International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Financial and Operational Risks in Universal Banks in the Province of Albay

Maria Lourdes Flores Segovia

Asst. Professor, Sbma, Divine Word College Of Legazpi

Abstract

This study advanced a need to concretize universal bank risks in the contexts of rising incidence of frauds in varying degrees of scope and magnitude, internal to or external to universal banks in the Province of Albay. Objectives for this study include: a. Determination of financial and operational risks experienced; b. Identification of challenges faced in addressing and managing financial and operational risks; c. Assessment of the effectiveness of existing banking systems in managing financial and operational risks; and recommendation of measures for enhancing bank systems to improve financial and operational risks management

The data domain for this study consisted of forty (40) universal banks with primary data generated through a survey questionnaire.

Significant outcomes verified by this study include: Financial and operational risks are experienced at moderate levels, with market risks and technology and cybersecurity risks as dominant financial and operational risks experienced, respectively. The topmost challenges in managing risks are credit (financial), internal process, and human error (operational). Existing banking systems in the management of financial and operational risk management are moderately effective. The top three recommended measures for enhancing universal bank systems with respect to: a. Financial Risk Management -- first, general risk management; second, foreign exchange risk management; third, liquidity risk testing; b. Operational Risk Management -- first, senior management; second, governance; third, risk management environment identification and assessment principles.

The study proposed several measures to mitigate financial and operational risks. Key recommendations include adopting dynamic credit scoring models that adjust to macroeconomic shifts, implementing market risk hedging strategies supported by real-time analytics, and enhancing liquidity planning through predictive cash flow forecasting and emergency funding strategies. On the operational side, the integration of regulatory technology (RegTech), continuous employee training, infrastructure upgrades, and the development of a risk-aware organizational culture were recommended to address compliance, cybersecurity, and internal process risks.

INTRODUCTION

Background

The microchip has given the world a link to the digital backbone of the world economy. Life after the worldwide web was first invented slowly, then exponentially developments in technology necessitated online transactions as a mode of choice or convenience, from communications, grocery shopping, food deliveries, work compensations, banking to business transactions emerged. From the simplest to the most complex interactions, the choice of transferring money to and from domestic or international accounts is

conveniently consummated with a few password-mediated clicks via the internet. Indeed, a modern technology-driven economy demands individuals and organizations to adopt into the cyber world. Such world is full of promise, and like the *Garden of Eden,* it too has back stories of pitfalls or trap doors when one is not careful in navigating this world heavily reliant on automatic AI facilitated systems – one click completes a transaction in split seconds.

Banks are lifelines of any economy more so now, that digital lifestyles is the choice of almost all individuals/organizations. They are institutions of trust buffered by legal structures and compliance standards imposed by their governments as well as the international monetary systems of the world. The digital economy has a parallel shift in borderless international finance. In these contexts of domestic and international finance banks in the Philippines must build fool-proof systems of security against fraud.

Any unauthorized intrusion into the banking systems threatens the bank, the banking institution, the domestic economy, with potential for concomitant consequences on the international economy.

Mindful of the immediate and long-term consequences of breaching bank security systems, this study is designed to document what and how this frontier defense of financial health of this country is made robust against any inadvertent or willful scams. Scams of all sorts, as evidenced by on-going Quad Committee investigations, has roots in the domestic as well as international landscape. The Quad Committee is a special committee in both the House of Congress and House of Representatives authorized to review crimes on dangerous drugs, public order and safety, human rights and public accounts.

What this study zeroed in is the present provisions and the future provisions for safeguarding the Philippine economy through reliable and dynamically effectively efficient anti-fraud systems technology of banks, specifically universal banks of Albay Province. Investments in updated anti-fraud technology require parallel developments as the fast-paced hackers of malware motivation advanced by illegal syndicates, generally supported by corrupt authorities. Batalla (2020) cites the unfair closure of prosecutorial cases involving grand corruption in big projects that skips standard transparency and accountability protocols. Transparency International in 2020, cites the country's corruption perception index to have fallen from 99th to 113th. Also a 50% increase in the

same year on fraud incidents have been recorded which cited aggravating causes include: poor use of digital systems to arrest economic crimes and laws on Bank Secrecy and Anti-Money Laundering (AML) that hinder full criminal investigations. (pwc, 2020).

Against the background of the banking institutions' economic functionality filtered through the rising tide of economic crimes in these modern times, this study justified its research commodity value as well as its substance. To initiate appropriate focus on safeguarding the country's banking systems is necessitated by the proliferation of scams domestically and across international borders is a sound academic mandate for a business school, hence this study contextualized in the domain of universal banks of a province.

Cyber crime is an illegal activity perpetrated by opportunity. Computer applications that use artificial intelligence to study how individuals of organizations behave as to mark the most opportune time to breach security systems to siphon funds illegally, has become the crime of choice of the 21st century. Any type of economic crime – asset misappropriation, bribery and corruption, and all forms of frauds --customer, cybercrime, deceptive business, accounting, human resources, intellectual property, money laundering – can be perpetrated via breach of cyber security. The PNP, in a span of six (6) years from 2013 – 2019, through its Cybercrime Unit has investigated 510 times more cybercrimes than in its initial year. (pwc, 2020). These are staggering statistics that is on the rise in the techno-mediated modern economy.

Phishing attacks in the Philippines increased by 34% in 2022 from 2021 figures (i.e 1.8 million from 1.34 million). These attacks included local bank attacks as well as e-commerce transactions and payment systems. (Balita, 2023). Imminent threat to bank fraud is a reality for banks at any time. Such bank work-risk was made clear with the 2016 RCBC involvement in a bank heist that shifted $81M from the Bangladesh Bank account in its NY Federal Reserve Bank to accounts in RCBC-Manila. Of this amount, only $15M was recovered from operators involved in Philippine casinos; RCBC was fined by the BSP with Php1B ($20M) for this heist. (Quadir, 2019).

Restrictive laws in effect in the country prevent full investigation of money laundering cases. These include the Secrecy of Bank Deposits and Anti-Money Laundering Laws. The International Monetary Fund (IMF) advanced that the country's secrecy laws pose direct challenge to sustaining financial stability, integrity, and reputation of the banking sector. This is why BSP is unable to fully review bank accounts requiring intense scrutiny. (Balute, 2023). The trend on transparency across the world seems not to effect a concomitant ripple effect in the country's legal provisions on Bank Secrecy covered by R.A. No. 1405.

R.A. No. 9060 established the rules on Anti-Money Laundering. It provides for legal actions against illegally obtained money via bank deposits intended to mask source and manner of fund acquisition. Detection, prevention and prosecution of money laundering from within or from without the country is framed against the AMLA provisions. R.A. Nos. 10167 and 10365 enacted amendments to R.A. No. 9060 in matters of, in the former, i) freezing of accounts; ii) authority to review bank accounts;

in the latter, iii) expanded definition of covered persons, iv) coverage of unlawful activities, v) refined meanings of precious stones, precious metals, vi) offenses categorized as money laundering, vii) prosecution and penalties, and viii) anti-money laundering council (AMLC).

A recent highly sensitive case filed with the AMLC is the Alice Guo POGO inquiry by the Quadcom committees of the Philippine Senate and Congress. It is related to tracing an alleged check payment for a Baguio property for Php85 million. The AMLC filing is for freezing of assets in 90 bank accounts of Ms. Gou in 14 bank institutions in the country. (Casucian, 2024).

Rationale

An interconnected world requires a digital infrastructure. The worldwide web allows for the borderless flow of money into and out of any country, region, or economic bloc (e.g., the European Union (EU), the North American Free Trade Agreement, and ASEAN). The financial infrastructure that underwrites this digital world is the banking industry.

In recognition of the critical role of the banking industry in the economic resilience of a community, this researcher chose to focus on Albay Province's universal banks management of financial and operations within the environment of risks arising from the digital, AI-enhanced financial systems which move all forms of money (cash, digital currency, crypto currency, credit, trust funds, investment bonds) across clients (individuals, merchants, organizations, etc). This study was rooted on:

a. Confirming the types and level of risks experienced by banks as the basis for possible action on building resilience and robustness of their risk management systems;
b. **Generating evidence** for top-level bank management, as well as the board of directors, on the necessity to establish an efficient and effective bank risk management system; and
c. **Documenting** bank managers' **collective feedback** on the realistic and achievable improvements in the present bank system's risk management; and

d. Utilizing the **researcher's experience as leverage** for understanding research results & in the identification of relevant implications of said results.

Current State of Research in the Field

Scams in the Philippines are highly prevalent. In fact, from a survey (FICO, 2023), 82% of sampled Filipinos received unsolicited e-communications as a component of a scam and 61% had friends of families victimized by scams. This FICO survey tapped 1001 adults who used real-time payments (RTP) via several digital payment merchants – Gcash, PayMaya, and the like. Of this sample, 98%, 97%, 95% and 85%, respectively sent, received, will use, and believe it is safe to use RTP.

