

Integrating Financial Controls and Risk Escalation in Casino Resorts: A Conceptual Framework

Esther Ogechi Nwozaku^{1,*}, Dominick Aondakaa², Joy Kweku Sakyi³

¹ *Cage Supervisor, MGM National Harbor Hotel & Casino, Maryland, United States*

² *California Miramar University, San Diego, California, United States*

³ *Independent Researcher, Rock Hill, South Carolina, United States*

***Corresponding author:** Esther Ogechi Nwozaku (nwozakuesther@gmail.com)

Email addresses: nwozakuesther@gmail.com (E. O. Nwozaku); aondakaadominick@gmail.com (D. Aondakaa); joy.sakyi@outlook.com (J. K. Sakyi)

Abstract

Casino resorts record large volumes of cash and cash-equivalent transactions, and the same records serve two purposes that are seldom designed to work together: finance teams use them to confirm revenue and protect assets, while compliance teams use them to meet anti-money laundering reporting duties. Because the handoff between these functions is usually informal, compliance-relevant facts can be closed as routine accounting corrections, finance staff can be drawn into judgments about suspicion, and compliance reviewers can receive referrals too late or with too little evidence. This paper examines how frontline transaction records, financial review and compliance escalation should interact in casino resort operations. Grounded in documented workflows, it develops a six-stage process framework that follows a transaction from first recording to governance and audit oversight. The central result is a clear division of judgment in which finance routes facts and compliance decides suspicion. An exception remains an accounting matter only when a recording, timing or system error fully explains it and no risk indicator is present; otherwise it is referred, and correcting the accounting never closes the compliance question. The framework specifies accountability at each handoff, the speed needed to protect the regulatory reporting period, and the records that must travel with each referral. It is designed to raise referral quality rather than volume, and closes with testable propositions.

Keywords: *casino resorts; internal control; anti-money laundering; Bank Secrecy Act; suspicious activity reporting; revenue audit; escalation; three lines model; process framework*

1. INTRODUCTION

A modern casino resort is several cash-intensive businesses operating under one roof and, frequently, under one patron identity. A guest may buy chips at a table, redeem a ticket at a kiosk,

deposit front money at the cage, settle a hotel folio in currency, and dine at an outlet charged to the room, all within a single gaming day. Each of these events produces a record. Each record is first created by a frontline employee whose principal job is customer service and accurate handling of cash and cash equivalents.

Two control systems then draw on those records. The first is the financial control system, anchored in state or tribal minimum internal control standards and in the casino's own written system of internal control. Its questions are whether revenue is complete and accurate, whether assets are safeguarded, and whether discrepancies are explained. The second is the anti-money laundering (AML) compliance system required of casinos under the Bank Secrecy Act (BSA) and its implementing regulations at 31 C.F.R. Part 1021. Its questions are whether reportable currency transactions have been captured and reported, and whether any activity is suspicious and must be reported to the Financial Crimes Enforcement Network (FinCEN).

These systems share data but differ in logic. A cash variance at a cage window is, in the first instance, an accounting matter. A pattern of transactions kept just under a reporting threshold is, in the first instance, a compliance matter. Yet the two often meet in the same document, on the same shift, in front of the same reviewer. When the interface between them is not designed, three failure modes appear. Compliance-relevant facts may be resolved as clerical corrections and never reach a qualified reviewer. Accounting staff may be drawn into making judgments about suspicion that they are not trained or authorized to make. Or compliance reviewers may receive referrals without the transactional evidence they need to reach a defensible decision within regulatory deadlines.

This paper addresses the following research question:

How should frontline transaction records, financial review, and compliance escalation interact in casino resort operations?

The paper makes three contributions. First, it maps the documented workflows that connect frontline recording, financial review, and compliance review, drawing on regulation, minimum internal control standards, industry guidance, and public enforcement records. Second, it proposes an explicit rule for separating accounting exceptions from concerns that require qualified

compliance review, together with a dual-track path for exceptions that are both. Third, it presents a process framework that assigns review responsibilities, defines escalation stages, and specifies evidence requirements, and it converts the framework into propositions and research questions that can be tested empirically.

The paper is conceptual. It does not report the results of interviews or field observation. Practitioner consultation is built into the research design as a validation step that will proceed if access to casino resort finance and compliance personnel can be arranged. The framework is written for United States casino operations, with the Nevada and federal tribal gaming regimes used as reference points, but its logic is intended to transfer to other jurisdictions with comparable internal control and AML obligations.

Gaming regulators have long treated internal control as a condition of licensure rather than a matter of management preference. In Nevada, Nevada Gaming Commission Regulation 6.090 requires each Group I licensee to establish administrative and accounting procedures both for determining its liability for gaming taxes and fees and for exercising effective control over its internal fiscal affairs. The Nevada Gaming Control Board has adopted Minimum Internal Control Standards (MICS) under that regulation as the floor for internal controls over gaming operations, and each licensee must prepare a written system of internal control that sets out detailed operating procedures complying with the MICS. An independent accountant must report annually on whether that written system complies with Regulation 6.090, and procedures that do not satisfy the MICS may be implemented only under a written variation granted by the Board (Nevada Gaming Commission, 2023; Nevada Gaming Control Board, 2022) (Meriç, 2021).

For tribal gaming, the National Indian Gaming Commission (NIGC) first published Minimum Internal Control Standards in 1999 with the stated aim of reducing the risk of loss arising from customer or employee access to cash and cash equivalents within a casino. Comprehensive standards for Class II gaming were adopted at 25 C.F.R. Part 543 in 2012 and later amended to address kiosks, drop and count, cage and vault, and surveillance (National Indian Gaming Commission, 2012; National Indian Gaming Commission, 2013; National Indian Gaming Commission, 2018). Class III operations are governed by tribal internal control standards

established under tribal-state compacts, often modeled on the Class III standards at 25 C.F.R. Part 542.

Across these regimes the architecture is similar. Standards specify segregation of duties, dual custody of cash, sequentially controlled forms, supervisor signatures, count procedures, and a revenue or income audit function that independently reconciles each gaming day's activity. Casino accounting texts describe these controls in operational detail, from cage cashiering and credit to count procedures and gaming tax reporting (Greenlees, 2008; Kilby et al., 2005), and early hospitality research described how regulator-mandated standards shape segregation of duties and accountability across the cage, the gaming floor, and the count room (DeFranco & Wortman, 1997). Comparative work on casino regulation shows that jurisdictions differ in how far they prescribe such controls or leave them to licensees (Cabot & Pindell, 2014). In lodging, internal control practices appear not to differ meaningfully by property age, size, or ownership (Annaraud et al., 2014), which suggests that control quality depends more on design and execution than on organizational characteristics. The standards are oriented toward accuracy and asset protection. They create a rich evidentiary trail, but they do not, on their own, say when a discrepancy should be treated as a possible indicator of financial crime.

Casinos and card clubs with gross annual gaming revenue above \$1 million are financial institutions for BSA purposes. Under 31 C.F.R. § 1021.210, each such casino must implement a written AML compliance program reasonably designed to assure and monitor compliance. At a minimum the program must provide for a system of internal controls to assure ongoing compliance, internal or external independent testing, training of personnel that includes identifying unusual or suspicious transactions, an individual or individuals responsible for day-to-day compliance, procedures for using all available information to verify identity and to determine whether reports are required, and the use of automated systems where the casino relies on them.

Three reporting and recordkeeping obligations are especially relevant to the interface studied here. First, casinos must file a Currency Transaction Report by Casinos (CTR) for each transaction in currency, involving cash in or cash out, of more than \$10,000 in a gaming day, and multiple transactions must be aggregated when the casino has knowledge that they are by or on behalf of the same person (31 C.F.R. §§ 1021.311, 1021.313). Structuring transactions to evade these

requirements is itself prohibited (31 C.F.R. § 1021.314). Casinos commonly maintain multiple transaction logs (MTLs) at points of sale to support aggregation. Second, a casino must report any transaction of at least \$5,000 that it knows, suspects, or has reason to suspect involves funds from illegal activity, is designed to evade reporting requirements, has no apparent lawful purpose, or involves use of the casino to facilitate criminal activity (31 C.F.R. § 1021.320). A Suspicious Activity Report by Casinos (SAR) is generally due within 30 calendar days after initial detection of facts that may constitute a basis for filing, and SARs and information that would reveal their existence are confidential. Third, required records must generally be retained for five years (31 C.F.R. § 1010.430).

FinCEN has issued interpretive guidance for casinos on aggregation, identity verification, front money and marker records, and suspicious activity monitoring (Financial Crimes Enforcement Network, 2012a). Its analysis of several years of casino SAR filings found structuring around chip redemptions and minimal gaming among the most frequently reported behaviors (Financial Crimes Enforcement Network, 2012b), which are exactly the patterns that first appear in cage and revenue audit records. Concern about the sector is long-standing: a federal review in the 1990s already linked the rapid growth of casinos to money laundering vulnerability and noted limits on oversight capacity (U.S. General Accounting Office, 1996). More recently, the national money laundering risk assessment identified compliance weaknesses at some regulated institutions as a persistent vulnerability (U.S. Department of the Treasury, 2024), and the government-wide AML priorities issued under the Anti-Money Laundering Act of 2020 are expected to be built into risk-based programs (Financial Crimes Enforcement Network, 2021).

The phrase "initial detection" matters for this paper. FinCEN has indicated that the 30-day period does not begin at the moment of the transaction but when the institution, after a reasonable review, knows or has reason to suspect that the activity meets the reporting criteria. The timeliness of the casino's internal escalation process therefore directly affects whether the regulatory clock is managed responsibly. A referral that sits in an accounting queue for weeks erodes the time available for compliance review, and a record that cannot be retrieved weakens the basis for either filing or not filing.

Public enforcement records offer a documented, if partial, view of where the interface between finance and compliance has broken down. In 2015 FinCEN assessed a \$10 million civil money penalty against Trump Taj Mahal Casino Resort, finding that the casino had willfully violated BSA requirements, including by failing to implement an effective AML program and failing to report suspicious activity relating to several transactions; FinCEN described its program as lacking adequate policies, procedures, and internal controls for monitoring transactions and filing SARs (Financial Crimes Enforcement Network, 2015b). In the same year, FinCEN found willful violations at Caesars Palace connected to weak controls over private gaming salons and foreign marketing offices and to unfiled SARs (Financial Crimes Enforcement Network, 2015a). In 2013, Las Vegas Sands entered a non-prosecution agreement with the U.S. Attorney's Office for the Central District of California and agreed to pay about \$47.4 million after funds associated with a foreign national later charged with drug offenses had moved through its accounts without a SAR being filed. In 2024, Wynn Las Vegas entered a non-prosecution agreement with the U.S. Department of Justice and agreed to forfeit approximately \$130 million in connection with the use of unlicensed money transmitting businesses to move patron funds.

Outside the United States, the inquiry led by Patricia Bergin into Crown Resorts in New South Wales (Bergin, 2021), the Royal Commission into the Casino Operator and Licence in Victoria (Royal Commission into the Casino Operator and Licence, 2021), the review led by Adam Bell into The Star in New South Wales (Bell, 2022), and the Perth Casino Royal Commission (Perth Casino Royal Commission, 2022) each documented ways in which financial transaction records, including hotel and non-gaming channels, were used to move funds while red flags were not escalated or were escalated without effect. In Canada, the Cullen Commission devoted several chapters to how illicit funds moved through British Columbia casinos and to the regulatory and operator failures that allowed it (Cullen, 2022), and Australia's financial intelligence agency assessed the money laundering risks of junket tour operations (Australian Transaction Reports and Analysis Centre, 2020). A recurring theme across these reports was that information existed somewhere in the organization but was not brought together in front of someone with the authority and expertise to act on it.

