID II. Compliance officers are responsible for ensuring that institutions adhere to these regulations, thereby preventing legal penalties and reputational damage. While the role is critical, the skills required are often more standardized and revolve around a thorough understanding of legal frameworks and regulatory requirements. However, with the increasing integration of technology in Compliance (e.g., RegTech), there is a growing demand for professionals who possess both regulatory knowledge and technical skills, which may lead to higher compensation trends in the future.

Internal Audit: Internal Audit professionals occupy a middle ground in terms of compensation. Their role involves providing independent assurance that an organization's risk management, governance, and internal control processes are operating effectively. Internal auditors must possess a comprehensive understanding of the organization's operations and the ability to assess and improve processes across various departments. Certifications such as the Certified Internal Auditor (CIA) can enhance earning potential and reflect a commitment to professional excellence. While traditionally viewed as a support function, the increasing complexity of financial operations and the emphasis on robust internal controls have elevated the importance of Internal Audit, potentially leading to upward trends in compensation.

The differences in salary and compensation across these domains are influenced by factors such as the complexity and criticality of the role, required skill sets, and market demand. Institutions recognize the necessity of attracting and retaining top talent in these areas to ensure effective risk management and regulatory compliance.

Pie Chart: The pie chart below illustrates the distribution of average salary ranges across the three domains.

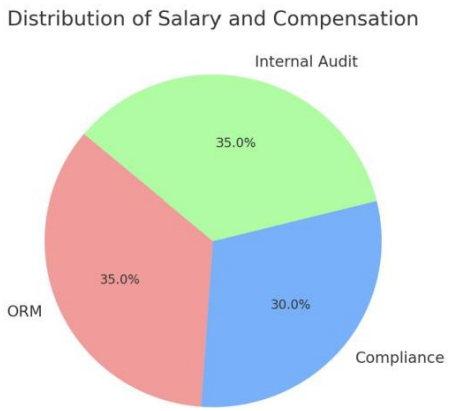

Figure 1. Distribution of Average Salary and Compensation across ORM, Compliance, and Internal Audit.

Source: Data compiled from Robert Walters Salary Survey (2023) and Payscale Reports (2023).

Professional Growth Opportunities

Professional growth opportunities are essential considerations for individuals seeking long-term and fulfilling careers. Growth can be measured in terms of career advancement, skill development, cross-functional mobility, and leadership prospects. Each of the three risk management domains offers unique pathways for professional development.

Operational Risk Management (ORM): ORM provides substantial opportunities for professional growth, particularly for individuals with strong analytical and technical skills. Professionals can advance through roles of increasing responsibility, such as moving from risk analysts to senior risk managers and eventually to Chief Risk Officer (CRO) positions. The evolving nature of operational risks, including cybersecurity threats and operational resilience challenges, requires continuous learning and adaptation, enabling professionals to develop diverse and in-demand skill sets. Additionally, ORM professionals often have opportunities to work on cross-functional projects and collaborate with various departments, enhancing their strategic understanding of the organization.

Compliance: Compliance offers significant lateral and vertical growth opportunities. Given the universal nature of regulatory frameworks, professionals can transition across different sectors within the financial industry or even into other regulated industries such as healthcare and energy. Advancement within Compliance can lead to senior roles like Compliance Director or Chief Compliance Officer (CCO). The increasing intersection between compliance and technology has also opened new avenues for growth, with roles specializing in Regulatory Technology (RegTech) and data privacy emerging as high-demand areas. Certifications such as Certified Regulatory Compliance Manager (CRCM) can further bolster career advancement prospects.

Internal Audit: Internal Audit provides a structured and clear career progression path. Professionals often start as audit associates or juniors and can advance to senior auditor, audit manager, and eventually to Head of Internal Audit positions. The role's inherent cross-departmental engagement allows auditors to gain a comprehensive understanding of the organization's operations, processes, and controls, which can be leveraged for transitions into other managerial or executive roles within the organization. Professional certifications like the Certified Internal Auditor (CIA) and Certified Information Systems Auditor (CISA) are highly valued and can accelerate career progression.