Review of Related Studies and Literature

Cyber security threats can take various forms and scope. It can be a global threat, country-wide threat or it can be an industry level threat. Pociumban (2023) in her study of Moldova's vulnerabilities identified massive cyber attacks aimed at government institutions. Such attacks were validated as the responsibility of a web-based channel, "People's CyberArmy."

Data that are at risk of being illegally used include: bank customer information, history of bank transactions, login history, financial instruments (account information, credit card information, and ATM information). Cyber security is about prevention, mitigation, recovery from breaches of banking financial systems. The robustness of a bank's systems security from cyber attacks will guarantee its resilience to bounce back immediately from any breach. In 2021, cyber attacks were made to organizations in the Philippines at 69% with 257% rise worldwide in API (applications programming interface) and web applications. (Kital, 2024)

There are three common cyber security risks for banks – Data Breaches, Ransomeware Attacks, and Phising. Data Breach is the most frequent form of attack. A data breach is consummated when a hacker is able to access bank client's information which make it possible for illegal use of the client's bank account in whatever form and manner the hacker desires. Ransomeware is facilitated with a software applications that locks a bank client's account until the client pays the hacker's asking fee/ransom. The average cost of a data breach in the U.S. was US$9.48M in 2023 and US$9.36M in 2024. (Statista, 2024). Phising is a technique of duping individuals in inadvertently clicking links or emailed notices of urgent action on bank accounts, else it will close or other similar reasons. Once a malicious link is enabled, sensitive information is captured and illegal use of the individual's bank account proceeds until the account holder notices unauthorized charges or withdrawals. This is a common threat in digital transactions, a regular habit of most people using online merchants for their everyday needs or e-access of their financial bank accounts. Online data breach was at 37 per 1000 in 2021, 11 per 1000 in 2022. (Statista RD, 2024).

Much is desired in terms of cybersecurity resilience of Philippine organizations. Balita (2023) is of the opinion that the country is at the seminal stage based on a 2022 survey which found that majority of companies have below average cyber security systems. Balita also warned of the need for individuals to cybercrime-proof themselves due to the increasing sophistication in malware development and deployment congruent to the increasing use of online transaction in the Philippines and across the world. Citing IBM data, the ASEAN countries average cost of data breach was at $3.23 million this 2024 from $3.05 million the prior year. The average global cost of data breach was at $4.88 million posting a 10 percent annual increase. The biggest ASEAN data breach cost was borne by the financial services industry at $5.51million. (ARAI, 2024). The U.S. data breach average cost was at $3.54 million in 2006 to %9.36

million in 2024. (Statistica, 2024). The IBM report cites costly business losses arising from the data breaches including loss of customers and reputation.

Data breaches for the ASEAN in 2024 consisted primarily of phishing at 16%.

(ARAI, 2024). For the Philippines, from Jan 1 to Dec 7, 2023, a total of 19,884 online scams of which 55.67% (at 11,071 cases) were recorded. This crime caseload makes online scams the top cybercrime for the year. Of the total scams, were illegal access (at 3,181 cases), computer facilitated identity theft (1,536 cases), ATM/credit card fraud (1,043 cases). (Tupas, 2023).

Fraud management systems by banks are essential tools to sustain its credibility from their clients' perspective as well as from the overall public perspective. A study adopted bank clients' assessment of bank systems on fraud management efficiency in protecting their deposits as well as personal information. It further evaluated how bank clients' patronage is influenced by clients' faith in the bank's fraud management. The results of the study established that exposure to bank fraud affects clients' confidence in the banks credibility as well as its integrity. Response time, communication, and compensation of breach of anti-fraud bank systems influence also commitment of clients to the banks efficiency in addressing fraud issues. (Azba, 2024). A restriction on the generality of Azba's research conclusions is its limited respondents of six adopting a set of qualitative data generated via interview.

A study which tapped seventeen (17) research participants purposively selected, consisting of technically qualified fraud investigation professionals including managers, investigators, specialists and data scientists, verified online fraud detection in banks of Africa and Spain. (Phiri et al., 2024). Said study established weaknesses in both countries online fraud detection practices – lack of experts in Africa and lack of legal sanctions in Spain specifically on online banking. Given the rapid pace of technology development in digital transactions, banks need to keep abreast with the latest innovations on bank systems anti-fraud applications with the concomitant policies regulating the bank industry in each country as well as in its compliance to international banking standards. The interconnected economy network of almost all countries, demands efficient anti-fraud systems of universal banks essentially linked to international financial transactions. In fact, Phiri et al. established that due to the lack of experts in fraud detection for banks, bank systems breaches have been rising for Africa, particularly with a 13% increase in bank fraud incidence in 2021 from the previous year. Spain fraud incidence is exacerbated by customers using same passwords across various platforms –cable subscription, FB accounts, etc, as well as bank accounts. That this disadvantage is heightened by lack of fraud regulation in the country. With fraudster focused on developing malware to hack into financial systems, the threat to financial accounts and information clients entrust to banks will be at high risk for unauthorized access or usage.

SRISK metrics measures the capital shortage in the event of a massive financial crisis. Said metric was applied to 8 banks in the Philippines for the period 2009 – 2019, and found an increasing trend in SRISK indicator reflective of systemic accumulation of bank debts requiring regulation (Gabrodi and Razote, 2020). This also implies a need to fortify policies governing the bank industry.

A study of financial fraud in Sudan's commercial banks revealed that heightened forensics fraud investigations resulted in decreased incidence of fraud in such banks.

(Mabior and Wanyama, 2024). From the results of a study of nine (9) commercial banks and 119 bank personnel, the researchers recommended use of systems that establish reliable high-end anti-fraud technologies including data analytics, forensic accounting and controls within the organizations. The study confirmed the belief of commercial bank personnel on the effectiveness of forensic accounting as a deterrent to commission of bank fraud.

Braithwaite (2022) emphasized that crime is better addressed or deterred through self-incapacitation. He subscribes to the school of thought that self-incapacitation is more powerful than preventive restriction even by the state both for individual and organizational crimes. A macrocriminological theory contribution of Braithwaite is a pyramid of incapacitation as a tool in addressing criminality. Said pyramid consists, from the base to the top of the following: education, persuasion, organizational self-incapacitation, enforced self-incapacitation, deterrent civil penalties, deterrent criminal penalties, temporary state incapacitation, and permanent state incapacitation.

A study of the banks of India covered the period 2012-2023; it focused on measures taken by the Reserve Bank of India with other banks to curtail fraud (Tirumalaraju, 2024). The study found that both private and government banks had similar amounts lost to fraud consisting of cheating, forgery and fraudulent encashment. Decreasing amounts of reported losses due to fraud by private and government banks were recorded from 2020 onwards because of proactive measures implemented by the banks. Another significant finding of this study is the greater number of financial manipulation by private bank customers than those of government banks. Thus, the recommendation to screen bank clients as a preventive anti-fraud measure was advanced.

Experts in fraud risk management invoke the need to involve bank managers, because of their short span of control of bank's daily transactions, to the core components of fraud risk management. In fact, involvement of all bank personnel in fraud risk management bolsters the institution's first line of defense against fraud. (IIA, 2015). It is a misnomer to entrust fraud detection to auditors or internal control staff. Unless a collective integrated system of fraud prevention is established and monitored to be functionally efficient and effective, fraud incidence will continue to plague the bank industry.

The Banko Sentral ng Pilipinas requires financial institutions to adopt automated fraud monitoring in real-time as a defense against fraud (Villanueva, 2022). BSP Circular No. 1140 enhances its IT Risk Management Framework guidelines by elevating the requirement of integrating fraud detection, anti-money laundering systems, and other cybercrime detection systems to fortify financial institutions against any or all forms of attacks. Prevention of crimes against financial institutions is a fundamental responsibility of management and it is a collective responsibility of all stakeholders internal and external to the institution.

Even with R.A. No. 1140 in effect, the Philippines is one of countries listed on the Financial Action Task Force (FATF) grey list. The country has to provide significant functional and effective actions on Anti-Money Laundering (AML) and Counter Financing of Terrorism. One focus of such set of actions will be on banking and remittance services as these sectors are vulnerable to cyber attacks. (Fortifying Against Financial Crime). The threat of considerable financial crimes commission in the Philippines is a reality that threatens the financial stability of the country. Definitive actions are required, not only to exit the grey list of FATF but also to ensure the country's economic sustainability

The economic burden of fraud detection is a two-edged sword. It cuts through the core of financial institutions' service quality. Maintaining an effective integrated fraud detection system is a significant burden which must be part of overhead expense of the organization. Using a less efficient and effective fraud detection system can lower the cost burden but it increases the threat to a weakened credibility client perception which translates to decreased bank client volume. A strategic option that balances the pros and cons of maintaining a high-end fraud detection system requires sustaining a sustainably competitive per-capita bank client subsidy of such a system. A study by Yoganandham (2024) highlighted the need to use

an interlinked fraud detection system heavily fortified by computer technology that insures, *a priori particularly,* the robustness of such detection system.