Scholarly analyses reach similar conclusions. Studies of Australian and Southeast Asian casinos trace exposure to junket operators, shadow banking, and organized crime (Langdale, 2022;

Langdale, 2024). Research on Macau documents how criminal groups shaped the VIP room and junket business (Lo & Kwok, 2017), and comparative legal work shows how the triggers for suspicious activity reporting and the obligations placed on casinos differ across jurisdictions (Kleiman, 2015; Lam & Greenlees, 2017). A review of gambling and organized crime notes that evidence on how well transaction reporting controls work remains limited (Ferentzy & Turner, 2009), and work on electronic gaming machines shows that laundering risk is not confined to the tables and the cage (Buchanan, 2018).

These cases do not show that finance personnel caused compliance failures. They show that the absence of designed connections between transaction recording, financial review, and compliance review can allow risk-relevant facts to remain fragmented, and that regulators judge casinos on whether the program as a whole surfaced and acted on available information.

The literature relevant to this question is spread across accounting, criminology, organizational behavior, hospitality management, and information systems. Much of the most directly applicable conceptual work comes from regulated financial services, health care, and other high-volume transaction environments rather than from gaming, and it is drawn on here for the design principles it offers.

Two general frameworks inform the allocation of responsibilities proposed here. The Committee of Sponsoring Organizations of the Treadway Commission defines internal control through five integrated components: control environment, risk assessment, control activities, information and communication, and monitoring activities (Committee of Sponsoring Organizations of the Treadway Commission, 2013). The information and communication component is directly relevant, because it requires that relevant, quality information reach the people who need it to carry out their responsibilities. The Institute of Internal Auditors' Three Lines Model assigns management and frontline operations the first-line role of owning and managing risk, specialist functions such as compliance the second-line role of expertise, support, monitoring, and challenge, and internal audit the third-line role of independent assurance (Institute of Internal Auditors, 2020). The 2020 update emphasizes that the lines describe roles and relationships rather than rigid structures, which suits casino resorts where finance staff perform both first-line reconciliation and some monitoring activities.

COSO's enterprise risk management framework extends this logic by connecting risk with strategy and performance (Committee of Sponsoring Organizations of the Treadway Commission, 2017). Critics note that the lines can blur in practice, with tensions over role clarity, independence, and accountability between business units, risk and compliance, and internal audit (Davies & Zhivitskaya, 2018). Field research shows that enterprise risk management takes different forms depending on existing organizational logics and on the calculative cultures of risk officers (Arena et al., 2010; Mikes, 2009), and Power (2009) warns that process-based risk management can become inward looking, demonstrating auditability rather than managing risk. For casino resorts, these critiques caution against treating a well-drawn organization chart as evidence that escalation actually works.

Industry guidance completes the picture. The American Gaming Association's Best Practices for Anti-Money Laundering Compliance, first issued in 2014 and revised in a third edition in 2022, advises casinos to analyze their risk and then structure their compliance function to mitigate it, and it describes the cooperation among cage, table games, slots, surveillance, and compliance that effective monitoring requires (American Gaming Association, 2022). Internationally, the Financial Action Task Force's guidance on a risk-based approach for casinos (Financial Action Task Force, 2008) and its joint typologies report with the Asia/Pacific Group on Money Laundering (Financial Action Task Force & Asia/Pacific Group on Money Laundering, 2009) describe the high volume and variety of casino transactions that make the sector vulnerable, and identify methods such as minimal-play cash conversion, chip purchases with little play, and the use of third parties and casino accounts.

Management control scholarship distinguishes between controls designed to ensure that routine processes run as intended and controls designed to surface strategic or emergent uncertainties (Merchant & Van der Stede, 2017; Simons, 1995), and it treats an organization's controls as an interrelated package rather than as separate devices (Malmi & Brown, 2008). Revenue audit in a casino is a strong example of the first kind. It is diagnostic: it compares actual results with expected results, identifies variances, and drives correction. Suspicious activity review belongs more to the second kind. It requires interpretation of behavior and intent under uncertainty, judgments that are context dependent and that carry legal consequences.

Evidence from the Sarbanes-Oxley era shows that internal control weaknesses are more common in smaller, younger, more complex, or rapidly changing organizations (Doyle et al., 2007) and that remediating them is followed by better accrual quality (Ashbaugh-Skaife et al., 2008). Higher quality internal audit is associated with less earnings management (Prawitt et al., 2009), and internal audit effectiveness depends on both organizational and individual factors (Lenz & Hahn, 2015). Conceptual work on risk-based internal control in banking and insurance (Akomolafe & Agu, 2019a), data-driven risk evaluation in financial institutions (Akomolafe & Agu, 2019b), technology-enabled risk assessment for internal audit (Akomolafe & Agu, 2018), risk-based auditing (Akomolafe et al., 2023a), and comparative reviews of SOX compliance frameworks (Agu et al., 2023) supports the same conclusion: controls should be designed around risk rather than applied uniformly. Variance analysis, the core analytical tool of revenue audit, requires deliberate training to apply well (Ebhojie et al., 2023b) and is increasingly supported by analytics for cost control (Aliliele, Eboh, et al., 2024).

Power (2007) observes that organizations increasingly convert uncertainty into auditable processes, sometimes producing documentation that demonstrates diligence without improving judgment. For casino resorts, this suggests a risk on both sides. If every accounting exception is forwarded to compliance, the result is volume without signal. If accounting staff are asked to screen for suspicion, the result can be a defensive process that records decisions without the expertise to support them. The design problem is to let each function do what it is competent to do, and to connect them at the point where the nature of the question changes.

Assurance research informs Stage 6 and the feedback loop. Relevant work covers internal audit quality (Akomolafe & Agu, 2018), audit liaison and corrective action planning in multinational organizations (Ebhojie et al., 2023a), internal audit systems in industrial operations (Obogo et al., 2020), maturity models that predict audit outcomes (Adeyelu & Dagodzo, 2024), regulatory evidence and corrective action protocols (Adeyelu, 2021), and security audit linked to enterprise risk assessment (Dosunmu & Ogundele, 2019). Evidence requirements draw on work on audit trails and tamper-proof regulatory recordkeeping (Anichukwueze et al., 2021; Oshoba et al., 2020), data sensitivity classification and regulatory traceability (Aliliele, Mbonu, et al., 2024), privacy-preserving data architectures for regulated analytics (Atakpa & Abolaji, 2022), role-based security and identity and access management (Badmus et al., 2024; Mbonu et al., 2020), data protection

impact assessment in financial infrastructure (Mbonu, Iwuanyanwu, et al., 2022), and regulatory transparency in cross-border data exchange (Kumuyi et al., 2023). These are relevant to the restricted handling that compliance case files require.

Escalation itself has analogues in information security and service management, where log analytics, incident response playbooks, and service ticketing define who acts on an alert, how fast, and with what evidence (Dosunmu & Ogundele, 2021; Ladapo et al., 2023; Mbonu et al., 2019). Standard operating procedures can serve as infrastructure for sustaining operational change (Agboada et al., 2019; Eyetsemitan et al., 2022), and standardized reporting and decision workflows improve data quality and management visibility (Alieme et al., 2022). Business analysis methods help structure ambiguous problems into defined processes (Alieme et al., 2024), and workflow standardization in legal operations shows how high-volume review can be made consistent (Uchechi et al., 2018; Uchechi et al., 2021). Performance monitoring through dashboards, real-time key performance indicators, and accountability frameworks (Ezeako et al., 2024; Ogbole et al., 2021; Sakyi et al., 2022; Tonoyan et al., 2024), cross-functional and multi-site indicator design (Akin-Oluyomi & Akhigbe, 2023; Seyi-Lande et al., 2022), process metrics for regulatory oversight (Anioke & Atima, 2023), and attention to workforce behavior and retention (Akhigbe et al., 2023; Falemi et al., 2023) supports the governance stage, where referral timeliness, classification accuracy, and recurring control failures must be tracked (Olagunju et al., 2023).

The compliance side of the interface has its own literature. Economic modeling shows that heavy penalties for missed reports can push institutions toward defensive over-reporting, diluting the information value of each report (Takáts, 2011). Comparative studies contrast rule-based and risk-based reporting regimes and link differences in report volume and quality to legal culture and to the incentives facing supervisors and reporting institutions (Dalla Pellegrina & Masciandaro, 2009; Unger & van Waarden, 2009). Broader assessments question how far the AML regime reduces crime relative to its costs and point to weak data for judging effectiveness (Levi & Reuter, 2006; Levi et al., 2018; Reuter & Truman, 2004). Other work warns that effectiveness methods may reward box-ticking (Pol, 2018), highlights measurement problems in suspicious transaction reporting (Chaikin, 2009), and documents the burden that reporting institutions perceive (Harvey, 2004).

Studies of compliance officers and private financial policing show that suspicion is produced through routine work by staff who balance prevention duties against commercial pressures (Amicelle & Iafolla, 2018; Verhage, 2011), and a federal review found that feedback to reporting institutions on the usefulness of their filings was irregular (U.S. Government Accountability Office, 2019). For the present framework this literature has two implications. A well-designed finance-to-compliance referral path should improve the quality of what reaches compliance rather than simply increase its volume, and the decision to file must remain with people who understand both the legal standard and the operating context.

Recent conceptual and review work outside gaming points in the same direction. It includes reviews of AML and anti-bribery regimes across emerging and developed markets (Ominyi & Anichukwueze, 2021), of predictive analytics for AML detection in banking (Atakpa, 2021), and of integrated cybersecurity and AML governance (Fadayomi et al., 2021). Frameworks have been proposed for AI-assisted compliance monitoring and anomaly detection in high-volume transaction environments (Ominyi et al., 2024), for real-time compliance pipelines linked to enterprise data governance (Uchechi et al., 2022), and for standardizing compliance controls in high-volume distribution networks (Uchechi et al., 2023). Work on sanctions and export-control compliance (Jones & Ominyi, 2023), controls for cross-border payment operations (Okafor, Farounbi, et al., 2024; Olaogun et al., 2023), AI-driven risk scoring for payment transactions (Adesuyi et al., 2024), and risk-based interdiction of illicit products (Aneke & Adesemoye, 2021) applies similar risk-based logic in other settings.

A large organizational behavior literature explains why relevant information often fails to move upward. Morrison & Milliken (2000) describe organizational silence as a collective condition in which employees withhold concerns because they expect speaking up to be futile or risky. Detert & Edmondson (2011) show that employees hold implicit beliefs about when voice is appropriate, such as not bypassing a supervisor or not raising issues without a solution. Interview evidence indicates that most employees have withheld concerns from superiors, often for fear of being labeled or damaging relationships (Milliken et al., 2003), and fear-based silence takes several distinct forms (Kish-Gephart et al., 2009). In a casino resort, a cage cashier who notices that a patron changed a transaction amount after being asked for identification may reasonably wonder

whether this is "their" issue, whether a supervisor will treat it as a nuisance, and whether a note on an MTL is enough.

The same literature identifies conditions that encourage voice. Employees speak up more when leaders are seen as open (Detert & Burris, 2007) and when teams share a belief that interpersonal risk taking is safe (Edmondson, 1999); Morrison (2014) synthesizes the antecedents and consequences of voice and silence. Research on whistleblowing models how people who observe wrongdoing decide whether to report (Near & Miceli, 1985), and evidence from large corporate frauds shows that employees are among the most important sources of detection (Dyck et al., 2010). Values-based ethics and compliance programs are associated with greater willingness to report problems (Treviño et al., 1999), and research on business compliance stresses that firms interpret and implement rules internally in ways that shape outcomes (Parker & Nielsen, 2011). Practical levers include ethics and compliance training designed for measurable behavioral change (Anichukwueze et al., 2020), cross-functional legal education as a form of risk mitigation (Anichukwueze et al., 2022), and awareness training aimed at insider behavior and the confidentiality of records (Onche et al., 2020; Onche et al., 2024).