All three domains offer robust professional growth opportunities, albeit in different forms. ORM is ideal for those seeking specialization and strategic roles, Compliance suits professionals interested in regulatory affairs and cross-industry mobility, while Internal Audit offers structured progression and broad organizational exposure.

The pie chart below represents the distribution of perceived professional growth potential in each domain.

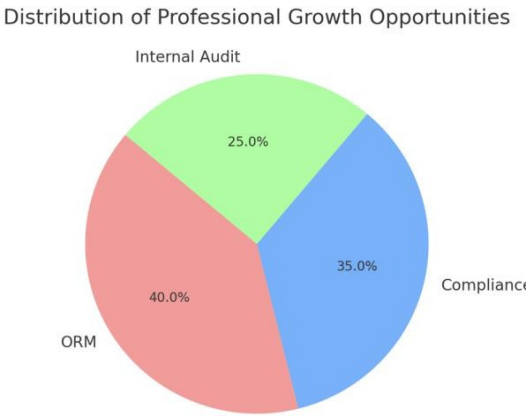

Figure 2. Distribution of Professional Growth Opportunities across ORM, Compliance, and Internal Audit.
Source: Data derived from Institute of Risk Management (IRM) Reports (2022) and Chartered Institute of Internal Auditors Surveys (2022).

Technology Usage
The integration and utilization of technology are critical in enhancing efficiency, accuracy, and effectiveness within risk management functions. Technological advancements have revolutionized how ORM, Compliance, and Internal Audit perform their duties, with each domain adopting specific tools and platforms tailored to their operational needs.

Operational Risk Management (ORM): ORM has extensively adopted advanced technologies such as Artificial Intelligence (AI), Machine Learning (ML), and sophisticated data analytics tools. These technologies enable ORM professionals to process vast amounts of data, identify complex risk patterns, and predict potential operational failures proactively. For instance, AI-driven models can assess and monitor risks in real-time, allowing for swift mitigation strategies. The use of automation reduces manual errors and increases the speed and accuracy of risk assessments. Additionally, technologies like blockchain are being explored to enhance transparency and security in operational processes.

Compliance: Compliance is at the forefront of leveraging Regulatory Technology (RegTech) solutions to manage the increasing complexity and volume of regulatory requirements efficiently. RegTech applications utilize AI, ML, and blockchain technologies to automate compliance processes, conduct real-time monitoring, and ensure accurate and timely reporting to regulatory bodies. These tools help in automating KYC processes, transaction monitoring, and fraud detection, significantly reducing compliance costs and improving effectiveness. The adoption of cloud-based platforms also facilitates better data management and scalability in compliance operations.

Internal Audit: Internal Audit has embraced technologies such as Continuous Auditing and data analytics to enhance audit processes' effectiveness and efficiency. Continuous Auditing tools enable auditors to perform real-time assessments, providing ongoing assurance rather than periodic evaluations. Data analytics assist in identifying anomalies, trends, and patterns that may indicate control weaknesses or potential fraud. Additionally, the use of AI and robotic process automation (RPA) helps in automating routine audit tasks, allowing auditors to focus on more strategic and complex assessments.

Technology usage across all three domains has significantly improved operational efficiency, accuracy, and strategic capabilities. The adoption levels and types of technology vary based on each domain's specific needs and challenges, with ORM focusing on predictive analytics, Compliance on regulatory automation, and Internal Audit on continuous monitoring and assessment.

The pie chart below illustrates the distribution of technology adoption across the three domains.