Consequences of cyber fraud are significant to both the bank client or credit card user as well as to bank personnel. Corollary consequences to the banking or financial sector is also generally substantial. Yoganandham recommends that use of cutting edge cybersecurity automated systems must be complemented with consumer education to

fortify protection of all stakeholders' financial resources, also the general economy's health. Every nation across the world is fundamentally linked to the digital world systems. Every domestic economy mirrors the digital global economy. Resilience and competitiveness are dual core characteristics of any fraud detection system particularly those undergirding the banking industry.

The complex process of detecting fraud requires a combination of tools – the detection model algorithm, the technology backbone, the fraud auditors, and other professionals who analyze human behavior. These group work towards providing the shortest fraud detection time when it happens and the development of the most robust system to prevent fraud. Banks are vulnerable institutions in that they are targeted by scammers. A systematic literature review revealed that publications have highlighted mature general fraud detection analyses but there is insufficient research focusing on human behavior or use of data mining techniques (Sanchez-Aguayo et al., 2021). This research used the fraud triangle model.

Endriano et al. (2022) also utilized the fraud triangle model in their analysis of preventing fraud in banks of Indonesia but adopted the qualitative research method and non-parametric statistical analysis. The researchers recommend use of a 3-pronged process – prevention, detection and response. Prevention involves decreasing the potential for fraud, detection by whistleblowing, response by reporting to authorities of crime and the generation of evidence required for criminal-judicial sanctions (Indrianto et al., 2023). The researchers recommended research on causes of fraud as a model for

fraud risk management.

The study by Hussain and Anees (2022) declared fraud risk management explained by bank performance with risk culture as mediating variable. The resulting regression analysis confirmed that fraud risk management is significantly explained by bank performance at an R^2 of 99%, in fact, preventive measures for fraud contributes to level of performance of Indonesian banks, both private and public banks. The researchers intended to address the need for improvements in banks of Pakistan's use of digital payment schemes within the country as well as in their international transactions.

Risk Management Practices in Philippine Banks

Cruz and David (2019) conducted a study on risk management practices in Philippine commercial banks. Their research identified that while banks in major cities like Metro Manila employ advanced risk management tools such as credit scoring models, those in provincial areas like Albay tend to use simpler, more traditional methods. The study highlighted a gap in the adoption of sophisticated risk management technologies and recommended training and development programs to improve risk management capabilities in smaller banks.

The importance of properly handling loans/credit risks is enlightened by Syadullah (2018) in establishing that there is direct association between net interest income-to-loans income and efficiency level of banks. Further, Syadullah recommends expansion of Indonesian banks to four ASEAN countries including the Philippines where demand for banks is high considering the significant contribution to the GDP of the financial and insurance sector in these countries. This implies the requisite efficiency of credit as a bank

commodity when ASEAN banks can operate outside of their base country.

Espinosa (2020) analyzed the effectiveness of existing risk management frameworks in Philippine banks. The study found that banks that have adopted the Basel III guidelines and BSP Circulars on risk management practices were better at mitigating credit and operational risks. However, the research also noted that many banks still struggle with integrating these guidelines into their daily operations, suggesting a need for continuous monitoring and evaluation to ensure compliance and effectiveness.

Santos (2020) analyzed the impact of Bangko Sentral ng Pilipinas (BSP) regulations on risk and stress management in Philippine banks. The study found that while compliance with BSP regulations helped reduce systemic risks, it also increased the workload and stress levels of bank managers due to the complexity and frequency of regulatory updates. The study suggested that regulatory bodies and banks work together to streamline compliance processes and provide additional support to bank managers to manage stress effectively.

Gonzales (2019) examined the effects of Anti-Money Laundering (AML) regulations on the stress levels of bank managers in the Philippines. The study revealed that the stringent requirements for monitoring transactions and reporting suspicious activities added significant pressure on bank managers. The research recommended that banks provide specialized training and technological tools to support managers in complying with AML regulations and reducing associated stress. Marasigan and Cruz

(2022) studied the influence of organizational culture on risk management practices in Philippine banks. Their research found that banks with a strong risk-aware culture—where risk management is embedded in every level of the organization—tend to perform better in identifying and mitigating risks. The study highlighted the need for banks in the Philippines to foster a culture of transparency, accountability, and continuous learning to improve risk management outcomes.

Lopez (2018) examined how organizational culture affects stress management in Philippine banks. The study found that banks that promoted an inclusive culture, where employees felt valued and heard, had lower levels of stress among managers. This research suggested that cultivating a positive work environment can play a crucial role in reducing stress and enhancing overall performance.

Aguila and Santos (2021) evaluated the effectiveness of training programs in risk and stress management for bank managers in the Philippines. The study found that banks that regularly conducted training workshops on risk management, stress reduction techniques, and leadership skills reported lower levels of stress and better risk management outcomes. It suggested that banks invest in continuous training and development programs tailored to the specific needs of their managers.

Domingo (2020) explored the impact of financial literacy and risk management training on decision-making among bank managers in provincial banks in the Philippines, including those in Albay. The study found that managers who received training in financial literacy and risk management were more confident in their decision-making and better equipped to handle stressful situations. The study recommended the expansion of training programs to include modules on emotional intelligence and resilience building.

Salvador and Torres (2020) conducted case studies on several banks in the Philippines to understand their risk and stress management practices. Their research found that banks that invested in digital tools for risk monitoring, such as automated risk assessment software, and provided regular training to their managers were more effective in managing both risk and stress. The study suggested that smaller banks in regions like Albay could benefit from adopting similar technologies and practices.

Villanueva and Cruz (2018) explored the risk management practices of rural banks in the Philippines, focusing on those in less urbanized areas like Albay. The study found that rural banks often face unique

challenges, such as limited access to technology and a lack of specialized personnel, which impact their risk management capabilities. The research recommended that rural banks collaborate with local government units and industry associations to improve risk management practices through knowledge sharing and capacity-building initiatives.

Reyes and Villanueva (2020) examined the adoption of advanced risk management tools such as Value at Risk (VaR), risk-based capital assessments, and stress testing in Philippine banks. Their study found that while these tools are more commonly used in larger banks, smaller regional banks, including those in areas like Albay, tend to rely on simpler methods, such as ratio analysis and historical data, due to resource constraints and lack of technical expertise. The authors advocate for targeted training and investment in risk management tools to enhance the capability of bank managers to manage risks effectively.

Castro (2019) discussed the slow adoption of digital tools and technologies in risk management among Philippine banks, particularly in provincial settings. The study highlighted the potential benefits of embracing digital transformation, such as real-time data analysis, automation of routine tasks, and improved accuracy in risk assessment. The literature suggests that banks in regions like Albay could greatly benefit from cost-effective digital solutions that are tailored to local needs.

Role of Government Bank Regulation and Economic Council

The role of government compliance guidelines can be inferred from results on banking performance regressed on different bank variables in the context of ASEAN countries (Laili et al., 2024). Two variables recorded significant relationship with banking performance – macroeconomic factors and country governance using corruption index as alternate variable.

In 2022, the Asean Macroeconomic Research Office (AMRO) performed a stress test on Philippine banks. (Tsang, 2022). They were found to be resilient, except for one small-medium bank, in the contexts of three different scenarios – a. recession, b, surge in interest rates, and combination of a and b. That is, the stress tests affirmed that almost all these banks will be able to comply with BSP's capital requirements. Bangko Sentralng Pilipinas aware, that despite the bank stress test results, some small-medium sized banks will be challenged by macroeconomic stressors, asserts that it provides the guidance in the development of risks framework in terms of their assessment and management. AMRO's 2023 report affirms the resilience of ASEAN+3 countries through the global financial crises in 2021 but warns of the potential recurrence of inflation that could potentially affect the ASEAN+3 countries.

AEC 2025 is a guideline on the integration of ASEAN countries as an Economic Community (BSP, 2025). This movement has three objective visions – integration, inclusion and stability of financial institutions in the said region ten (10) years onwards. The AEC 2025 benefits the Philippines with greater influx of trade and capital; a stronger network of markets; and synchronous payment systems. Complimentary risks dovetail these benefits.

Human Resource Practices and Risk Reduction in Philippine Banks

Domingo and Bautista (2020) studied the role of human resource practices in managing stress among bank managers in the Philippines. Their research highlighted the significance of practices such as flexible work arrangements, employee recognition programs, and career development opportunities in reducing stress levels. The study emphasized that effective human resource management is critical to maintaining the well-being of bank managers and enhancing their ability to manage risks. Lopez (2019) focuses on the impact of leadership styles on stress management among bank employees, including managers. The

research found that transformational leadership, which involves inspiring and motivating employees, was more effective in reducing stress compared to transactional leadership, which focuses on tasks and performance metrics.

Ortega (2021) explored the role of cultural factors in shaping risk management practices in the Philippines. The study suggested that local cultural attitudes, such as a preference for conservative financial strategies and a hierarchical decision-making structure, can affect the adoption and effectiveness of risk management practices. In regions like Albay, where local culture may be more pronounced, understanding these cultural dynamics is crucial for designing effective risk management strategies that align with local values and practices. Similarly, De la Cruz (2020) discusses the influence of Filipino cultural traits, such as "hiya" (shame) and "pakikisama" (getting along), on stress management and risk-taking behaviors among bank managers. The literature suggests that these cultural factors can sometimes hinder open communication and transparent decision-making, thereby affecting risk management outcomes. The study recommends fostering a culture of openness and trust within banks to overcome these barriers.