Research on high reliability organizations points to design responses. Weick & Sutcliffe (2007) emphasize preoccupation with small failures, reluctance to simplify interpretations, and deference to expertise. Vaughan (1996) shows how repeated anomalies can come to be treated as acceptable risk, and Reason (1997) explains how latent conditions in organizational defenses combine with everyday errors. Applied here, these ideas suggest that recurring cash variances should not be corrected routinely without anyone asking whether they form a pattern, that frontline and finance staff should be expected to report small anomalies without first deciding whether they matter, that exception categories should not collapse ambiguous cases into clerical corrections, and that the decision about suspicion should be deferred to the people with the relevant expertise. FinCEN's 2014 advisory on promoting a culture of compliance makes a similar point in regulatory terms, stressing that relevant information from across the organization should be shared with compliance staff (Financial Crimes Enforcement Network, 2014).

Fraud theory adds a further reason to design the interface carefully. Cressey's study of embezzlers, which became the basis of the fraud triangle (Cressey, 1953), and its later extension to include the

perpetrator's capability (Wolfe & Hermanson, 2004) both stress opportunity, which control design can reduce. The occupational fraud literature reports that tips, many of them from employees, are the leading method of detection, and it analyzes food service and hospitality as a distinct sector (Association of Certified Fraud Examiners, 2024). A systematic review concludes that fraud in hospitality remains under-researched (Kassem, 2024), and survey evidence links employee theft in hospitality to understaffing and weak training (Poulston, 2008).

Related conceptual work extends these concerns to digital channels and to identity, which matters in casinos because identification at reporting thresholds is itself a control point. It includes models for classifying insider threats (Akeju et al., 2018), financial forensics for cyber-enabled fraud (Ekechi et al., 2022), detection of synthetic identity fraud (Elebe et al., 2023), privacy-focused digital identity verification (Kumuyi et al., 2024), and fraud exposure and risk assessment in investment settings (Eboh & Aliliele, 2023; Eboh & Aliliele, 2024).

Casino operations texts describe the cage, count rooms, table games, slots, and credit functions in considerable detail (Kilby et al., 2005), but integrated resorts add a layer that standards and texts treat less fully. Hotel, food and beverage, retail, entertainment, and convention revenues are usually recorded in separate property management and point-of-sale systems with their own controls and reconciliations. Hotel operations rely on front office and night audit procedures (Bardi, 2010), a standardized departmental chart of accounts (Hotel Association of New York City, 2014), and accounting conventions specific to lodging and food service (Schmidgall & DeFranco, 2022). A review of hospitality technology research finds that systems are applied separately across many functional units (Law et al., 2014), which reinforces the silo problem.

A patron's resort footprint may therefore be visible only when data from several systems are joined. This matters for AML purposes because the obligation to use all available information, and the knowledge relevant to aggregation and suspicion, do not stop at the casino floor. It matters for finance because cross-outlet transfers, comps, and folio settlements are themselves sources of accounting exceptions. Data quality has intrinsic, contextual, representational, and accessibility dimensions (Wang & Strong, 1996), so the usefulness of a joined patron view depends on more than technical connectivity. Work on data integration and interoperability (Badmus et al., 2019; Badmus et al., 2022; Ilodigwe & Adesemoye, 2021), API governance in financial institutions

(Aliliele et al., 2023), risk-based business intelligence architecture (Mbonu, Aliliele, et al., 2021), data integrity failures and remediation in regulated operations (Aneke et al., 2023), automated financial consolidation (Bola-Sadipe et al., 2023), and reconciliation-centered workflow redesign (Dogbatsey et al., 2019) offers design patterns for joining these records reliably.

Process management literature frames this as a problem of the "white space" between functions, where handoffs are unowned and performance degrades (Rummler & Brache, 1995). The literature reviewed here suggests that the weakest point in many casino resort control systems is not the strength of any single control but the handoff between the finance and compliance functions and between gaming and non-gaming systems.

Anomaly detection techniques are well established across domains (Chandola et al., 2009). Accounting research on continuous assurance proposes automated monitoring of transactions and controls that generates exceptions and alarms for human follow-up (Alles et al., 2008; Vasarhelyi et al., 2004), and big data and process mining allow auditors to analyze full populations and to see how processes actually run (Appelbaum et al., 2017; Jans et al., 2013). Reviews of predictive analytics and machine learning for financial fraud and AML detection describe models that surface unusual patterns at a scale beyond manual review (Atakpa & Abetoh, 2022; Atakpa, 2021), and related work proposes anomaly detection for financial time series (Atakpa & Fobellah, 2023) and adaptive risk scoring for real-time transaction monitoring (Fadayomi et al., 2024).

Applications in adjacent sectors include forensic analytics for fraud detection and compliance monitoring (Mbonu, Iwuanyanwu, et al., 2021), predictive analytics for financial risk detection in public systems (Adelanwa et al., 2023), audit analytics for financial oversight (Abetoh & Atakpa, 2024), AI-based detection of payment fraud in health care (Atakpa et al., 2024), revenue assurance in service-intensive organizations (Sakyi et al., 2023), and predictive compliance monitoring based on complaint data (Adeyelu, 2018). For casino resorts, these approaches suggest ways to strengthen financial review and exception triage, for example by flagging patron-level patterns across outlets. They do not remove the need for a qualified reviewer to decide on reporting. Work on human-in-the-loop machine learning (Ladapo et al., 2022; Ladapo et al., 2024), on algorithmic accountability and model risk management (Ominyi & Anichukwueze, 2023), and on responsible governance of automated decision systems in regulated industries (Ominyi & Anichukwueze,

2024) supports keeping that judgment with people. The framework therefore treats analytics as an input to Stages 3 and 4, not as a substitute for Stage 5.

A further strand argues for integrating controls that are often designed separately. Conceptual models of integrated governance and compliance strategies (Akomolafe & Agu, 2019c), harmonized risk governance, technology infrastructure, and compliance frameworks (Okafor, Osuji, et al., 2024), quantitative compliance risk assessment (Akomolafe et al., 2023b), and cybersecurity risk management and regulatory compliance in financial institutions (Bello et al., 2024) share this paper's premise that controls work better as a connected system than as parallel silos. Fadayomi et al. (2021) make a similar case for joining AML governance with other control domains, and work on controls for cross-border payment operations emphasizes end-to-end monitoring across handoffs (Okafor, Farounbi, et al., 2024).

Work on financial reporting and accountability adds detail on how such integration can be achieved. It includes accounting systems designed to strengthen transparency and regulatory compliance (Bola-Sadipe et al., 2019), financial reporting models for compliance and organizational accountability (Medon & Oduleye, 2022), data-driven tax compliance and tax governance analytics (Bola-Sadipe et al., 2022; Lawal & Oduleye, 2018), translation of regulatory requirements into operational compliance workflows (Eyetsemitan et al., 2021), budget compliance and statutory reporting (Dogbatsey & Ebhojie, 2018), and data-led cost governance (Adesuyi et al., 2023). Studies of compliance integration after mergers and in cross-border regulatory clearance (Ominyi & Anichukwueze, 2020; Ominyi, 2020), harmonization of data protection obligations (Ominyi & Anichukwueze, 2022), shared responsibility across jurisdictions (Ominyi et al., 2021), and multinational compliance strategy (Anichukwueze et al., 2019) show how obligations from several sources can be mapped to a single operating model. Related frameworks address procurement risk (Bello et al., 2023), enterprise risk management linked to human resources strategy (Falemi et al., 2024), risk-based decision-making in regulated manufacturing (Aneke & Adesemoye, 2020), and AI-enabled IT general controls and SOX audit automation (Mbonu, Aliliele, et al., 2022).

Regulatory sources specify what must be recorded and what must be reported. Industry guidance describes red flags and program elements. Governance frameworks allocate roles in general terms,

and adjacent literatures offer design patterns for analytics, integration, escalation, and assurance. What is less developed, at least in publicly available sources, is an explicit model of how a frontline record in a casino resort becomes a financial review item, how that item is classified, when and how it moves to qualified compliance review, and what evidence must accompany it. This paper proposes such a model.

2. RESEARCH METHOD

The study uses a conceptual design of the kind Jaakkola (2020) describes as a model-building approach, which aims to construct a framework that predicts relationships among constructs and can later be tested. Following MacInnis (2011), the contribution sought is one of delineation and integration: identifying the relevant entities and stages and then relating them in a structure that was not previously explicit. In line with Whetten (1989), the framework specifies what its elements are, how they relate, why they relate as proposed, and the conditions under which the claims should hold.

Three categories of documents were used, following the logic of document analysis as a systematic qualitative method (Bowen, 2009). The first is binding requirements: 31 C.F.R. Part 1021 and related BSA provisions; Nevada Gaming Commission Regulation 6.090 and the Nevada MICS; and 25 C.F.R. Part 543. The second is guidance: FinCEN advisories and casino guidance, the American Gaming Association's AML best practices, FATF guidance and typologies, COSO's Internal Control Integrated Framework, and the IIA Three Lines Model. The third is documented practice as revealed in public enforcement actions and inquiry reports, which describe actual workflows and where they failed. Academic literature on management control, risk management, organizational voice, fraud, data integration, and process management was used to interpret the documents.

Workflows were mapped in four steps, drawing on process identification and modeling techniques from business process management (Dumas et al., 2018). First, recording points were inventoried, meaning every location in a casino resort where a cash or cash-equivalent transaction is first documented. Second, for each recording point, the documented review steps were traced from shift-level verification through revenue audit, using MICS requirements as the baseline. Third, the

points at which BSA obligations attach to the same records were identified, including MTL entries, identification requirements, CTR aggregation, and SAR monitoring. Fourth, handoffs between functions were marked, and for each handoff the sources were examined for a defined owner, timing, and evidence standard. Handoffs lacking one or more of these attributes were treated as design gaps that the framework should close. This procedure follows the logic of reconciliation-centered workflow redesign described by Dogbatsey et al. (2019).

The framework has not yet been reviewed by practitioners. A validation phase is planned in which casino resort finance, revenue audit, cage, compliance, surveillance, and internal audit personnel would be asked to review the stage definitions, the classification rule, the responsibility assignments, and the evidence requirements, and to identify any that conflict with operating realities. This phase is contingent on access. If access is obtained, consultation would use semi-structured interviews or structured review sessions, and comparison across properties could follow established procedures for building theory from cases (Eisenhardt, 1989). Consultation would not request any SAR or SAR-related information and would follow the confidentiality limits in 31 C.F.R. § 1021.320(e). If access is not obtained, the framework remains a theory-grounded proposal and the propositions presented in the Results and Discussion define what later empirical work would need to test.

The framework is also informed by the author's professional experience in casino resort operations, where the practical questions addressed here arise in daily work: how a variance found at reconciliation should be handled, whether an observation at a non-gaming outlet belongs to anyone in particular, and what documentation a compliance reviewer will need. [Insert a brief description of the author's specific roles, departments, and responsibilities in casino resort operations, and the period of that experience.] This experience was used to identify recording points and handoffs to examine in the documents, not as a source of data.

3. RESULTS AND DISCUSSION

This section presents the framework that results from the workflow mapping and synthesis, and then discusses its interpretation, implications, limitations, and directions for future research.

Six principles, derived from the regulatory requirements and literature above, govern the framework.

1. **Record once, use twice.** Frontline records should be designed to serve both financial accuracy and compliance monitoring, so that the same entry supports reconciliation and aggregation without re-keying.
2. **Route facts, not conclusions.** Frontline and finance personnel report observed facts and exceptions. They do not decide whether activity is suspicious, and they are not asked to.
3. **Default to referral when in doubt.** An exception that is not fully explained by a documented recording, timing, or system cause, or that carries any listed risk indicator, is referred to compliance.
4. **Dual tracks are allowed.** An exception can be corrected as an accounting matter and referred as a compliance matter at the same time. Correction does not close the compliance question.
5. **Every handoff has an owner, a clock, and an evidence standard.** No transfer between functions is informal.
6. **Close the loop.** Exception trends and compliance outcomes, at an aggregate level that respects SAR confidentiality, feed back into risk assessment, training, and control redesign.