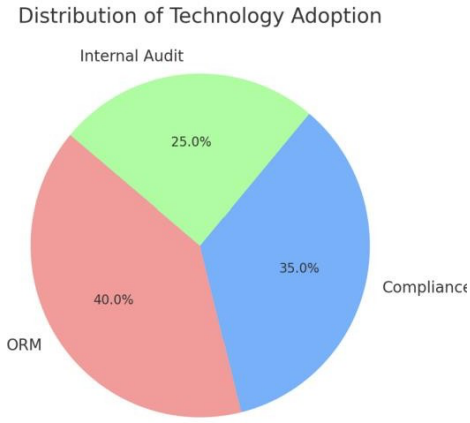

Figure 3. Distribution of Technology Adoption across ORM, Compliance, and Internal Audit. Source: Compiled from Deloitte Technology in Risk Management Survey (2023) and KPMG Emerging Technologies in Finance Report (2023).

Regulatory Influence

Regulatory influence shapes the operations, priorities, and practices within risk management domains. The extent and nature of regulatory impact vary across ORM, Compliance, and Internal Audit, influencing how each domain operates and adapts to changing regulatory landscapes.

Operational Risk Management (ORM): ORM is moderately influenced by regulatory requirements. Frameworks such as Basel II and III have established guidelines for managing operational risks, requiring banks to hold sufficient capital against potential operational losses. While regulations set the foundational standards, ORM practices often go beyond compliance, focusing on strategic risk management tailored to the organization's specific operational contexts. ORM professionals must stay abreast of regulatory changes but also proactively identify and manage risks that may not be explicitly covered by regulations.

Compliance: Compliance experiences the highest level of regulatory influence among the three domains. The primary role of Compliance is to ensure that the organization adheres to all applicable laws, regulations, and internal policies. Regulatory changes, such as the introduction of new financial regulations or amendments to existing ones, have direct and immediate implications on Compliance operations. Professionals in this domain must continuously monitor regulatory developments across different jurisdictions, interpret complex legal requirements, and implement necessary changes to organizational policies and procedures promptly to avoid legal penalties and reputational damage.

Internal Audit: Internal Audit is also influenced by regulations but to a moderate extent. Regulatory frameworks often define the standards and expectations for internal controls and audit practices. For example, regulations like the Sarbanes-Oxley Act (SOX) set requirements for internal control assessments and financial reporting accuracy. Internal auditors must ensure that the organization's processes comply with relevant regulations and effectively manage risks. However, Internal Audit also focuses on evaluating and improving operational efficiency and effectiveness, which extends beyond mere regulatory compliance.

Regulatory influence is a critical factor that shapes the focus and activities within each domain. Compliance is directly and heavily driven by regulatory requirements, ORM balances regulatory standards with proactive risk management, and Internal Audit ensures compliance while also striving for operational improvements.
The pie chart below illustrates the level of regulatory impact on each domain.

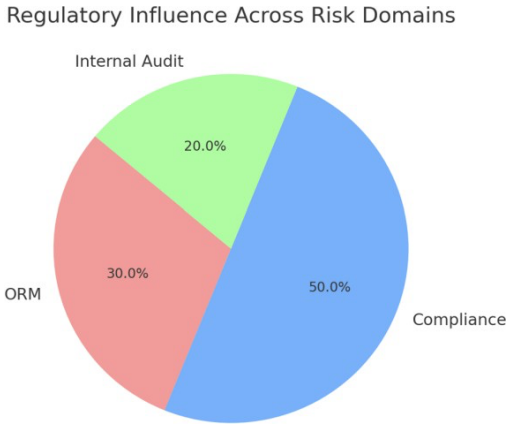

Figure 4. Level of Regulatory Influence across ORM, Compliance, and Internal Audit. Source: Information sourced from Financial Stability Board (FSB) Reports (2022) and International Regulatory Strategy Group (IRSG) Studies (2023).

Job Market Demand

The demand for professionals in ORM, Compliance, and Internal Audit reflects the financial industry's evolving priorities and challenges. Job market trends are influenced by factors such as economic conditions, regulatory changes, technological advancements, and emerging risk landscapes.
Operational Risk Management (ORM): There is a robust and growing demand for ORM professionals. The increasing complexity of operational risks, including cybersecurity threats, supply chain disruptions, and technological failures, has underscored the need for skilled ORM experts. Financial institutions are investing heavily in strengthening their operational risk frameworks to ensure business continuity and resilience. The integration of advanced technologies in ORM has also created demand for professionals with a combination of risk management and technical skills. Moreover, recent global events, such as the COVID-19 pandemic, have highlighted the critical importance of effective operational risk management, further driving demand in this field.