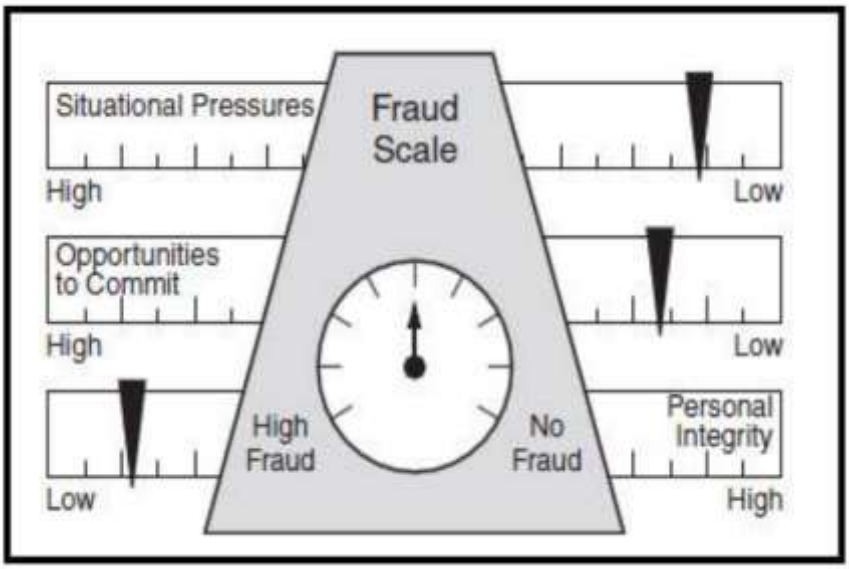
Impact of External Economic Factors on Risk and Stress Management

Aguila (2018) examined how external economic factors, such as inflation, currency volatility, and regulatory changes, impact risk and stress management in Philippine banks. The study found that these factors often create additional layers of complexity for bank managers, who must navigate uncertain economic conditions while maintaining profitability and regulatory compliance. The research suggests that scenario planning and stress testing should be integral parts of the risk management process to prepare managers for various economic scenarios. Torres and Ruiz (2022) studied the effect of global financial trends on local banks in the Philippines, particularly those in less urbanized areas like Albay. Their research indicated that global events such as trade wars, changes in international interest rates, and pandemics can significantly impact local banks' operations and increase stress levels among managers. The study highlighted the need for local banks to develop flexible risk management strategies that can adapt to both local and global changes.

Theoretical Framework

Three models of fraud detection in various occupations were utilized as frameworks of this research. These are the fraud triangle, the fraud diamond, and the fraud scale. The Fraud Triangle by Cressey (Machado, 2016) posits that there are three elements that nurture fraud. These are, opportunity, pressure and rationalization. Forensic auditors and financial auditors generally use this theory in the identification of loopholes and conduits of fraud for any organization. The Fraud Diamond Theory advances that fraud occurs when four elements are in place. These are: opportunity, pressure, rationalization and capacity. Capacity is the fourth element which elevates the Fraud Triangle theory to the Fraud Diamond theory. The latter theory underscores the existence of the fourth element for fraud to be consummated. That is, without the capacity to commit fraud, even when the other three elements are in existence, consummation of an illegal act will not be easily consummated.

The Fraud Scale was developed by Steve Albrecht in the 1980s. (Fisher, 2015). It is a means of scaling the fraud risk with measures of three elements of Fraud, similar to that of the Fraud Triangle, except rationalization is replaced with personal integrity. The Fraud Scale is useful for the determination of preventive estimation of an individual's predisposition to fraud. Albrecht offered 10 criteria that identified such predisposition



Fraud Scale, Steve Albrecht (Kranacher et al., 2011).This study utilizes the Fraud Diamond Theory as its theoretical framework to guide direction and substance of this proposed research. Figure 1 illustrates said theoretical framework.

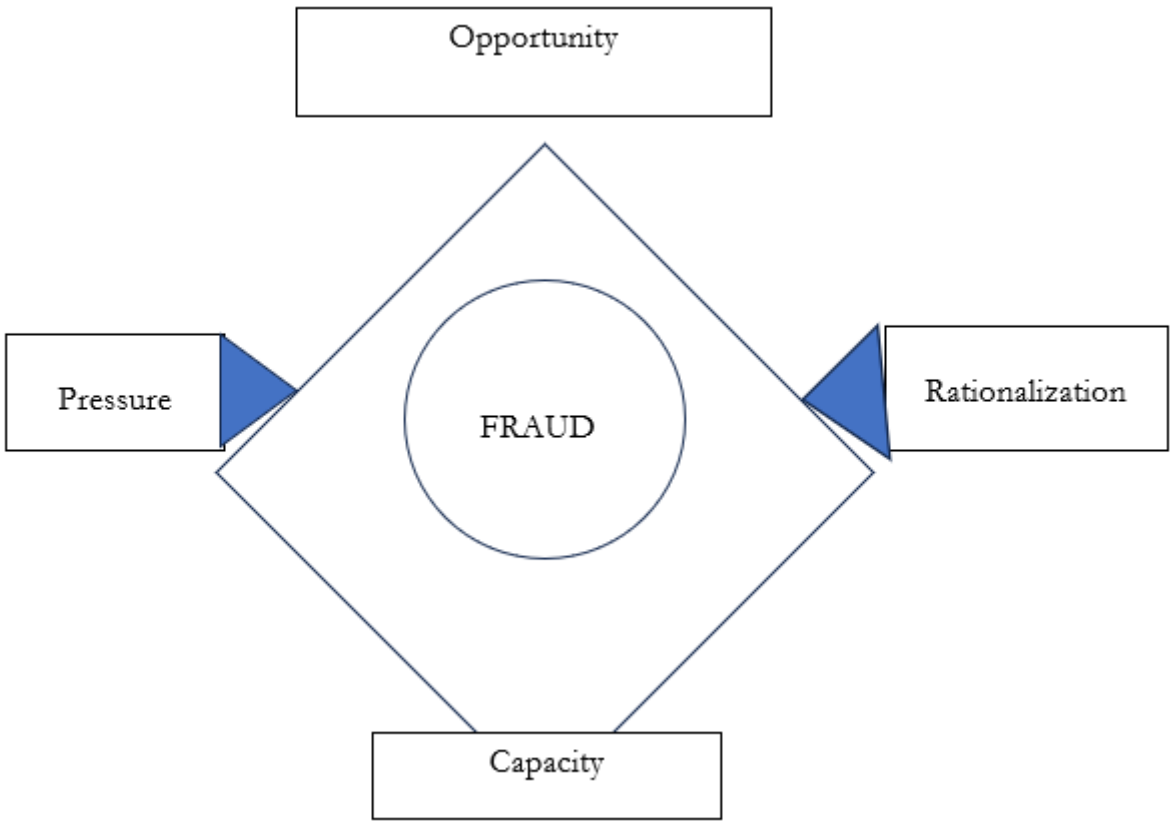


Figure 1. Theoretical Paradigm

Conceptual Framework

Studies that deal with anti-fraud management utilize either the Fraud Triangle, the Fraud Diamond, and

the Fraud Scale Theories as theoretical bases. Hermanson and
Wolfe (2024) even proposed consideration of additional elements to these theories with a view of refining the anti-fraud efficiency of certified public accountants or financial forensics practitioners. Moore (2020) proposed an expanded model for occupational fraud analysis which combines all three fraud management models with organizational culture as an additional component. Said proposed expanded model consists of four elements, namely, pressure, opportunity, rationalization, and organizational culture. This new model of fraud analysis is applicable to first time offenders, not to repeat offenders. The researcher recommended assessment of their expanded fraud model as a process of refining its generality and applicability.

A literature review on use of the fraud triangle by Suryandari et al. (2023) covered 25 articles on the topic. Of these articles, 80% addressed the elements of the fraud triangle with 60% of these supporting the tenet that such elements prompt commission of fraud. The researchers forwarded the need for additional inputs to the refinement of the elements of the fraud triangle similar to that of Moore (2020) and Hermanson and Wolfe (2024).

The present study used the framework of the Fraud Diamond Theory as a template for a review of how risks in banks in Albay Province can be blocked or minimized with recognition of conduits of such risks including fraud. The principle tracked by this study is a route that can create significant improvements in Banks of Albay management of risks particularly financial and operational risks. It has also the potential of strengthening the base structure of the fraud diamond elements.

Identification of financial and operations risks of Albay will pinpoint specific conduits of cyber security risks, fraud, threats, and human risks involved in the daily bank operations. By the nature of these risks, parallel bank policy needs will be implied by them. The identified risks in bank management, ideally will have corresponding systems intended to block or minimize these, relative to how these can affect banks' financial and operational efficiency. Thus, by determining the Banking Systems in the Management of Financial and Operation Risks vis-à-vis the specific risks – with potential or actual incidence, can tighten a meshed basis for the understanding of the fraud diamond that rationalizes commission of almost all forms of deception intended to illegally obtain money from others.