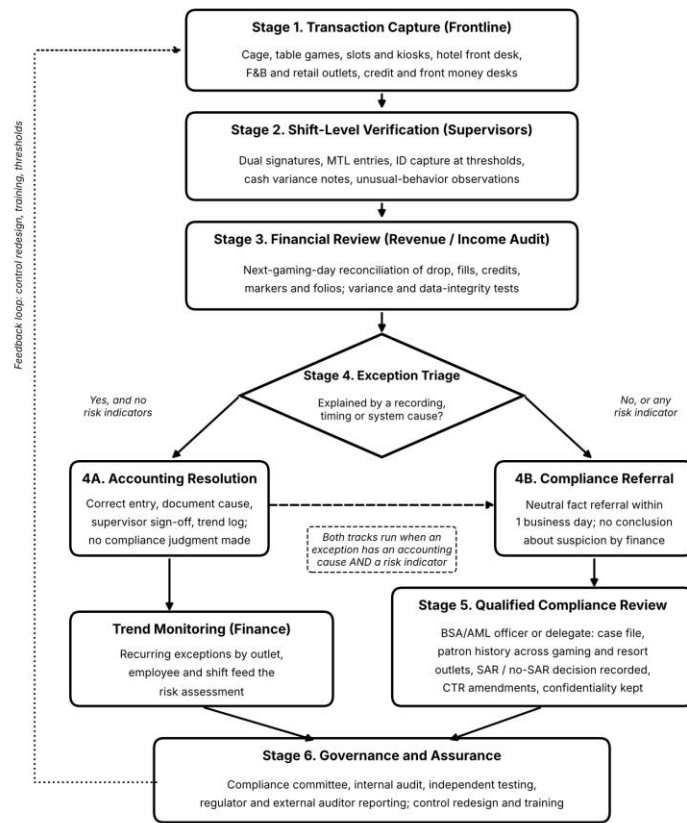


Figure 1. Integrated Financial Control and Risk Escalation Framework for casino resorts

Figure 1 presents the framework. It consists of six stages, with a branch at the fourth stage into an accounting resolution track and a compliance referral track.

Stage 1: Transaction capture. Frontline employees at the cage, gaming tables, slot and kiosk operations, credit and front money desks, hotel front desk, and food, beverage, and retail outlets create the original record. In the framework, capture includes the transaction details required by the MICS together with the patron identifiers and MTL entries required to support BSA aggregation. For non-gaming outlets, capture includes the folio or ticket link to a known patron account where one exists.

Stage 2: Shift-level verification. Supervisors verify records before the close of the shift: dual signatures, form sequence, cash counts, and MTL completeness. Supervisors also record any behavioral observations reported by frontline staff, such as a patron declining to provide

identification or reducing a transaction amount after a threshold is mentioned. These observations are recorded as facts, without characterization.

Stage 3: Financial review. Revenue or income audit reconciles the gaming day's activity on the next business day, comparing drop, fills, credits, markers, front money, folios, and system reports. This stage produces exceptions: variances, missing signatures, out-of-sequence forms, unmatched transfers, and data-integrity failures. Revenue audit is also well placed to notice items that are financially minor but behaviorally unusual, such as repeated small corrections tied to the same patron account.

Stage 4: Exception triage. Each exception is classified using the classification rule set out below. An exception that is fully explained by a documented recording, timing, or system cause and carries no risk indicator follows Track 4A, accounting resolution. Any other exception follows Track 4B, compliance referral. An exception with both an accounting cause and a risk indicator follows both tracks.

Stage 5: Qualified compliance review. The BSA/AML compliance officer or a trained delegate opens a case, gathers patron history across gaming and resort systems, consults surveillance and other departments as needed, and decides whether a SAR is warranted. The decision, whether to file or not to file, is documented with its basis. CTR amendments or late filings identified through the review are handled here. SAR confidentiality is maintained, so the referring department is informed only that the referral has been received and closed, not of the outcome.

Stage 6: Governance and assurance. A compliance committee, internal audit, independent BSA testing, and external audit review the operation of the process. Aggregate information on exception volumes, referral timeliness, and recurring control failures is reported, and the results drive control redesign, threshold calibration, and training, consistent with risk-based auditing and corrective action planning (Akomolafe et al., 2023a; Ebhojie et al., 2023a). This stage closes the feedback loop to Stage 1.

The core of the framework is a classification rule that keeps two different kinds of question with the people competent to answer them. An **accounting exception** is a discrepancy between records, or between a record and a standard, that is fully explained by a documented recording, timing, or

system cause and that has no attached risk indicator. A **compliance concern** is any exception that is not fully explained, or any observation, with or without a financial discrepancy, that matches a risk indicator listed in the casino's AML program. The rule is deliberately asymmetric: the burden is on explaining an exception fully before it can stay on the accounting track alone. Table 1 illustrates how the rule applies.

Table 1. Illustrative classification of exceptions

Observed exception	Typical accounting cause	Risk indicators that trigger referral	Track
Cage window short or over at shift end	Miscount, payout error, unrecorded paid-out	Shortage linked to an unrecorded large patron transaction; repeated variances tied to one employee or patron	4A, or both if indicator present
MTL entry missing for a recorded cash transaction	Busy window, entry posted to wrong log	Missing entries cluster around one patron or near reporting thresholds; aggregation now exceeds CTR threshold	Both (CTR review and referral)
Patron changes transaction amount after ID request	None	Possible structuring or avoidance of identification	4B
Chip purchase with little or no play, then redemption by check or wire	None	Minimal-play conversion of funds	4B
Hotel folio settled in large currency amount	Normal guest payment	Amount inconsistent with stay; split payments; third-party payer; patron also active at cage	4A, or 4B if indicator present
Front money deposit from third party	Documentation incomplete	Source of funds unclear; payer not the patron	4B
Marker or credit reversal outside normal cycle	Posting correction	Reversal follows unusual repayment source or method	4A, or both
System interface mismatch between slot, kiosk, and cage systems	Interface or timing lag	Mismatch conceals or alters patron-level totals used for aggregation	4A, or both

Note. Examples are illustrative and draw on indicators described in FinCEN guidance and industry and international typologies (American Gaming Association, 2022; Financial Action Task Force & Asia/Pacific Group on Money Laundering, 2009; Financial Crimes Enforcement Network, 2012b). Each casino's AML program should define its own indicator list based on its risk assessment.

Two further rules protect the separation. First, a finance reviewer who refers an item does not describe it as suspicious or speculate about motive. The referral form records facts, sources, and the reason the item could not be fully explained or the indicator that applies. Second, closing an accounting exception never closes a related compliance referral. The compliance reviewer decides when the compliance question is resolved.

Table 2 assigns responsibilities across the stages using a simplified accountability model. The assignments follow the Three Lines logic: frontline operations and their supervisors own the accuracy of records and the first report of anomalies; finance owns reconciliation and routing; compliance owns the judgment about suspicion and reporting; internal audit and independent testers provide assurance.

Table 2. Review responsibilities by stage

Stage	Responsible (does the work)	Accountable (owns the outcome)	Consulted	Informed
1. Transaction capture	Cashiers, dealers, slot and hotel staff, outlet staff	Department managers	Supervisors	Revenue audit
2. Shift-level verification	Shift supervisors	Department managers	Surveillance (as needed)	Revenue audit; compliance for observations
3. Financial review	Revenue / income audit	Director of finance or controller	Department managers; IT	Compliance (exception log)
4. Exception triage	Revenue audit lead	Controller	Compliance (for unclear cases)	Department managers
4A. Accounting resolution	Revenue audit; department	Controller	Department managers	Internal audit (trends)
4B. Compliance referral	Referring reviewer	Controller (timeliness)	None required	Compliance officer
5. Compliance review	Compliance analysts	BSA/AML compliance officer	Surveillance, cage, credit, hotel	Compliance committee (aggregate)
6. Governance and assurance	Internal audit; independent tester	Compliance committee / audit committee	Finance and compliance leadership	Board; regulators as required

Escalation is defined as the movement of an item to a function with greater authority or expertise. Table 3 sets out the escalation levels and proposed time standards. The time standards are design targets for testing, not regulatory requirements. They are chosen to protect the 30-day SAR period by keeping internal transfer times short relative to the time needed for investigation.

Table 3. Escalation levels and proposed time standards

Level	Trigger	From / To	Proposed time standard
E1. Supervisor notice	Frontline observation of unusual behavior or a threshold-related event	Frontline staff to shift supervisor	Same shift

E2. Finance exception	Variance or record defect found at reconciliation	Revenue audit to controller's exception log	Next business day after the gaming day
E3. Compliance referral	Exception not fully explained, or risk indicator present	Revenue audit or supervisor to compliance	Within one business day of classification
E4. Compliance case	Referral accepted for investigation	Compliance analyst to compliance officer	Decision documented within the SAR filing period
E5. Governance escalation	Repeated control failures, overdue cases, or significant reportable matters	Compliance officer or controller to compliance committee	At next scheduled meeting, or immediately if material

A direct path from frontline staff to compliance should also exist, so that employees can report concerns without going through a supervisor when that is more appropriate. This path complements, and does not replace, the routine flow through Stages 2 to 4.

Each handoff carries an evidence standard. The purpose is to make every stage auditable and to ensure that compliance reviewers receive what they need to make a defensible decision. Records should be complete, retrievable, and protected from alteration, which is the core of audit readiness (Anichukwueze et al., 2021). Table 4 summarizes the minimum evidence at each stage.

Table 4. Minimum evidence requirements by stage

Stage	Minimum evidence	Retention and access
1. Capture	Original transaction record; patron identifier where required; MTL entry; employee and location identifiers; time stamp	Per MICS and BSA retention (generally five years); finance and compliance read access
2. Verification	Supervisor sign-off; count sheets; variance notes; factual record of behavioral observations	Attached to shift package
3. Financial review	Reconciliation workpapers; system reports; exception list with reference to source records	Revenue audit files
4. Triage	Classification decision; documented cause for 4A items; indicator or reason for 4B items; reviewer and date	Exception log, accessible to internal audit
4A. Resolution	Correcting entry; approval; root cause; trend code	Finance files; trend data reported quarterly
4B. Referral	Referral form with facts, source documents, patron identifiers, related transactions across outlets; no conclusion about suspicion	Compliance case system; restricted access
5. Compliance review	Case file; patron history; surveillance and departmental inputs; SAR or no-SAR decision and rationale; filing records; CTR amendments	Restricted; SAR confidentiality maintained
6. Assurance	Committee minutes; key metrics; audit and independent testing reports; corrective action tracking	Governance records

The following hypothetical scenarios show how the framework would operate. They are constructed for illustration and do not describe actual events.

Scenario A: an accounting exception that remains accounting. A table games fill slip is recorded with a transposed amount. Revenue audit identifies the mismatch with the cage record, the supervisor confirms the transposition, and the correcting entry is approved. There is no patron involvement and no indicator. The item follows Track 4A and is coded for trend monitoring.

Scenario B: an exception that runs on both tracks. Revenue audit finds that a cage window was \$3,000 short at shift end and that an MTL entry for a patron's \$4,000 cash chip purchase is missing. The cashier explains that the patron completed two purchases and that the second was not logged. The shortage is resolved as a recording error on Track 4A. Because the reconstructed patron total for the gaming day now exceeds \$10,000 in cash in, and the patron's two purchases occurred minutes apart at different windows, the item is also referred on Track 4B. Compliance reviews whether a CTR is required, files it if so, and assesses separately whether the pattern warrants a SAR.