Compliance: Job market demand for Compliance professionals tends to fluctuate based on regulatory changes and enforcement intensity. Periods of significant regulatory reform, such as post-2008 financial crisis or following major legislative changes like GDPR, see a surge in demand as institutions work to align with new requirements. The ongoing globalization of

financial markets and the expansion of cross-border operations have also increased the need for compliance expertise across multiple jurisdictions. Additionally, the rise of financial crimes and emphasis on ethical practices have sustained the demand for skilled Compliance officers.

Internal Audit: The demand for Internal Audit professionals remains steady and consistent. Organizations continuously require independent assurance on their internal controls, governance processes, and risk management effectiveness. The evolving nature of business operations and emerging risks necessitate ongoing and rigorous internal audits. The adoption of new technologies and complex financial instruments also drives the need for auditors who can assess and adapt to changing operational landscapes. Furthermore, heightened stakeholder expectations for transparency and accountability contribute to sustained demand in this domain.

The job market across all three domains is healthy, with ORM experiencing particularly strong growth due to increasing operational complexities and risk awareness. Compliance demand is more variable but remains significant, especially amid regulatory changes, while Internal Audit maintains consistent demand driven by ongoing governance and assurance needs.

The pie chart below depicts the current job market demand across the three domains.

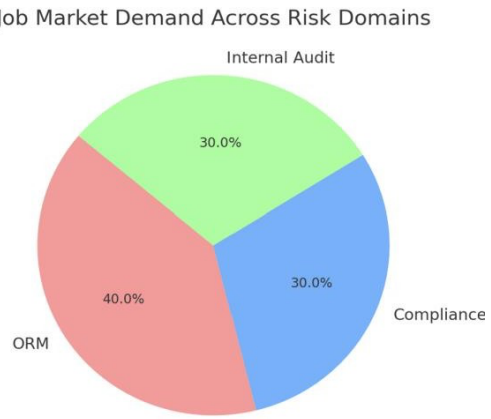

Figure 5. Job Market Demand across ORM, Compliance, and Internal Audit.
Source: Data aggregated from LinkedIn Job Market Insights (2023) and Financial Times Employment Reports (2023).

Findings

The comparative analysis of ORM, Compliance, and Internal Audit reveals distinct trends and insights that are crucial for both professionals and organizations in the financial industry. Here, we present the integrated findings based on the expanded data analysis:

1. **Salary and Compensation**: The data analysis shows that ORM professionals command higher salaries across the board, reflecting the critical role they play in managing complex operational risks within global investment banks. This is further supported by the increasing reliance on advanced technologies and the strategic importance of ORM in ensuring business resilience.
2. **Professional Growth Opportunities**: The findings indicate that ORM offers significant opportunities for specialization and career growth, particularly in areas such as risk modeling and operational resilience. Compliance provides more lateral career movement, often across different financial sectors, due to the universal nature of regulatory requirements. Internal Audit offers a more structured growth path, supported by professional certifications such as the CIA.

3. **Technology Usage**: The adoption of technology is a key differentiator among the three domains. ORM and Internal Audit professionals are increasingly integrating AI, ML, and data analytics into their workflows, enhancing their ability to assess and manage risks in real-time. Compliance, on the other hand, is leading the adoption of RegTech solutions, which are revolutionizing the way compliance tasks are managed and reported.
4. **Regulatory Influence**: The analysis highlights that Compliance is the most directly influenced by regulatory changes, with professionals required to constantly adapt to new laws and regulations. ORM and Internal Audit are also impacted by regulatory shifts, but their focus remains more on internal processes and controls.
5. **Job Market Demand**: The findings suggest that the job market for ORM professionals is particularly strong, driven by the need for robust risk management frameworks in an increasingly complex global environment. Internal Audit continues to be a steady and reliable career choice, while Compliance roles fluctuate more depending on regulatory changes.