The ideal perspective to bank management of risks are mostly reflected in various bank policies, central bank regulations, and accounting/audit standards. Realistically, the ideal and the actual implementation of these policies governing the banking industry, including the banks of Albay Province, are not completely congruent. Deviations are willfully or inadvertently practiced to benefit or to put to disadvantage the banks' efficiency, credibility, or fiscal compliance. It is in this context of strengthening the bank systems of managing their financial and operational efficiency that strategic approaches to achieving higher levels of financial and operation efficiency are necessary. In view of this consideration, this study determined the banks Strategies for the Management of Financial and Operational Risks.

The triad of factors considered in the assessment of banks' financial and operational risks are: (1) the specific bank risks -security risks, threats, fraud, human risks, (2) the bank systems for addressing these risks, and (3) the strategies for managing these risks are all intended to understand, extract the major conduits of risks, then develop systems for blocking or resolving these risks. When these triplet of anchors for this
study are established, they then become collective inputs to the development of an Improved Bank Financial and Operational Management System (IBFOS). The IBFOS is the target output of this study.

In adherence to the need for underscoring elements that can refine the Fraud Diamond Framework, this study expanded the scope of fraud as those that encompass risks to bank's security, anti-fraud policies, threats to financial and operational efficiency, as well as those posed/caused by its human resource.
The conceptual framework illustrates the relationship between the key components of the study: the types of risk encountered by universal banks, the strategies they employ to manage these risks, the challenges they face, and the resulting recommendations. This framework served as the logical structure guiding the investigation.

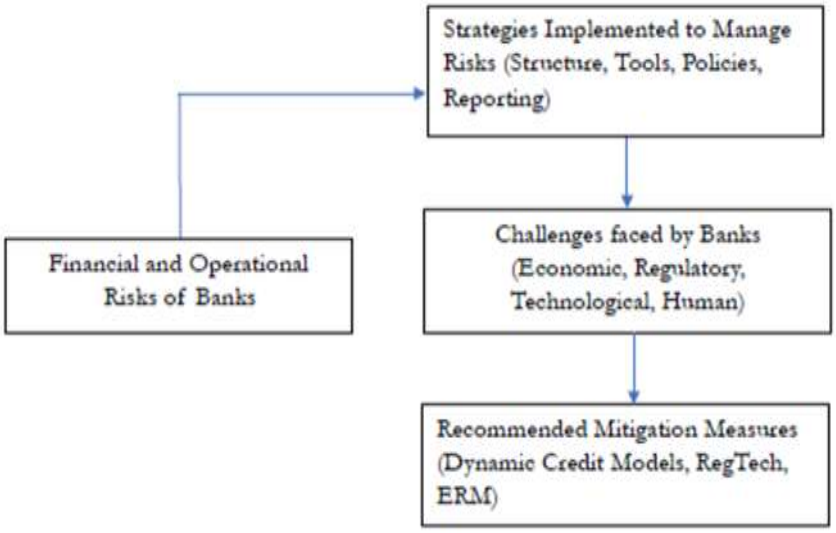


Figure 1: Conceptual Framework of Risk Management in Universal Banks in Albay

The framework begins with the identification of Financial and Operational risks that universal banks in Albay must manage. These risks—spanning credit, market, liquidity, compliance, technological, and internal processes—drive the need for structured risk management strategies. These strategies are implemented through organizational structures, tools, policies, and reporting practices. However, despite these efforts, banks face a range of challenges that hinder effective risk management. This includes macroeconomic volatility, rapid regulatory changes, technological vulnerabilities, and human-related errors.
In response to these challenges, the study proposed recommendations aimed at improving institutional risk resilience. These include the use of AI-enhanced risk models, real-time market analytics, regulatory technology systems, upgraded cybersecurity infrastructure, and comprehensive risk management training programs. The arrows in the framework show a linear progression from problem identification to strategic intervention and eventually solutions. This logical flow supports the study's purpose of assessing and enhancing risk management practices in the banking sector of Albay.

Synthesis of the Art

Risks in the banking industry have been identified to be of different types and degrees. These risks consist mainly of data breaches that take the form of cyber-security risks, threats, fraud or human risks. The degree or scope by which these risks are committed could be global, country-wide, region-wide or institutional perpetrated by
individuals or a syndicate Pociumna, 2023; Phiri et al., 2024, Mabior and Wanyama,2024; Hussain and

Anees, 2022) . Aggravating circumstances for the commission of banks' data breaches include corrupt groups or individuals, weak risks management systems or inadequate level of internal and external risks control.

Banks' vulnerability to all forms of risks are established globally, by international economic zone, and domestically. Costs of risks computed as average cost of data breaches have been established to be significant across such levels (Statista, 2024; ARAI, 2024; Tupas, 2023). Risks management systems for the bank industry in these levels/groups are within a spectrum – from the simplex to the complex high end using artificial intelligence with embedded data analytics. These take the form of bank performance as explanatory variable for bank risks (Hussain and Anees, 2022); Interlinked fraud detection using computer technology (Yoganandham, 2024); fraud forensics (Mabior and Wanyama, 2024); Self-incapacitation or the pyramid of incapacitation for fraud (Braithwaite, 2022); Screening bank clients for potential predisposition to fraud (Tirumalaria, 2024), Use of the Basel III Guidelines (Espinosa, 2020) or linking with government organizations for reinforced bank risks management system (Villanueva and Cruz, 2018). Internal and external bank risks controls also come in varied form, from the standard accounting and audit systems to fraud risks forensics.

Philippine banks have been victims of syndicated data breaches. Banks in the country are generally identified to adopt/implement bank risks management systems not yet at par with the global high-end standards (FICO, 2023; Kital, 2024; Castro, 2019;

Espinosa, 2020; Cruz and David, 2019, and Balita, 2023). As a scaffold to anti-financial sabotage which can affect domestic, regional, or international economies, nations, including this country impose relevant laws and regulatory standards for bank risks management. Villanueva (2022) cites the use of Automatic Fraud Detection rule for banks by the Bangko Sentral ng Pilipinas, R.A. 1140 (Risk Management Framework Guidelines).

Problems with inadequate legal sanctions on fraud, specifically bank fraud have been advanced by researchers (Phiri et al., 2024, Gabrodi and Razote, 2020). Recommendations on actions for improved anti-fraud or anti-risk management in banks have also been advanced by researchers to include improving bank management efficiency (Azba, 2024); Involvement of bank managers in the risk management system (IIA, 2015); and investment in validated risk management tools (Reyes and Villanueva, 2020.

Human risks arising from various forms of factors in Philippine bank operations, primarily stress, have been identified by various researchers (Santos, 2020; Gonzales, 2019). Identified mitigating interventions to human risks in banks include: bank leadership (Lopez, 2019), improved human resources practices (Domingo and Bautista, 2020), cultural factors (Ortega, 2021; Dela Cruz, 2020), risk-aware culture (Marasigan and Cruz, 2022), and inclusive culture (Lopez, 2018).

Recommendations on the management of bank risks have been inferred by

researchers. Indrianto (2023) advanced the need to study the causes of fraud. Sanchez-Aguayo et al. advanced the inclusion of human behavior and data mining as relevant factors in bank risks analysis. Endriano (2022) advanced the use of qualitative refinements to such studies.

Gap Bridged by the Study

The primary gap is a research on bank risks hoped to be bridged by this study which is the local context of these risks in universal banks serving the domestic economy of a province. Understanding the underlying distinctive explanatory factors of such bank risks to be able to fully grasp the comprehensive dimensions for their management. That a robust and resilient bank risk management system is essentially

validated by how comprehensive these risks are understood, measured, and anticipated cannot be overemphasized.

Disaggregating the financial risks from the operational risks of universal banks provides a granular filter for their unique set of characteristics, therefore a more refined discernment of what, how and why an integrated bank risk management system may be developed, is another research gap addressed by this study. While there are separate divisions/responsible individuals designated to focus on financial risks and those on operational risks, a unified framework and core principles for both will easily build the risk management as a component of the banks' seal of good governance.

Identification of challenges to existing bank systems in the management of bank risks vis-à-vis the recommended strategies for addressing these challenges as defined by standard principles for maintaining financial and operational resilience of the banking industry. This combination of perspectives allows for a more open analysis and validation of anchors for the scientific outcomes of this study. This bootstrapping process is a gap this research bridges.

Respecting the inputs of all universal banks of the Province of Albay in recognition of their field-level experience across varying lengths of service, grants the primary data utilized as scaffolds for shaping the substance of this research, is a gap on pooling the private and public sector banks as equally credible stakeholders in developing a more robust framework for bank risk management. Said field level experience can validate what threats/risks continue to plague the banking industry, therefore can also help confirm what could tighten the banking system against threats and crimes from within and without individual universal banks.

Objectives of the Study

This study aimed to assess the strategies in managing financial and operational risks among universal banks in the Province of Albay to mitigate financial and operational risk. Specifically, it addresses the following specific objectives:

1. To determine the risk that universal banks have experienced along:
   - Financial
   - Operational;
2. To describe the strategies implemented by the Universal Banks in managing financial and operational risks,
3. To identify challenges faced by universal banks relative to financial and operational risks.
4. To recommend measures to mitigate the financial and operational risks.