Scenario C: a concern with no financial discrepancy. A hotel front desk agent notes that a guest settled a large folio in currency, split across several payments, while the same guest had redeemed chips at the cage the previous evening with little recorded play. The hotel records reconcile perfectly, so there is no accounting exception. Under the framework, the supervisor records the observation at Stage 2 and refers it to compliance under E3, because a risk indicator is present. Without a defined path from non-gaming outlets, this observation would likely never reach a compliance reviewer.

The framework answers the research question in four parts. First, frontline transaction records should be designed from the outset to serve both financial control and compliance monitoring, which means that patron identifiers, MTL entries, and cross-outlet links are part of the record rather than an afterthought. Second, financial review should act as the systematic filter that converts records into exceptions and routes them, without taking on the judgment about suspicion. Third, compliance escalation should be triggered by a defined, asymmetric rule that sends unexplained exceptions and any indicator-bearing observation to qualified reviewers, and it should allow dual-track handling so that accounting correction never closes a compliance question.

Fourth, every handoff should have an owner, a time standard, and an evidence requirement, with governance and assurance closing the loop.

For casino resort finance leaders, the framework suggests that the exception log is a compliance asset as well as an accounting tool, and that the controller is accountable for the timeliness of referrals even though compliance owns their outcome. For compliance officers, it suggests that referral quality depends on investment in finance-side training designed to change behavior (Anichukwueze et al., 2020) and in data links between gaming and non-gaming systems. Analytics such as anomaly detection and risk scoring can help prioritize review queues (Atakpa & Fobellah, 2023; Fadayomi et al., 2024), provided that their alerts are routed into the same triage rule. For internal audit, it offers testable control points: classification accuracy, referral timeliness, completeness of evidence, and the proportion of compliance cases that originate in finance review. For regulators and independent testers, it provides a vocabulary for assessing whether the AML program's internal controls actually draw on the information the casino already holds.

Documented workflows describe intended practice and may differ from actual practice. Enforcement records are a biased sample of failures. Requirements differ by jurisdiction, and the framework uses the U.S. federal, Nevada, and NIGC regimes as reference points rather than a comprehensive survey. Many of the adjacent-sector sources are conceptual frameworks or reviews rather than empirical tests, so they are used for design ideas rather than as evidence of effectiveness. Finally, the framework is normative: it describes how the interaction should be designed, not how it is currently organized across the industry.

The framework also assumes a property with distinct finance, compliance, and internal audit functions. Smaller properties may combine roles, and in such cases the separation between routing facts and deciding suspicion may need to be preserved through procedure rather than structure. The framework also assumes that data from gaming and non-gaming systems can be joined at the patron level, which may not hold where systems are legacy or outsourced. Finally, the time standards in Table 3 are proposed for testing and may need calibration to transaction volumes and staffing.

Because the framework is conceptual, its value depends on whether its claims hold in practice. Table 5 converts the framework into propositions and research questions, with suggested methods and data sources for future study.

Table 5. Propositions and research questions

Proposition	Research question	Suggested method and data
P1. Properties with a written rule separating accounting exceptions from compliance concerns will have a higher share of compliance cases originating from finance review.	RQ1. How do casino resorts currently classify exceptions found during revenue audit, and is the rule written?	Document review of written systems of internal control and AML procedures; practitioner interviews (contingent on access)
P2. Dual-track handling reduces the number of compliance-relevant items closed as clerical corrections.	RQ2. How often do exceptions corrected on the accounting track carry indicators that are not referred?	Retrospective review of exception logs by internal audit; sample testing
P3. Shorter internal referral times are associated with more complete compliance case files and fewer late filings.	RQ3. What is the distribution of time from gaming day to compliance referral, and how does it relate to case outcomes?	Analysis of referral time stamps and independent testing findings
P4. Properties that link non-gaming outlet records to patron accounts identify more cross-channel risk indicators.	RQ4. To what extent do hotel, food and beverage, and retail records reach compliance review?	System mapping; case studies at integrated resorts
P5. Training finance staff to route facts rather than conclusions increases referral volume without reducing referral quality.	RQ5. How do finance staff understand their role in AML monitoring, and what beliefs inhibit referral?	Survey and interviews informed by voice and silence research
P6. Feedback from compliance to finance on aggregate trends improves classification accuracy over time.	RQ6. What feedback mechanisms exist, and how are they constrained by SAR confidentiality?	Governance document review; longitudinal comparison

These questions can be pursued in sequence. RQ1 and RQ4 are descriptive and can begin with document analysis. RQ2 and RQ3 require access to internal records and are best conducted with or by internal audit. RQ5 and RQ6 require practitioner engagement. Any empirical work must avoid collecting SARs or information that would reveal whether a SAR was filed, and should be designed with legal review.

4. CONCLUSION

Casino resorts already create most of the information needed to detect both accounting errors and financial crime risk. The weakness is often in how that information moves. This paper has proposed an integrated framework that treats frontline records as dual-purpose, positions financial

review as a systematic filter and router, reserves judgments about suspicion for qualified compliance reviewers, and gives every handoff an owner, a time standard, and an evidence requirement. The framework's central rule, that finance routes facts and compliance decides suspicion, is simple to state but depends on careful design of records, classification criteria, and feedback. The propositions offered here are intended to move the discussion from principle to evidence.

The work forms part of a broader agenda on strengthening financial integrity in hospitality and gaming organizations. Its next steps are to test the propositions set out in Table 5, beginning with document analysis and, where access permits, practitioner consultation, and then to translate the findings into practical tools such as exception classification guides, referral templates, training modules for finance staff, and audit programs for testing the interface. The integrity of casino financial records matters beyond individual properties because it supports accurate tax collection, effective AML reporting to the authorities, and public confidence in a regulated industry.

REFERENCES

1. Abetoh, N. F., & Atakpa, M. I. (2024). Audit analytics in healthcare financial oversight: Leveraging data science to strengthen accountability in multilateral grant ecosystems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(6), 2710-2747. <https://doi.org/10.32628/CSEIT2410791>
2. Adelanwa, A., Basnet, A., & Anene, U. N. (2023). Predictive analytics models for financial risk detection and fraud prevention in public systems. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6). <https://doi.org/10.62225/2583049X.2023.3.6.5969>
3. Adesuyi, M. O., Akomolafe, O., Olaogun, B. O., Ndukwe, V. U., & Sakyi, J. K. (2024). AI-driven risk scoring model for global cross-border trade payment transactions. *International Journal of Advanced Multidisciplinary Research and Studies*, 4(1), 1569-1581. <https://doi.org/10.62225/2583049X.2024.4.1.5281>
4. Adesuyi, M. O., Kalu, A., & Walawalkar, G. (2023). Data-led cost governance in technology-intensive enterprises. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(3), 877-896. <https://doi.org/10.32628/IJSRCSEIT>

5. Adeyelu, O. O. (2018). A predictive compliance monitoring framework for detecting systemic safety risks through aviation consumer complaint data. *Iconic Research and Engineering Journals*, 1(8), 250-276. <https://doi.org/10.64388/IREV1I8-1718478>
6. Adeyelu, O. O. (2021). A framework for managing encroachments and unauthorized structures around airport boundaries: Regulatory evidence, enforcement, and corrective action protocols for Nigerian civil aviation. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), 954-972. <https://doi.org/10.54660/IJMRGE.2021.2.6.954-972>
7. Adeyelu, O. O., & Dagodzo, D. (2024). A maturity model for predicting airport safety audit outcomes in resource-constrained regulatory environments. *International Journal of Scientific Research in Civil Engineering*, 8(4), 132-170. <https://doi.org/10.32628/IJSRCE248423>
8. Agboada, P., Ezeako, R., Okoli, I. E., & Uzundu, C. S. (2019). Standard operating procedures as change infrastructure: A conceptual framework for sustaining operational improvement. *Iconic Research and Engineering Journals*, 3(6), 706-730. <https://doi.org/10.64388/IREV3I6-1723313>
9. Agu, M. U., Akomolafe, O., & Bello, A. (2023). A comparative review of SOX compliance frameworks in cross-border financial auditing. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2297-2306. <https://doi.org/10.62225/2583049X.2023.3.6.5362>
10. Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual model for insider threat classification and risk modeling in complex digital systems. *Iconic Research and Engineering Journals*, 1(9), 476-492. <https://doi.org/10.64388/IREV1I9-1713778>
11. Akhigbe, R., Falemi, A., & Akin-Oluyomi, O. T. (2023). A conceptual model for improving customer experience using workforce behavior and real-time operational data. *International Journal of Multidisciplinary Research and Growth Evaluation*, 4(6), 1322-1338. <https://doi.org/10.54660/ijmrge.2023.4.6.1322-1338>
12. Akin-Oluyomi, O. T., & Akhigbe, R. (2023). An advanced framework for improving multi-site operational efficiency using data-driven performance indicators. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), 1763-1781. <https://doi.org/10.62225/2583049X.2023.3.1.5343>

13. Akomolafe, O., & Agu, M. U. (2018). A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. *Iconic Research and Engineering Journals*, 1(9), 458-475.
14. Akomolafe, O., & Agu, M. U. (2019a). A conceptual framework for developing risk-based internal control models in the insurance and banking sectors. *Iconic Research and Engineering Journals*, 2(8), 335-354.
15. Akomolafe, O., & Agu, M. U. (2019b). A review of data-driven risk evaluation models for emerging market financial institutions. *Iconic Research and Engineering Journals*, 3(6), 433-448.
16. Akomolafe, O., & Agu, M. U. (2019c). Advances in financial resilience through integrated governance and compliance strategies. *Iconic Research and Engineering Journals*, 2(10), 607-620.
17. Akomolafe, O., Agu, M. U., & Bello, A. (2023a). A conceptual model for implementing risk-based auditing in strategic financial management. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2274-2286. <https://doi.org/10.62225/2583049X.2023.3.6.5359>
18. Akomolafe, O., Agu, M. U., & Bello, A. (2023b). A quantitative conceptual model for assessing compliance risk in emerging economies. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2287-2296. <https://doi.org/10.62225/2583049X.2023.3.6.5360>
19. Alieme, J. I., Sule, A., & Obukadata, V. O. (2022). Standardization of reporting and decision workflows: A framework for improving efficiency, data quality, and management visibility. *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), 1190-1218. <https://doi.org/10.54660/IJMRGE.2022.3.6.1190-1218>
20. Alieme, J. I., Sule, A., & Obukadata, V. O. (2024). From ambiguity to AI-ready requirements: A business analysis framework for structuring business problems for intelligent process automation. *International Journal of Multidisciplinary Research and Growth Evaluation*, 5(6), 2088-2117. <https://doi.org/10.54660/IJMRGE.2024.5.6.2088-2117>
21. Aliliele, C., Eboh, E. E., & Oluwo, K. (2024). Advances in variance analytics for cost control in manufacturing and industrial enterprises. *International Journal of Advanced*

Multidisciplinary Research and Studies, 4(6), 3163-3185.
<https://doi.org/10.62225/2583049X.2024.4.6.6012>

22. Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2023). A review of API governance and risk prioritization frameworks in modern financial institutions. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(10), 395-433. <https://doi.org/10.32628/CSEIT2361072>
23. Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2024). A conceptual framework for enterprise data sensitivity classification and regulatory traceability mechanisms. *International Journal of Advanced Multidisciplinary Research and Studies*, 4(6), 3103-3124. <https://doi.org/10.62225/2583049X.2024.4.6.5991>
24. Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. *Journal of Information Systems*, 22(2), 195-214. <https://doi.org/10.2308/jis.2008.22.2.195>
25. American Gaming Association. (2022). *Best practices for anti-money laundering compliance* (3rd ed.). American Gaming Association.
26. Amicelle, A., & Iafolla, V. (2018). Suspicion-in-the-making: Surveillance and denunciation in financial policing. *The British Journal of Criminology*, 58(4), 845-863. <https://doi.org/10.1093/bjc/azx051>
27. Aneke, O. B., & Adesemoye, A. C. (2020). A conceptual framework for risk-based decision-making in good manufacturing practice environments. *Iconic Research and Engineering Journals*, 4(6), 325-341.
28. Aneke, O. B., & Adesemoye, A. C. (2021). Reframing trade and import compliance: A conceptual model for risk-based interdiction of illicit medical products. *International Journal of Scientific Research in Science and Technology*, 8(6), 1226-1248.
29. Aneke, O. B., Sydney, E., & Adesemoye, A. C. (2023). Data integrity and governance in regulated life sciences operations: A review of failures, controls, and remediation strategies. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(10), 538-568.
30. Anichukwueze, C. C., Ominyi, M., Uzougbo, N. S., & Jones, B. C. (2022). Cross-functional legal education as risk mitigation: Empirical analysis of contract error reduction in engineering teams. *International Journal of Engineering and Modern Technology*, 8(5), 142-180. <https://doi.org/10.56201/ijemt.v8.no5.2022.pg142.180>

31. Anichukwueze, C. C., Osuji, V. C., & Oguntegbe, E. E. (2019). Global marketing law and consumer protection challenges: A strategic framework for multinational compliance. *IRE Journals*, 3(6), 325-333.
32. Anichukwueze, C. C., Osuji, V. C., & Oguntegbe, E. E. (2020). Designing ethics and compliance training frameworks to drive measurable cultural and behavioral change. *International Journal of Multidisciplinary Research and Growth Evaluation*, 1(3), 205-220.
33. Anichukwueze, C. C., Osuji, V. C., & Oguntegbe, E. E. (2021). Blockchain-based architectures for tamper-proof regulatory recordkeeping and real-time audit readiness. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), 485-504.
34. Anioke, S. C., & Atima, M. E. (2023). Public health governance models using process optimization and performance metrics for regulatory oversight. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2534-2548. <https://doi.org/10.62225/2583049X.2023.3.6.5491>
35. Annaraud, K., Singh, D., & Lively, H. (2014). Assessing and analyzing internal control practices in the lodging industry. *Journal of Hospitality Financial Management*, 22(1), 26-31. <https://doi.org/10.1080/10913211.2014.909251>
36. Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory*, 36(4), 1-27. <https://doi.org/10.2308/ajpt-51684>
37. Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, 35(7), 659-675. <https://doi.org/10.1016/j.aos.2010.07.003>
38. Ashbaugh-Skaife, H., Collins, D. W., Kinney, W. R., & LaFond, R. (2008). The effect of SOX internal control deficiencies and their remediation on accrual quality. *The Accounting Review*, 83(1), 217-250. <https://doi.org/10.2308/accr.2008.83.1.217>
39. Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. Association of Certified Fraud Examiners.
40. Atakpa, M. I. (2021). A review of predictive analytics models for anti-money laundering detection in commercial banking systems. *International Journal of Scientific Research in*

Computer Science, Engineering and Information Technology, 7(2), 778-804.
<https://doi.org/10.32628/CSEIT2064813>

41. Atakpa, M. I., & Abetoh, N. F. (2022). A systematic review of machine learning advances in financial fraud detection for banking systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 8(2), 771-801. <https://doi.org/10.32628/CSEIT23906220>
42. Atakpa, M. I., & Abolaji, T. O. (2022). A privacy-preserving data architecture model for regulated industry analytics under GDPR and HIPAA compliance. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 8(3), 781-808. <https://doi.org/10.32628/CSEIT22558>
43. Atakpa, M. I., & Fobellah, A. N. (2023). Anomaly detection in financial time-series data: A conceptual model for healthcare and banking applications. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(2), 967-997. <https://doi.org/10.32628/CSEIT2342441>
44. Atakpa, M. I., Abetoh, N. F., & Akeju, B. (2024). Advances in artificial intelligence for healthcare payment fraud detection: A review of NHS applications. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(4), 1161-1194. <https://doi.org/10.32628/CSEIT26123240>
45. Australian Transaction Reports and Analysis Centre. (2020). *Money laundering and terrorism financing risk assessment: Junket tour operations in Australia*.
46. Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2019). A conceptual model for ETL design and data integration in Salesforce-centric enterprise architectures. *Iconic Research and Engineering Journals*, 3(5).
47. Badmus, O., Jooda, D., & Anunagba, C. O. (2024). A privacy-by-design framework for role-based security architecture in Salesforce environments handling sensitive personal data. *International Journal of Advanced Multidisciplinary Research and Studies*, 4(6), 3244-3254. <https://doi.org/10.62225/2583049X.2024.4.6.6243>
48. Badmus, O., Jooda, D., Ozowara, D. E., & Anunagba, C. O. (2022). A systematic review of MuleSoft ESB integration patterns in multi-cloud Salesforce architectures. *Gyanshauryam, International Scientific Refereed Research Journal*, 5(3), 462-481.
49. Bardi, J. A. (2010). *Hotel front office management* (5th ed.). John Wiley & Sons.

50. Bell, A. (2022). *Review of The Star Pty Ltd: Inquiry under sections 143 and 143A of the Casino Control Act 1992 (NSW)*. New South Wales Independent Casino Commission.
51. Bello, A. D., Elebe, O., Hammed, N. I., Omoegun, G. O., & Fadayomi, O. (2024). A cybersecurity risk management and regulatory compliance framework for financial institutions. *Iconic Research and Engineering Journals*. <https://www.irejournals.com/paper-details/1713553>
52. Bello, A., Akomolafe, O., & Agu, M. U. (2023). A conceptual framework for data-driven procurement risk management in multinational enterprises. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2307-2316. <https://doi.org/10.62225/2583049X.2023.3.6.5363>
53. Bergin, P. A. (2021). *Report of the inquiry under section 143 of the Casino Control Act 1992 (NSW)*. Independent Liquor and Gaming Authority, New South Wales.
54. Bola-Sadipe, D., Aliliele, C., & Eboh, E. E. (2019). Conceptual model for strategic accounting systems strengthening financial transparency and regulatory compliance. *IRE Journals*, 3(6), 535-564. <https://doi.org/10.64388/IREV3I6-1715327>
55. Bola-Sadipe, D., Aliliele, C., & Odihi, F. (2023). Conceptual model for automated financial consolidation and transparency in multinational corporations. *Gyanshauryam, International Scientific Refereed Research Journal*, 6(6), 414-455. <https://doi.org/10.32628/GISRRJ236645>
56. Bola-Sadipe, D., Eboh, E. E., & Odihi, F. (2022). Advances in data-driven tax compliance and financial reporting systems in banking institutions. *Shodhshauryam, International Scientific Refereed Research Journal*, 5(1), 366-403. <https://doi.org/10.32628/SHISRRJ247137>
57. Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27-40. <https://doi.org/10.3316/QRJ0902027>
58. Buchanan, J. (2018). Money laundering through gambling devices. *Society and Business Review*, 13(2), 217-237. <https://doi.org/10.1108/SBR-08-2017-0057>
59. Cabot, A. N., & Pindell, N. (Eds.). (2014). *Regulating land-based casinos: Policies, procedures, and economics*. UNLV Gaming Press.

60. Chaikin, D. (2009). How effective are suspicious transaction reporting systems? *Journal of Money Laundering Control*, 12(3), 238-253. <https://doi.org/10.1108/13685200910973628>
61. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), Article 15. <https://doi.org/10.1145/1541880.1541882>
62. Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control: Integrated framework*. COSO.
63. Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance* (Executive summary). https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf
64. Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.
65. Cullen, A. F. (2022). *Commission of Inquiry into Money Laundering in British Columbia: Final report*. Commission of Inquiry into Money Laundering in British Columbia.
66. Dalla Pellegrina, L., & Masciandaro, D. (2009). The risk-based approach in the new European anti-money laundering legislation: A law and economics view. *Review of Law & Economics*, 5(2), 931-952. <https://doi.org/10.2202/1555-5879.1422>
67. Davies, H., & Zhivitskaya, M. (2018). Three lines of defence: A robust organising framework, or just lines in the sand? *Global Policy*, 9(S1), 34-42. <https://doi.org/10.1111/1758-5899.12568>
68. DeFranco, A. L., & Wortman, J. F. (1997). Internal control practices in casino gaming. *Journal of Hospitality Financial Management*, 5(1), 34-48.
69. Detert, J. R., & Burris, E. R. (2007). Leadership behavior and employee voice: Is the door really open? *Academy of Management Journal*, 50(4), 869-884.
70. Detert, J. R., & Edmondson, A. C. (2011). Implicit voice theories: Taken-for-granted rules of self-censorship at work. *Academy of Management Journal*, 54(3), 461-488.
71. Dogbatsey, E. A., & Ebhojie, O. (2018). *Budget compliance and statutory reporting in Sub-Saharan Africa: A systematic review of frameworks, gaps, and reform pathways*. Zenodo. <https://doi.org/10.5281/zenodo.20446859>

72. Dogbatsey, E. A., Ebhojie, O., & Oyeleye, A. O. (2019). *Reconciliation control and financial workflow redesign in emerging market organizations: A conceptual framework*. Zenodo. <https://doi.org/10.5281/zenodo.20447103>
73. Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. *Iconic Research and Engineering Journals*, 3(5), 434-447. <https://doi.org/10.64388/IREV315-1713225>
74. Dosunmu, A. A., & Ogundele, P. O. (2021). Incident response and digital forensics strategies for rapid cyber attack containment. *Gyanshauryam, International Scientific Refereed Research Journal*, 4(4), 239-258.
75. Doyle, J., Ge, W., & McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics*, 44(1-2), 193-223. <https://doi.org/10.1016/j.jacceco.2006.10.003>
76. Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2018). *Fundamentals of business process management* (2nd ed.). Springer. <https://doi.org/10.1007/978-3-662-56509-4>
77. Dyck, A., Morse, A., & Zingales, L. (2010). Who blows the whistle on corporate fraud? *The Journal of Finance*, 65(6), 2213-2253.
78. Ebhojie, O., Dogbatsey, E. A., & Oyeleye, A. O. (2023a). Audit liaison, corrective action planning, and control compliance in multinational organisations: A systematic literature review. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2839-2850. <https://doi.org/10.62225/2583049X.2023.3.6.6200>
79. Ebhojie, O., Dogbatsey, E. A., & Oyeleye, A. O. (2023b). Simulation-based tools in graduate accounting education: A conceptual framework for bridging variance analysis theory and practice. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2851-2862. <https://doi.org/10.62225/2583049X.2023.3.6.6201>
80. Eboh, E. E., & Aliliele, C. (2023). Portfolio risk optimization models for venture capital investment strategy and fraud exposure analysis. *Iconic Research and Engineering Journals*, 7(4), 759-792. <https://doi.org/10.64388/IREV714-1715305>
81. Eboh, E. E., & Aliliele, C. (2024). AI-driven data analytics framework for risk assessment and detection of venture capital and private equity investment fraud in U.S. capital markets. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(6), 2624-2665. <https://doi.org/10.32628/CSEIT2410787>

82. Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly*, 44(2), 350-383. <https://doi.org/10.2307/2666999>
83. Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532-550.
84. Ekechi, N. V., Anunagba, C. O., & Ozowara, D. E. (2022). Advances in financial forensics techniques for detecting cyber-enabled fraud in telemedicine services. *Shodhshauryam, International Scientific Refereed Research Journal*, 5(1), 428-450.
85. Elebe, O., Hammed, N. I., Omoegun, G. O., Fadayomi, O., & Bello, A. D. (2023). *An advanced machine learning model for detecting synthetic identity fraud in e-commerce platforms* [Preprint]. ResearchGate.
86. Eyetsemitan, R. A., Ambali, K. B., Oyeleye, A. O., & Fadayomi, O. (2021). Translating tax and regulatory requirements into SME compliance workflows: A conceptual framework for implementing IAS 12, VAT, PAYE, and withholding tax. *Iconic Research and Engineering Journals*, 4(11), 621-641. <https://doi.org/10.64388/IREV4I11-1716956>
87. Eyetsemitan, R. A., Oyeleye, A. O., Ambali, K. B., & Fadayomi, O. (2022). Standard operating procedures as strategic assets in small business operations: A systematic review and implementation framework. *Gyanshauryam, International Scientific Refereed Research Journal*, 5(2), 438-465. <https://doi.org/10.32628/GISRRJ225356>
88. Ezeako, R., Ibeh, A. V., Alugwe, S., & Awulu, I. (2024). Performance dashboards and data-driven decision-making in operations management: A conceptual framework for leadership visibility. *International Journal of Advanced Multidisciplinary Research and Studies*, 4(6), 3520-3538. <https://doi.org/10.62225/2583049X.2024.4.6.6930>
89. Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O. (2021). *An integrated cybersecurity and anti-money laundering governance framework for financial crime prevention* [Preprint]. ResearchGate.
90. Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O. (2024). An adaptive fraud risk scoring model for real-time transaction monitoring at scale. *IIARD International Journal of Banking and Finance Research*, 10(10), 212-230.
91. Falemi, A., Akhigbe, R., & Akin-Oluyomi, O. T. (2023). A proposed framework for integrating employee retention systems with operational productivity metrics. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), 1704-1724. <https://doi.org/10.62225/2583049X.2023.3.1.5339>

92. Falemi, A., Akhigbe, R., & Akin-Oluyomi, O. T. (2024). A conceptual enterprise risk management model that integrates HR strategy with operational analytics. *International Journal of Multidisciplinary Research and Growth Evaluation*, 5(6), 1730-1753. <https://doi.org/10.54660/ijmrge.2024.5.6.1730-1753>
93. Ferentzy, P., & Turner, N. (2009). Gambling and organized crime: A review of the literature. *Journal of Gambling Issues*, 23, 111-155.
94. Financial Action Task Force & Asia/Pacific Group on Money Laundering. (2009). *Vulnerabilities of casinos and gaming sector*. FATF/OECD and APG.
95. Financial Action Task Force. (2008). *RBA guidance for casinos*. FATF/OECD.
96. Financial Crimes Enforcement Network. (2012a). *Frequently asked questions: Casino recordkeeping, reporting, and compliance program requirements* (FIN-2012-G004).
97. Financial Crimes Enforcement Network. (2012b). *Suspicious activity reporting in the gaming industry: Based on filings of suspicious activity reports by casinos and card clubs from January 1, 2004, through June 30, 2011*.
98. Financial Crimes Enforcement Network. (2014). *Advisory to U.S. financial institutions on promoting a culture of compliance* (FIN-2014-A007). U.S. Department of the Treasury.
99. Financial Crimes Enforcement Network. (2015a). *Assessment of civil money penalty: Caesars Palace* (No. 2015-10).
100. Financial Crimes Enforcement Network. (2015b). *In the matter of Trump Taj Mahal Associates, LLC d/b/a Trump Taj Mahal Casino Resort: Assessment of civil money penalty* (No. 2015-02). U.S. Department of the Treasury.
101. Financial Crimes Enforcement Network. (2021). *Anti-money laundering and countering the financing of terrorism national priorities*. U.S. Department of the Treasury. [https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20\(June%2030,%202021\).pdf](https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030,%202021).pdf)
102. Greenlees, E. M. (2008). *Casino accounting and financial management* (2nd ed.). University of Nevada Press.
103. Harvey, J. (2004). Compliance and reporting issues arising for financial institutions from money laundering regulations: A preliminary cost benefit study. *Journal of Money Laundering Control*, 7(4), 333-346. <https://doi.org/10.1108/13685200410810047>

104. Hotel Association of New York City. (2014). *Uniform system of accounts for the lodging industry* (11th rev. ed.). American Hotel & Lodging Educational Institute.
105. Ilodigwe, L., & Adesemoye, A. C. (2021). The data backbone of health system transformation: A governance and architecture framework for interoperability, data quality, and advanced analytics at national scale. *International Journal of Health and Pharmaceutical Research*, 6(2), 52-76. <https://doi.org/10.56201/ijhpr.vol.6.no2.2021.pg52.76>
106. Institute of Internal Auditors. (2020). *The IIA's Three Lines Model: An update of the Three Lines of Defense*. The Institute of Internal Auditors.
107. Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 10(1-2), 18-26.
108. Jans, M., Alles, M. G., & Vasarhelyi, M. A. (2013). The case for process mining in auditing: Sources of value added and areas of application. *International Journal of Accounting Information Systems*, 14(1), 1-20. <https://doi.org/10.1016/j.accinf.2012.06.015>
109. Jones, B. C., & Ominyi, M. (2023). Reviewing compliance frameworks for technology transfers between developed and emerging markets in an era of export controls and sanctions. *World Journal of Innovation and Modern Technology*, 7(2), 121-149. <https://doi.org/10.56201/wjimt.v7.no2.2023.pg121.149>
110. Kassem, R. (2024). Spotlight on fraud risk in hospitality a systematic literature review. *International Journal of Hospitality Management*, 116, Article 103630. <https://doi.org/10.1016/j.ijhm.2023.103630>
111. Kilby, J., Fox, J., & Lucas, A. F. (2005). *Casino operations management* (2nd ed.). John Wiley & Sons.
112. Kish-Gephart, J. J., Detert, J. R., Treviño, L. K., & Edmondson, A. C. (2009). Silenced by fear: The nature, sources, and consequences of fear at work. *Research in Organizational Behavior*, 29, 163-193. <https://doi.org/10.1016/j.riob.2009.07.002>
113. Kleiman, K. E. (2015). Keeping casinos clean: The problem with dirty money and international differences in anti-money laundering regulations for casinos. *UNLV Gaming Law Journal*, 6(1), 81.

114. Kumuyi, O., Akeju, B., Uzoka, E., & Ozowara, D. E. (2023). Framework for blockchain-based cross-border data exchange and regulatory transparency. *International Journal of Multidisciplinary Futuristic Development*, 4(1), 99-113.
115. Kumuyi, O., Uzoka, E., Akeju, B., & Ozowara, D. E. (2024). Framework for privacy-focused digital identity verification supporting financial inclusion in Africa. *International Journal of Advanced Multidisciplinary Research and Studies*, 4(6), 3150-3162. <https://doi.org/10.62225/2583049X.2024.4.6.6005>
116. Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2022). Human-in-the-loop machine learning: A state of the art. *Journal of Frontiers in Multidisciplinary Research*, 3(1), 656-669. <https://doi.org/10.54660/.JFMR.2022.3.1.656-669>
117. Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2023). An IT service management literature review: Challenges, benefits, opportunities, and implementation practices. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 2875-2889. <https://doi.org/10.62225/2583049X.2023.3.6.6205>
118. Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2024). Keeping humans in the loop: Human-centered automated annotation with generative AI. *International Journal of Multidisciplinary Futuristic Development*, 5(1), 81-95. <https://doi.org/10.54660/IJMFD.2024.5.1.81-95>
119. Lam, C. S., & Greenlees, M. (2017). Casino money laundering regulations: Macao and USA. *Journal of Money Laundering Control*, 20(1), 52-69. <https://doi.org/10.1108/JMLC-04-2016-0015>
120. Langdale, J. (2022). Money laundering in Australian casinos. *Journal of Money Laundering Control*, 26(7), 99-109. <https://doi.org/10.1108/JMLC-09-2022-0136>
121. Langdale, J. (2024). Combatting money laundering in Southeast Asian and Australian casinos. In D. Goldbarsht & L. de Koker (Eds.), *Financial crime and the law: Identifying and mitigating risks* (pp. 225-246). Springer. https://doi.org/10.1007/978-3-031-59543-1_9
122. Law, R., Buhalis, D., & Cobanoglu, C. (2014). Progress on information and communication technologies in hospitality and tourism. *International Journal of Contemporary Hospitality Management*, 26(5), 727-750. <https://doi.org/10.1108/IJCHM-08-2013-0367>

123. Lawal, O. A., & Oduleye, T. E. (2018). A review and conceptual framework for tax governance and cross-border compliance analytics. *Iconic Research and Engineering Journals*, 2(5).
124. Lenz, R., & Hahn, U. (2015). A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. *Managerial Auditing Journal*, 30(1), 5-33. <https://doi.org/10.1108/MAJ-08-2014-1072>
125. Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice*, 34, 289-375. <https://doi.org/10.1086/501508>
126. Levi, M., Reuter, P., & Halliday, T. (2018). Can the AML system be evaluated without better data? *Crime, Law and Social Change*, 69(2), 307-328. <https://doi.org/10.1007/s10611-017-9757-4>
127. Lo, T. W., & Kwok, S. I. (2017). Triad organized crime in Macau casinos: Extra-legal governance and entrepreneurship. *British Journal of Criminology*, 57(3), 589-607. <https://doi.org/10.1093/bjc/azw014>
128. MacInnis, D. J. (2011). A framework for conceptual contributions in marketing. *Journal of Marketing*, 75(4), 136-154.
129. Malmi, T., & Brown, D. A. (2008). Management control systems as a package: Opportunities, challenges and research directions. *Management Accounting Research*, 19(4), 287-300. <https://doi.org/10.1016/j.mar.2008.09.003>
130. Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2020). A review of identity and access management integration strategies in hybrid and multi cloud environments. *International Journal of Multidisciplinary Research and Growth Evaluation*, 1(5), 795-810. <https://doi.org/10.54660/IJMRGE.2020.1.5.795-810>
131. Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2021). A conceptual framework for risk based business intelligence architecture in financial technology platforms. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), 731-746. <https://doi.org/10.54660/IJMRGE.2021.2.6.731-746>
132. Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2022). A conceptual framework for AI enabled IT general controls and SOX audit automation processes. *Gyanshauryam, International Scientific Refereed Research Journal*, 5(5), 384-414. <https://doi.org/10.32628/GISRRJ2256239>

133. Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2021). A review of VoIP forensic analytics models for financial fraud detection and regulatory compliance monitoring. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), 711-730. <https://doi.org/10.54660/IJMRGE.2021.2.6.711-730>
134. Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2022). A review of data protection impact assessment models in multi cloud financial infrastructure systems. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 8(1), 589-623. <https://doi.org/10.32628/CSEIT25442>
135. Mbonu, I. S., Iwuanyanwu, U., Uzoka, E., & Oluoha, O. M. (2019). Advances in enterprise log analytics and automated incident response architectures using Python and SIEM platforms. *Iconic Research and Engineering Journals*, 3(2), 1000-1019. <https://doi.org/10.64388/IREV3I2-1714915>
136. Medon, J. J., & Oduleye, T. E. (2022). A comprehensive financial reporting model for strengthening compliance and organizational accountability systems. *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(6), 768-777.
137. Merchant, K. A., & Van der Stede, W. A. (2017). *Management control systems: Performance measurement, evaluation and incentives* (4th ed.). Pearson.
138. Meriç, E. (2021). Using main courante and daily revenue report methods in accounting of daily revenues in touristic accommodation enterprises. IGI Global. <https://www.igi-global.com/chapter/using-main-courante-and-daily-revenue-report-methods-in-accounting-of-daily-revenues-in-touristic-accomodation-enterprises/265930>
139. Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, 20(1), 18-40. <https://doi.org/10.1016/j.mar.2008.10.005>
140. Milliken, F. J., Morrison, E. W., & Hewlin, P. F. (2003). An exploratory study of employee silence: Issues that employees don't communicate upward and why. *Journal of Management Studies*, 40(6), 1453-1476. <https://doi.org/10.1111/1467-6486.00387>
141. Minimum Internal Control Standards for Class II Gaming, 25 C.F.R. pt. 543 (2024).
142. Morrison, E. W. (2014). Employee voice and silence. *Annual Review of Organizational Psychology and Organizational Behavior*, 1, 173-197. <https://doi.org/10.1146/annurev-orgpsych-031413-091328>