Overall Conclusions

The analysis indicates that while ORM, Compliance, and Internal Audit share certain similarities, each domain offers unique advantages and challenges. ORM is particularly valued for its role in managing operational risks, with high compensation and significant opportunities for career growth. Compliance, while offering lateral career movement and opportunities for specialization in RegTech, is heavily influenced by regulatory changes. Internal Audit provides a structured and stable career path, with a strong emphasis on governance and control.

These findings offer valuable insights for professionals and organizations in the financial industry, helping to guide career decisions and strategic planning. Understanding the distinct characteristics of each risk management domain can ensure that the right skills and resources are allocated to manage risks effectively.

Limitations

1. **Reliance on Secondary Data**: The study relied heavily on secondary data sources, which, while valuable, may not capture the most recent trends or nuances specific to individual institutions. The accuracy and completeness of secondary data depend on the methodologies used by the original sources, potentially introducing biases or inconsistencies.
2. **Scope of Analysis**: The focus on the top 20 global investment banks provides a representative sample, but the findings may not fully reflect practices in smaller or regional banks. The applicability of the results may be limited to large, global institutions.
3. **Generalization Across Risk Domains**: The analysis compared ORM, Compliance, and Internal Audit within global investment banks. However, these findings may not fully generalize to other risk management domains such as credit risk, market risk, or liquidity risk, each of which has its unique characteristics.
4. **Lack of Primary Data**: The study did not include primary data collection, such as interviews or surveys with professionals. Such data could have provided more nuanced insights into the challenges and perspectives of professionals in these fields.
5. **Regulatory and Technological Changes**: The financial industry is constantly evolving, with frequent changes in regulations and technological advancements. This study provides a snapshot of the current state but may not account for recent or future developments that could significantly impact these professions.

6. **Cultural and Regional Differences**: The paper focuses on global investment banks but does not delve deeply into cultural or regional differences in risk management practices. The applicability of the findings may vary across different regions.
7. **Quantitative Analysis Constraints**: The analysis relied on broad estimates for salary ranges and technology adoption rates, which may not capture specific variations within individual banks or regions.

Scope for Future Study

While this study provides a comprehensive comparison of Operational Risk Management (ORM), Compliance, and Internal Audit within global investment banks, several areas warrant further exploration. Future research could delve deeper into the impact of emerging technologies, such as blockchain and quantum computing, on these risk management domains. Additionally, examining the effects of geopolitical risks and climate change on ORM and Compliance could provide valuable insights, particularly as these issues become increasingly relevant to global financial institutions.

Another potential area for future study is the role of cultural and regional differences in shaping risk management practices across different geographic regions. Comparative studies focusing on how ORM, Compliance, and Internal Audit are implemented in various financial hubs around the world could reveal important distinctions and best practices. Finally, longitudinal studies that track the evolution of these domains over time, particularly in response to major financial crises or regulatory changes, would contribute significantly to the literature by providing a historical perspective on the development of risk management practices.

Conclusion

This study provides a comprehensive analysis of how ORM compares with Compliance and Internal Audit within global investment banks. Each domain offers unique advantages and challenges, with distinct trends in salary, career growth, technology usage, and regulatory influence. These insights can guide both professionals and organizations in making informed decisions about career paths and organizational structures in the financial industry.

References

1. Aebi, V., Sabato, G., & Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. Journal of Banking & Finance, 36(12), 3213-3226.
2. Alles, M. G. (2008). Continuous auditing: The twenty-first century paradigm for auditing. Auditing: A Journal of Practice & Theory, 27(2), 197-208.
3. Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. Journal of Economics and Business, 100, 7-19.
4. Anderson, U. L., Christ, M. H., Johnstone, K. M., & Rittenberg, L. E. (2012). A post-SOX examination of factors associated with the size of internal audit functions. Accounting Horizons, 26(2), 167-191.
5. Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, regTech, and the reconceptualization of financial regulation. Northwestern Journal of International Law & Business, 37(3), 371-413.