METHODS

Research Design

This study employed a qualitative-descriptive research design, complemented by elements of grounded theory and developmental research. The descriptive design allowed the research to systematically examine the financial and operational risks experienced by universal banks in Albay Province. It provided a means to document observable patterns and conditions without manipulating the study environment. Grounded theory was incorporated to explore emerging themes from qualitative inputs, especially concerning the strategies used and the challenges encountered. Meanwhile, developmental research was applied in the formulation of a contextually relevant and enhanced risk management framework based on the study's findings. Collectively, these approaches provided a robust structure to achieve all four objectives:

identifying types and levels of risk, examining implemented strategies, uncovering operational challenges, and developing recommendations for improved risk management practices.

Population of the Study

The population of this study included all forty (40) universal bank branches in the Province of Albay, representing eleven (11) different financial institutions. These are Banco de Oro (BDO), Nank of the Philippine Islands (BPI), China Banking Corporation (CBC), Development Bank of the Philippines (DBP), East-West Bank (EWB), Land Bank of the Philippines (LBP), Metro Bank (MB), Philippine National Bank (PNB), Rizal Commercial Banking Corporation (RCBC), Security Bank (SB), and Union Bank (UB). Total enumeration was used, allowing comprehensive representation from the entire population. Each bank branch was represented by a key informant, typically a branch manager or an operations officer knowledgeable in the institution's risk management processes. To protect confidentiality, the identity of individual banks and branches was masked using randomly assigned codes such as Branch One to Branch Forty, and bank labels from UB1 to UB11.

Table 1

Universal Banks in the Province of Albay

Bank Branch	UB1	UB2	UB 3	UB4	UB5	UB6	UB7	UB8	UB9	UB10	UB11	**Total**
Legazpi	3	2	2	1	2	3	1	1	1	1	1	18
Old Albay	1	1			1		1					4
Daraga	1	1		1	1							4
Tabaco		1	1	1	1	1	1	1	1			8
Ligao		1	1		1							3
Polangui	1			1	1							3
Total	**6**	**6**	**4**	**4**	**7**	**4**	**3**	**2**	**2**	**1**	**1**	**40**

Research Instrument

Two instruments were developed to collect the required data. The first was a structured questionnaire designed to gather information on the types of financial and operational risks experienced, the bank's perceived level of exposure, and the effectiveness of the existing risk mitigation systems. This instrument also included sections on the strategies adopted and their adequacy.

The secondary data collection form was used to extract and document risk-related information from annual reports, incident logs, regulatory notices, and other archival sources relevant to the banks' experience of cyberattacks, fraud, and human-related risks.

NUMERICAL RATING	MEAN RATING	ADJECTIVAL DESCRIPTION
5	4.50-5.00	Very High Risk(VH)
4	3.50-4.49	High Risk (H)
3	2.50-3.49	Moderate Risk (M)
2	1.50-2.49	Low Risk (L)
1	1.00-1.49	Very Low Risk(VL)

Data Collection Methods

The research adopted a mixed methods approach that integrated both quantitative and qualitative techniques. Primary data were collected through a structured survey questionnaire. The survey focused on identifying and quantifying the financial and operational risks experienced by banks, as well as evaluating the systems in place to mitigate such risks. Secondary data were also utilized to validate and support the findings from primary sources. This included regulatory reports, annual bank risk disclosures, internal documentation on fraud and operational breaches, and court case records related to banking offenses.

Data Analysis

Quantitative data collected through the questionnaire were analyzed using descriptive statistics such as frequency distributions, percentages, and means. These statistics helped summarize the extent and patterns of risk exposure and strategy application across different bank branches. All quantitative data were processed using SPSS software.

Ethical Considerations

Ethical standards were strictly observed in the conduct of this study. Written informed consent was obtained from all participants after fully explaining the research objectives and procedures. The respondents' right to privacy and confidentiality was respected through anonymous coding of banks and branches. Furthermore, the researcher signed an affidavit pledging to uphold the ethical handling of all data collected. This document was made available to all participants as part of the ethical assurance process.

RESULTS AND DISCUSSION

This section presents the results and findings from the assessment of financial and operational risks among universal banks in the Province of Albay. The analysis covered the various types of financial and operational risks identified, the strategies implemented to manage these risks, and the challenges encountered. The discussion is structured based on the specific objectives outlined in the study, supported by relevant tables for clarity and precision.

Financial and Operational Risks Experienced by Universal Banks

Universal banks in Albay experience a range of financial and operational risks. These risks are broadly categorized into credit, market, liquidity, compliance, technological, and internal process risks. A comprehensive understanding of these risk profiles is critical for effective risk management and long-term financial stability.

Financial risk along Credit Risks

The findings in Table 2 indicate that, on average, universal banks experience relatively low levels of credit risk (WM = 2.22). This overall low risk rating reflects the effectiveness of existing credit evaluation systems under stable economic conditions. However, the data also revealed critical vulnerabilities during economic downturns, as evidenced by the high-risk score for the impact of economic downturns on credit exposure (WM = 3.87). This suggests that despite generally sound credit practices, external macroeconomic shocks remain a significant threat to financial stability. To address this, banks must prioritize dynamic credit scoring models and adaptive loan loss provisioning strategies that reflect the cyclical nature of the economy, thereby enhancing resilience against economic disruptions.

Table 2
Financial Risks along Credit

a. Credit Risk	WM	Interpretation
1. The bank's loan loss provisions are not adequate to cover potential defaults.	1.81	Low Risk
2. The current credit scoring system is not sufficient for borrowing evaluation	1.81	Low Risk
3. Loan restructuring strategies does not effectively mitigate credit risk	1.81	Low Risk
4. Economic downturns increase the bank's exposure to credit risk.	3.87	High Risk
5. The bank experiences a high number of load defaults.	1.81	Low Risk
6. Borrowers frequently delay loan repayments.	1.75	Low Risk
Average Weighted Mean	**2.22**	**Low Risk**

Furthermore, the consistently low risk in areas such as loan loss provisions (WM = 1.81) and credit scoring adequacy (WM = 1.81) indicate that these mechanisms are generally effective under stable conditions. However, these systems may be insufficient in rapidly changing financial environments, highlighting the need for continuous risk assessment and timely adjustments to credit policies.

Financial Risk along Market

Market risk, as presented in Table 3, poses a more substantial challenge, with a moderate overall risk level (WM = 2.72). This moderate risk is primarily driven by high exposure to stock market volatility (WM = 3.57) and interest rate fluctuations (WM = 3.42), both of which can significantly impact portfolio stability and profitability. The moderate risk level for foreign exchange rate volatility (WM = 3.08) further underscores the importance of comprehensive market risk management.

Table 3
Financial Risks along Market

b. Market Risk	WM	Interpretation
1. The bank does not actively adjust investment strategies based on the market trends.	1.97	Low Risk
2. Changes in stock market condition impact the bank's portfolio decision.	3.57	High Risk
3. Interest rate fluctuations significantly impact the bank's profitability	3.42	Moderate Risk
4. Foreign exchange rate volatility creates financial instability.	3.08	Moderate Risk
5. Inflation affects the bank's ability to manage assets and liabilities.	2.46	Low Risk
6. The bank lacks effective hedging strategies to manage market risks.	1.84	Low Risk
Average Weighted Mean	**2.72**	**Moderate Risk**

Given these findings, it is imperative for banks to implement real-time market analytics, diversify their investment portfolios, and adopt proactive hedging strategies to buffer against sudden market shifts. These measures can enhance financial stability and reduce vulnerability to market disruptions.

Financial Risks along Liquidity

As shown in Table 4, Liquidity risk, though generally low (WM = 1.92), presents significant challenges during periods of financial stress. The moderate risk score for sudden changes in deposit levels (WM = 2.63) indicates that banks must remain vigilant in managing their liquidity positions. Effective liquidity management, including regular stress testing and improved cash flow forecasting, is essential to prevent liquidity shortfalls during crises. This proactive approach not only ensures operational continuity but also builds market confidence, reinforcing the institution's financial stability.

Table 4
Financial Risks along Liquidity Risks

c. Liquidity Risks	WM	Interpretation
1. The bank does not effectively conduct liquidity stress testing.	1.97	Low Risk
2. Cash flow projection does not help in managing short-term obligations.	2.18	Low Risk
3. Sudden changes in deposit levels impact the bank's liquidity.	2.63	Moderate Risk
4. Unexpected withdrawals put financial strain on the bank.	1.84	Low Risk

5. The bank struggles to maintain adequate cash reserves.	1.53	Low Risk
6. The bank has difficulty balancing asset growth and liquidity requirements.	1.57	Low Risk
Average Weighted Mean	**1.92**	**Low Risk**

Operational Risk

Operational risks were likewise found to be moderate in some areas. Compliance, technological, and internal process-related risks were assessed.