143. Morrison, E. W., & Milliken, F. J. (2000). Organizational silence: A barrier to change and development in a pluralistic world. *Academy of Management Review*, 25(4), 706-725.
144. National Indian Gaming Commission. (2012). Minimum internal control standards; Final rule. *Federal Register*, 77(184), 58708.
145. National Indian Gaming Commission. (2013). Minimum internal control standards. *Federal Register*, 78(207), 63873.
146. National Indian Gaming Commission. (2018). Minimum internal control standards. *Federal Register*, 83(245), 65506.
147. Nature of Records and Retention Period, 31 C.F.R. § 1010.430 (2024).
148. Near, J. P., & Miceli, M. P. (1985). Organizational dissidence: The case of whistle-blowing. *Journal of Business Ethics*, 4(1), 1-16. <https://doi.org/10.1007/BF00382668>
149. Nevada Gaming Commission. (2023). *Regulation 6: Accounting regulations* (Regulation 6.090, Internal control for Group I licensees). State of Nevada.
150. Nevada Gaming Control Board. (2022). *Minimum internal control standards: Release of proposed revisions* (Industry Notice No. 2022-94). State of Nevada. <https://gaming.nv.gov/uploadedFiles/gamingnvgov/content/about/industry-notice/2022-94.pdf>
151. Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2020). Advances in internal QHSE audit systems for industrial engineering operations. *Iconic Research and Engineering Journals*, 4(4), 399-417. <https://doi.org/10.64388/IREV4I4-1715499>
152. Ogbole, J. I., Okoruwa, P. O., Babatope, O. M., & Oyewole, T. (2021). Developing an integrated data visualization model for continuous business performance monitoring and optimization. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 7(5), 441-467. <https://doi.org/10.32628/IJSRCSEIT>
153. Okafor, C. M., Farounbi, B. O., Adesanya, O. S., & Akinola, A. S. (2024). Controls for cross-border payments operations: Correspondent banking risk reduction via end-to-end monitoring. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(4), 1050-1071.

154. Okafor, C. M., Osuji, V. C., & Dako, O. F. (2024). Harmonizing risk governance, technology infrastructure, and compliance frameworks for future-ready banking systems. *International Journal of Scientific Research in Humanities and Social Sciences*, 1(1), 316-337.
155. Olagunju, E. O., Edivri, J., & Oteri, O. (2023). A conceptual governance model for change, incident, and problem management in mission-critical enterprise IT environments. Gyanshauryam, *International Scientific Refereed Research Journal*, 6(6). <https://doi.org/10.32628/GISRRJ>
156. Olaogun, B. O., Adesuyi, M. O., Akomolafe, O., Ndukwe, V. U., & Sakyi, J. K. (2023). Regulatory compliance adaptation model for cross-border payment product redesign. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(1), 1651-1662. <https://doi.org/10.62225/2583049X.2023.3.1.5279>
157. Ominyi, M. (2020). Developing a conceptual framework for post-merger compliance integration in multi-jurisdictional banking transaction. *IIARD International Journal of Banking and Finance Research*, 6(3), 78-95. <https://doi.org/10.56201/ijbfr.vol.6.no3.2020.pg78.95>
158. Ominyi, M., & Anichukwueze, C. C. (2020). A review of regulatory clearance frameworks for cross-border mergers and acquisitions in African financial markets. *Journal of Accounting and Financial Management*, 6(4), 73-99. <https://doi.org/10.56201/jafm.vol.6.no4.2020.pg73.99>
159. Ominyi, M., & Anichukwueze, C. C. (2021). A systematic review of anti-money laundering and anti-bribery compliance regimes across emerging and developed markets. *International Journal of Economics and Financial Management*, 6(2), 89-118. <https://doi.org/10.56201/ijefm.v6.no2.2021.pg89.118>
160. Ominyi, M., & Anichukwueze, C. C. (2022). A conceptual framework for harmonizing data protection compliance across GDPR, NDPR, and United States privacy regimes. *International Journal of Social Sciences and Management Research*, 8(5), 148-174. <https://doi.org/10.56201/ijssmr.v8.no5.2022.pg148.174>
161. Ominyi, M., & Anichukwueze, C. C. (2023). A review of algorithmic accountability and model risk management approaches in financial services. *Journal of Accounting and Financial Management*, 9(12), 218-238. <https://doi.org/10.56201/jafm.v9.no12.2023.pg218.238>

162. Ominyi, M., & Anichukwueze, C. C. (2024). Conceptualizing responsible AI governance structures for automated decision systems in regulated industries. *International Journal of Social Sciences and Management Research*, 10(11), 403-430. <https://doi.org/10.56201/ijssmr.v10.no11.2024.pg.403.430>
163. Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2024). Developing a conceptual framework for AI-assisted compliance monitoring and anomaly detection in high-volume transaction environments. *World Journal of Innovation and Modern Technology*, 8(6), 204-228. <https://doi.org/10.56201/wjimt.v8.no6.2024.pg204.228>
164. Ominyi, M., Uchechi, N., Anichukwueze, C. C., & Jones, B. C. (2021). Shared responsibility and multi-jurisdictional alignment in global supply chain governance. *International Journal of Multidisciplinary Evolutionary Research*, 2(2), 131-147. <https://doi.org/10.54660/IJMER.2021.2.2.131-147>
165. Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2020). Information-security awareness and records confidentiality in Nigerian university registries: A behavioural assessment. *International Journal of Multidisciplinary Research and Growth Evaluation*, 1(5), 1032-1044. <https://doi.org/10.54660/IJMRGE.2020.1.5.1032-1044>
166. Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2024). Effectiveness of cybersecurity awareness training on insider-threat behavior among university administrators: An integrative academic review. *International Journal of Computer Science and Mathematical Theory*, 10(2), 117-144. <https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg117.144>
167. Oshoba, T. O., Hammed, N. I., & Odejebi, O. D. (2020). Blockchain-enabled compliance and audit trail model for cloud configuration management. *Journal of Frontiers in Multidisciplinary Research*, 1(1), 193-201.
168. Parker, C., & Nielsen, V. L. (Eds.). (2011). *Explaining compliance: Business responses to regulation*. Edward Elgar.
169. Perth Casino Royal Commission. (2022). *Perth Casino Royal Commission: Final report*. Government of Western Australia.
170. Pol, R. F. (2018). Anti-money laundering effectiveness: Assessing outcomes or ticking boxes? *Journal of Money Laundering Control*, 21(2), 215-230. <https://doi.org/10.1108/JMLC-07-2017-0029>

171. Poulston, J. (2008). Rationales for employee theft in hospitality: Excuses, excuses. *Journal of Hospitality and Tourism Management*, 15(1), 49-58. <https://doi.org/10.1375/jhtm.15.1.49>
172. Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press.
173. Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, 34(6-7), 849-855. <https://doi.org/10.1016/j.aos.2009.06.001>
174. Prawitt, D. F., Smith, J. L., & Wood, D. A. (2009). Internal audit quality and earnings management. *The Accounting Review*, 84(4), 1255-1280. <https://doi.org/10.2308/accr.2009.84.4.1255>
175. Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.
176. Reuter, P., & Truman, E. M. (2004). *Chasing dirty money: The fight against money laundering*. Institute for International Economics.
177. Royal Commission into the Casino Operator and Licence. (2021). *Report* (R. Finkelstein, Commissioner). State of Victoria.
178. Rules for Casinos and Card Clubs, 31 C.F.R. pt. 1021 (2024).
179. Rummler, G. A., & Brache, A. P. (1995). *Improving performance: How to manage the white space on the organization chart* (2nd ed.). Jossey-Bass.
180. Sakyi, J. K., Filani, O. M., Nnabueze, S. B., Okojie, J. S., & Ogedengbe, A. O. (2022). Developing KPI frameworks to enhance accountability and performance across large-scale commercial organizations. *Journal of Frontiers in Multidisciplinary Research*, 3(2), 81-93. <https://doi.org/10.54660/IJFMR.2022.3.2.81-93>
181. Sakyi, J. K., Nnabueze, S. B., Filani, O. M., & Okojie, J. S. (2023). Revenue assurance strategies leveraging artificial intelligence and big data in service-intensive organizations. *International Journal of Multidisciplinary Evolutionary Research*, 4(2), 58-75. <https://doi.org/10.54660/IJMER.2023.4.2.58-75>
182. Schmidgall, R. S., & DeFranco, A. (2022). *Hospitality industry managerial accounting* (9th ed.). American Hotel & Lodging Educational Institute.
183. Seyi-Lande, O. B., Arowogbadamu, A. A. G., & Oziri, S. T. (2022). Cross-functional key performance indicator frameworks for driving organizational alignment and

sustainable business growth. *International Journal of Multidisciplinary Futuristic Development*, 1(2), 1-18.

184. Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal*. Harvard Business School Press.
185. Takáts, E. (2011). A theory of "crying wolf": The economics of money laundering enforcement. *The Journal of Law, Economics, and Organization*, 27(1), 32-78. <https://doi.org/10.1093/jleo/ewp018>
186. Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2024). Real-time KPI tracking systems: A review of automated performance monitoring and data-driven decision making. *World Journal of Innovation and Modern Technology*, 8(6), 247-281. <https://doi.org/10.56201/wjimt.v8.no6.2024.pg247.281>
187. Treviño, L. K., Weaver, G. R., Gibson, D. G., & Toffler, B. L. (1999). Managing ethics and legal compliance: What works and what hurts. *California Management Review*, 41(2), 131-151. <https://doi.org/10.2307/41165990>
188. U.S. Department of the Treasury. (2024). *2024 national money laundering risk assessment*. <https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf>
189. U.S. General Accounting Office. (1996). *Money laundering: Rapid growth of casinos makes them vulnerable* (GAO/GGD-96-28).
190. U.S. Government Accountability Office. (2019). *Bank Secrecy Act: Agencies and financial institutions share information but metrics and feedback not regularly provided* (GAO-19-582). <https://www.gao.gov/products/GAO-19-582>
191. Uchechi, N., Ominyi, M., & Jones, B. C. (2018). Procedural standardization and workflow optimization in high-volume dispute resolution clinics: A systematic review. *Iconic Research and Engineering Journals*, 2(6), 420-452. <https://doi.org/10.64388/IREV2I6-1722789>
192. Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2021). Standardizing contract review workflows in enterprise legal operations: A systematic review. *International Journal of Multidisciplinary Evolutionary Research*, 2(2), 148-166. <https://doi.org/10.54660/IJMER.2021.2.2.148-166>

193. Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2022). Real-time compliance pipelines: A review of automated risk monitoring and enterprise data governance. *International Journal of Multidisciplinary Futuristic Development*, 3(2), 66-94. <https://doi.org/10.54660/IJMFD.2022.3.2.66-94>
194. Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2023). Advances in standardizing un-standardized compliance controls for high-volume non-traditional distribution networks. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6). <https://doi.org/10.62225/2583049X.2023.3.6.6838>
195. Unger, B., & van Waarden, F. (2009). How to dodge drowning in data? Rule- and risk-based anti money laundering policies compared. *Review of Law & Economics*, 5(2), 953-985. <https://doi.org/10.2202/1555-5879.1423>
196. Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting*, 1(1), 1-21. <https://doi.org/10.2308/jeta.2004.1.1.1>
197. Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. University of Chicago Press.
198. Verhage, A. (2011). *The anti money laundering complex and the compliance industry*. Routledge.
199. Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems*, 12(4), 5-33. <https://doi.org/10.1080/07421222.1996.11518099>
200. Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty* (2nd ed.). Jossey-Bass.
201. Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of Management Review*, 14(4), 490-495. <https://doi.org/10.5465/amr.1989.4308371>
202. Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38-42.