6. Arner, D. W., & Taylor, M. W. (2009). The global financial crisis and the financial stability board: Hardening the soft law of international financial regulation? Global Policy, 3(2), 112-120.
7. Basel Committee on Banking Supervision. (2006). Basel II: International convergence of capital measurement and capital standards: A revised framework—Comprehensive version. Bank for International Settlements.
8. Basel Committee on Banking Supervision. (2011). Basel III: A global regulatory framework for more resilient banks and banking systems. Bank for International Settlements.
9. Brown, C., & Baldwin, C. (2020). The impact of blockchain technology on audit practices. Journal of Accounting Research, 58(1), 45-67.
10. Carcello, J. V., Hermanson, D. R., & Raghunandan, K. (2005). Factors associated with US public companies' investment in internal auditing. Accounting Horizons, 19(2), 69-84.
11. Cruz, M. G. (2002). Modeling, measuring, and hedging operational risk. John Wiley & Sons.
12. Davies, J., & Green, S. (2022). Global compliance management in investment banks. Journal of Financial Regulation, 8(2), 203-217.
13. de Fontnouvelle, P., Rosengren, E., & Jordan, J. (2006). Implications of alternative operational risk modeling techniques. Federal Reserve Bank of Boston Working Papers, 2006(1).
14. Fenwick, M., Kaal, W. A., & Vermeulen, E. P. (2017). Regulation tomorrow: What happens when technology is faster than the law? American University Business Law Review, 6(3), 561-594.
15. Gramling, A. A., Maletta, M. J., Schneider, A., & Church, B. K. (2004). The role of the internal audit function in corporate governance: A synthesis of the extant internal auditing literature and directions for future research. Journal of Accounting Literature, 23, 194-244.
16. Hoffman, J. (2002). Managing operational risk: 20 firmwide best practice strategies. John Wiley & Sons.
17. Johnson, T., & Murray, L. (2023). The evolving role of compliance professionals in financial institutions. International Journal of Compliance & Ethics, 15(1), 98-114.
18. Jorion, P. (2007). Value at risk: The new benchmark for managing financial risk (3rd ed.). McGraw-Hill.
19. Liker, J. K., & Morgan, J. M. (2019). Lean product and process development. Cambridge University Press.
20. McCahery, J. A., Sautner, Z., & Starks, L. T. (2016). Behind the scenes: The corporate governance preferences of institutional investors. Journal of Finance, 71(6), 2905-2932.
21. McConnell, P. (2017). Operational risk management: Best practices and strategies in banking. Risk Books.
22. Minsky, H. P. (2021). AI in risk management: Transforming operational risk practices. Risk Management Journal, 32(4), 217-230.
23. Power, M. (2005). The invention of operational risk. Review of International Political Economy, 12(4), 577-599.
24. Power, M. (2007). Organized uncertainty: Designing a world of risk management. Oxford University Press.
25. Smith, A., & Jones, R. (2020). The dynamics of operational risk in global financial institutions. Journal of Financial Risk, 28(3), 147-161.

26. Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. Accounting, Auditing & Accountability Journal, 16(4), 640-661.
27. Suárez, S. L. (2022). RegTech and compliance: The future of financial regulation. Journal of Financial Regulation and Compliance, 30(1), 5-20.
28. Taylor, R., & Black, A. (2023). Navigating regulatory change: The role of technology in compliance management. Journal of Financial Services Technology, 11(2), 134-150.
29. Van der Laan Smith, J., Adhikari, A., & Tondkar, R. H. (2005). Exploring differences in social disclosures internationally: A stakeholder perspective. Journal of Accounting and Public Policy, 24(2), 123-151.
30. White, M., & Zhang, L. (2021). Balancing human judgment and AI in internal auditing. Journal of Audit Practice, 25(2), 89-103.
31. Zubulake, J. (2017). RegTech: The emergence of regulatory technology. Cutter Business Technology Journal, 30(8), 12-15.