Operational Risk Along Compliance and Regulatory

Table 5 presents the operational risks related to compliance and regulatory adherence are rated as moderate (WM = 2.08). This reflects challenges associated with frequent regulatory changes (WM = 2.61) and high compliance costs (WM = 2.50), which can strain financial performance. Although some areas, such as automated compliance monitoring (WM = 1.53) and employee awareness of regulations (WM = 1.53), are well-managed, the overall moderate risk level indicates ongoing pressures to maintain compliance. To mitigate these risks, banks should invest in automated compliance systems and continuous employee training to enhance regulatory alignment and reduce the risk of financial penalties.

Table 5
Operational Risk Along Compliance and Regulatory

a. Compliance and Regulatory Risk	WM	Interpretation
1. Frequent changes in banking regulations create compliance difficulties.	2.61	Moderate Risk
2. Compliance requirements are costly and impact profitability.	2.50	Moderate Risk
3. The bank lacks automated compliance monitoring systems.	1.53	Low Risk
4. Employees have limited knowledge of updated regulatory requirements.	1.53	Low Risk
5. The bank has faced penalties due to non-compliance in the past.	1.57	Low Risk
6. Regulatory audits often uncover unexpected risk areas.	2.76	Moderate Risk
Average Weighted Mean	**2.08**	**Moderate Risk**

Operational Risk Along Technological and Cybersecurity Risks

Table 6 highlights that technological and cybersecurity risks remain a significant concern, with a moderate overall risk level (WM = 2.50). Key risk areas include the need for stronger cybersecurity defenses (WM = 3.26) and outdated technological infrastructure (WM = 3.11), both of which can expose banks to

financial losses and reputational damage. Additionally, the moderate risk level for customer data security (WM = 2.71) emphasizes the need for stringent data protection measures. Investing in cutting-edge cybersecurity tools, regular infrastructure upgrades, and continuous staff training can substantially reduce these vulnerabilities, ensuring long-term operational resilience.

Table 6
Operational Risk Along Technological and Cybersecurity Risks

b. Technological and Cybersecurity Risks	WM	Interpretation
1. The bank has experienced cybersecurity threats (e.g. hacking, fraud).	2.26	Low Risk
2. Employees lack adequate training in cybersecurity best practices.	1.65	Low Risk
3. The bank's fraud detection systems need improvement.	2.00	Low Risk
4. Keep up with evolving cyber threats is a major challenge.	3.26	Moderate Risk
5. Customer data security measures need further enhancement.	2.71	Moderate Risk
6. Technological infrastructure needs upgrades to mitigate risks.	3.11	Moderate Risk
Average Weighted Mean	**2.50**	**Moderate Risk**

Operational Risk Along Internal Process and Human Error Risks

Table 7 shows the internal process and human error risks; Internal process inefficiencies and human errors also present moderate operational risks (WM = 2.30). High-risk areas include employee training gaps (WM = 3.21) and inconsistent procedural clarity, which can lead to costly mistakes and operational disruptions. Strengthening internal controls, enhancing process standardization, and fostering a risk-aware organizational culture are critical to minimizing these risks and improving overall operational efficiency.

Table 7
Operational Risk Along Internal Process and Human Error Risks

c. Internal Process and Human Error Risks	WM	Interpretation
1. Human errors frequently lead to operational inefficiencies.	2.87	Moderate Risk
2. The bank has faced losses due to internal fraud or misconduct.	2.13	Low Risk
3. There are gaps in the internal control system that increase operational risks.	2.16	Low Risk
4. Inadequate employee training leads to frequent procedural mistakes.	3.21	Moderate Risk

5. Risk management policies are not well-communicated to employees.	1.84	Low Risk
6. The bank lacks a strong incident response plan for operational failures.	1.61	Low Risk
Average Weighted Mean	**2.30**	**Moderate Risk**

Summary of Risk that Universal Banks have Experience

Table 8 provides a comprehensive summary of the financial and operational risks experienced by universal banks in Albay. It consolidates data from earlier tables, capturing average weighted mean (WM) scores across different risk categories, including credit, market, liquidity, compliance, technological, and internal process risks. This holistic perspective is crucial for understanding the overall risk landscape that these institutions navigate.

The assessment of financial risks revealed varying levels of concern across different categories. Credit risks, with a weighted mean (WM) of 2.22, indicate a generally low risk perception among universal banks in Albay. However, the elevated exposure to economic downturns (WM = 3.87) highlights a critical vulnerability that can significantly impact borrowers' repayment capacities. This disparity between low-risk elements like credit scoring

adequacy (WM = 1.81) and high-risk economic factors underscores the importance of robust stress testing and adaptive credit policies that can swiftly respond to macroeconomic shifts, enhancing portfolio resilience. Similarly, market risks present a moderate threat (WM = 2.72), driven by stock market volatility (WM = 3.57) and interest rate fluctuations (WM = 3.42). These elements can directly affect profitability and capital adequacy, necessitating dynamic portfolio management, effective hedging, and real-time market analytics to mitigate potential financial losses.

Table 8
Summary of Risk that Universal Banks have Experience

a. Financial	**WM**	**Interpretation**
1. Credit Risks	2.22	Low Risk
2. Market Risks	2.72	Moderate Risk
3. Liquidity Risks	1.92	Low Risk
b. Operational		
1. Compliance and Regulatory Risk	2.08	Low Risk
2. Technological and Cybersecurity Risks	2.50	Moderate Risk
3. Internal Process and Human Error Risks	2.30	Low Risk

Operational risks also vary, reflecting the diverse challenges faced by financial institutions. Compliance and regulatory risks are generally low (WM = 2.08) but are influenced by frequent regulatory changes (WM = 2.61) and high compliance costs (WM = 2.50), highlighting the need for robust compliance frameworks and automated monitoring systems
to reduce exposure. Technological and cybersecurity risks, with a moderate WM of 2.50, remain a critical concern due to the high-risk nature of outdated IT infrastructure (WM = 3.11) and cybersecurity vulnerabilities (WM = 3.26). This calls for continuous technological upgrades and rigorous cybersecurity measures to protect sensitive financial data. Lastly, internal process and human error risks (WM = 2.30) suggest a need for stronger internal controls, standardized processes, and continuous employee training to minimize the risk of operational disruptions.

The findings in Table 8 underscore the importance of a proactive and integrated risk management approach for universal banks in Albay. While many risk categories remain in the low to moderate range, specific high-risk elements, such as economic downturn exposure and cybersecurity threats, warrant immediate attention. Effective risk management strategies should encompass enhanced credit risk assessment frameworks that consider economic volatility, dynamic market risk management through real-time analytics and diversification, and strengthened liquidity buffers supported by contingency funding plans. Additionally, institutions must implement robust compliance systems to ensure streamlined regulatory adherence, invest in advanced cybersecurity measures to safeguard digital infrastructure, and promote continuous staff training to minimize human error and enhance operational efficiency.

Addressing these critical areas will help banks build a more resilient risk profile, ensuring financial stability and operational continuity in an increasingly complex financial landscape.

Strategies Implemented by the Universal Banks in Managing Financial and Operational Risks

This section presents the findings from a survey conducted on the implementation of risk management of universal banks in Albay. The study assessed the structure, tools, policies and reporting frameworks used by these institutions to manage financial and operational risks.

Strategies Implemented Along Risk Management Structure and Organization

The results in Table 1 indicate that all surveyed banks have dedicated risk management departments, demonstrating a foundational commitment to structure risk oversight. However, the variation in full-time staffing levels suggests significant differences in the scale and complexity of risk management operations. Smaller teams (1-5 employees) may struggle with comprehensive risk analysis, while larger teams (more than 15 employees) likely have greater capacity for proactive risk mitigation.

Table 9
Risk Management Structure and Organization

Metrics	Description	Observations
Dedicated Risk Management Department	Presence of a dedicated unit responsible for risk management	All banks have a dedicated risk management department, reflecting a foundational commitment to risk oversight.

Full-time Employees Dedicated to Risk Management	Number of staff fully dedicated to risk management functions	Majority have 1-5 employees, some have 6-10, and one bank reported over 15 employees, indicating varied levels of risk capacity.
Risk Committees	Specialized committees focused on different risk types	Includes CRC, MRC, ORI, ALCO, IT, and other specialized groups, reflecting a multi-layered approach to risk governance.
Frequency of Meetings	Regularity of committee meetings	Mostly monthly, with some reporting quarterly, weekly, or as-needed meetings, suggesting varying levels of risk oversight rigor.

The diversity in committee structures, including the presence of CRC, MRC, ORI, ALCO, and IT committees, indicates that banks recognize the need to address specific risk categories separately. However, the flexibility in meeting frequencies might indicate differing levels of risk maturity and responsiveness, potentially impacting the effectiveness of risk management strategies. Banks with smaller risk management teams may benefit from investing in training and technology to enhance their risk identification and response capabilities. More consistent committee meeting schedules could improve risk awareness and decision-making, reducing the likelihood of unforeseen financial shocks.

Strategies Implemented Along Risk Management Tools and Systems

Table 2 highlights the widespread use of specialized tools like credit scoring systems and cybersecurity monitoring platforms suggests that universal banks in Albay are investing in advanced technologies to strengthen their risk management frameworks. However, the differences in assessment frequency could be a reflection of varying levels of resource availability or differing organizational priorities regarding risk sensitivity.

Banks that assess risks less frequently may face challenges in promptly identifying emerging threats, potentially leading to delayed responses during critical situations. Regular assessments, supported by automated systems, are essential for maintaining robust risk profiles.

Table 10
Risk Management Tools and Systems

Metrics	Description	Observations
Risk Management Tools Used	Technologies and systems used for monitoring and mitigating risk	Includes CSS, MRA, ORI, CMS, CMT, and integrated

		platforms, reflecting a broad approach to risk management.
Frequency of Risk Assessments	How often risk assessments are conducted	Primarily monthly, with some banks conducting quarterly or as-needed assessments, indicating varying risk response agility.

Universal banks should consider adopting more frequent, real-time monitoring solutions to improve risk visibility and responsiveness. This approach can enhance operational resilience and reduce the likelihood of financial losses.

Strategies Implemented Along Risk Management Policies and Procedures

As shown in Table 11, frequent updates to risk management frameworks are essential for keeping pace with regulatory changes and evolving market dynamics. However, banks that rely heavily on manual communication methods may struggle to disseminate real-time updates, potentially leading to gaps in risk awareness. Embracing digital platforms can enhance the speed and consistency of policy communication, ensuring a more informed and prepared workforce.

Table 11
Risk Management Policies and Procedures

Metrics	Description	Observations
Framework Update Frequency	How often risk management frameworks are revised	Most banks update within 1-2 years, while a few update within 6 months, reflecting varying levels of regulatory alignment.
Policy Communication Methods	Channels used to communicate risk policies to employees	Includes internal circulars, intranet, online resources, and department meetings, indicating a mix of traditional and digital methods.

Banks that lag in updating their frameworks or rely heavily on manual communication methods may face compliance challenges and reduced agility in responding to emerging risks. Investing in more integrated communication platforms can help bridge this gap.

Strategies Implemented on Risk Reporting and Monitoring

The data in Table 12 show that regular risk reporting is a common practice, critical for maintaining financial stability. However, the absence of real-time metrics in some banks might limit their ability to anticipate and mitigate emerging risks effectively. Implementing real-time analytics could enhance risk foresight and strengthen decision-making processes.

To strengthen their risk management, banks should consider integrating real-time analytics and predictive risk models into their reporting frameworks, enhancing both transparency and responsiveness to emerging threats.

The study found that universal banks employ a variety of strategies to manage financial

Table 12
Risk Reporting and Monitoring

Metrics	Description	Observations
Frequency of Risk Reports	How often risk reports are generated	Primarily monthly, with some banks producing weekly or quarterly reports.
Recipients of Risk Reports	Key stakeholders receiving regular risk reports	Includes department heads, senior management, and risk committees, reflecting a structured approach to risk oversight.
Key Risk Metrics	Metrics used to track and measure risk levels	KRIs, KPIs, RTL, VaR, indicating a quantitative focus in risk assessment.

and operational risks, as detailed in Tables 9 to 12. These include structured risk management frameworks, regular risk assessments, and the use of advanced technological tools. However, variations in resource allocation and assessment frequency highlight potential gaps in risk response agility. Smaller institutions, in particular, may struggle to address complex risk scenarios effectively, underscoring the need for targeted investments in technology, training, and process automation.

Key findings include:

- All banks maintain dedicated risk management departments, though staffing levels vary widely.
- Banks employ a range of specialized tools, including credit scoring systems and cybersecurity platforms, but differ in their assessment frequencies.
- Policies are updated regularly, though some banks lag in adopting real-time communication methods.
- Risk reporting is typically conducted monthly, with most institutions focusing on key financial metrics like KRIs and KPIs.

Universal banks employ structured risk management practices, with all surveyed institutions maintaining dedicated departments. However, disparities in staffing and technological capability revealed unequal risk readiness. While most banks utilize tools like credit scoring systems and cybersecurity platforms, the frequency of assessments and reporting varies. Policies are updated regularly, though manual communication persists in some institutions, limiting agility. These strategies partially align with identified risks, but inconsistencies in implementation suggest room for improvement, particularly in real-time monitoring and automated compliance.

Challenges Faced by Universal Banks Relative to Financial and Operational Risks.

Table 13 presents the specific financial challenges encountered by universal banks in Albay. Key insights

from this table revealed that economic conditions significantly influence loan repayment, as evidenced by the high frequency (89.47%) of respondents identifying this as a critical challenge. This finding underscores the importance of macroeconomic stability in maintaining healthy loan portfolios. Additionally, while banks have implemented measures like creditworthiness assessments (78.95%) and loan restructuring (71.05%), the persistence of high default rates (63.16%) suggests potential gaps in these risk mitigation strategies. These gaps may be due to outdated credit evaluation tools or ineffective borrower monitoring, highlighting the need for more adaptive and real-time credit risk assessment systems.

Table 13
Challenges faced by Universal Banks Relative to Financial Risks

a. Credit Risk	**Frequency**	**Percentage**
1. Economic conditions influence loan repayment.	34	89.47
2. Policies and measures are in place for enforcing loan repayment.	31	81.58
3. Borrow creditworthiness is assessed using available tools.	30	78.95
4. Loan restructuring is part of risk mitigation.	27	71.05
5. Credit risk evaluation tools are used in decision-making.	26	68.42
6. The bank experiences loan defaults.	24	63.16
b. Market Risk		
1. Interest rate fluctuations affect financial performance.	30	78.95
2. Inflation affects financial planning and decision-making.	27	71.05
3. Stock market conditions impact investment strategies.	26	68.42
4. Foreign exchange rate changes influence financial stability.	25	65.79
5. Market risk analysis is conducted regularly.	25	65.79
6. The bank utilizes hedging strategies for market risks.	24	63.16
c. Liquidity Risk		
1. The bank manages cash reserves for liquidity.	28	73.68
2. Short-term liquidity planning is part of financial management.	28	73.68

3. Asset growth and liquidity are balanced in operation	27	71.05
4. Large withdrawals are considered in liquidity planning.	25	65.79
5. Emergency funding sources are identified.	21	55.26
6. Liquidity stress testing is conducted periodically.	20	52.63

Market risk challenges are also prominent, with interest rate fluctuations (78.95%) and inflation (71.05%) identified as key concerns. These factors directly impact financial planning and profitability, emphasizing the need for robust interest rate risk management and inflation hedging strategies. Regular market risk analysis and diversified investment approaches can help reduce exposure to these volatile elements.
Liquidity challenges, including short-term planning (73.68%) and balancing asset growth with liquidity (71.05%), reflect the ongoing struggle to maintain adequate cash reserves. This is critical, as liquidity shortages can quickly escalate into solvency crises, particularly during periods of economic stress. Effective liquidity management frameworks, including stress testing and contingency funding plans, are essential to mitigate these risks.

Challenges faced by Universal Banks Relative to Operational Risks

Table 14 focuses on the operational risks faced by universal banks, highlighting significant vulnerabilities in compliance, technology, and internal processes. The high frequency of regulatory challenges (65.79%) reflects the ongoing pressure to adapt to evolving regulatory standards. This challenge is compounded by the financial burden of compliance (47.37%) and the risk of penalties for non-compliance (23.68%). To address these issues, banks should invest in automated compliance systems and continuous training to reduce the cost and complexity of regulatory adherence.

Table 14
Challenges faced by Universal Banks Relative to Operational Risks

a. Compliance and Regulatory	Frequency	Percentage
1. Keeping up with new regulatory requirements.	25	65.79
2. Frequent changes in banking regulations make compliance difficult.	24	63.16
3. Audit often reveal risk management gaps.	22	57.89
4. High costs associated with compliance affect profitability.	18	47.37
5. Bank has faced penalties due to regulatory non-compliance.	9	23.68
6. Employees lack sufficient training on compliance rules.	8	21.05

b.	**Technological & Cybersecurity**		
1.	Fraud detection systems need significant improvement.	18	47.37
2.	The bank has experienced cybersecurity threats (e.g., hacking, fraud).	17	44.74
3.	Keep up with evolving cyber threats.	16	42.11
4.	IT infrastructure is outdated and requires upgrading.	9	23.68
5.	Employees are not adequately trained in cybersecurity.	7	18.42
6.	Data protection policies are not strictly enforced.	4	10.53
c.	**Internal Process and Human Error**		
1.	Internal fraud or misconduct poses a major risk.	25	65.79
2.	Employee errors frequently lead to financial losses.	24	**63.16**
3.	Incident response plans are established and updated.	21	**55.26**
4.	Inefficiencies in internal processes affect operation.	18	47.37
5.	Risk management policies are not consistently followed by staff.	8	21.05
6.	Decision-making is delated due to unclear risk management protocols.	8	21.05

Technological and cybersecurity challenges are also critical, with nearly half of the respondents (47.37%) citing inadequate fraud detection systems and 44.74% reporting past cybersecurity incidents. These findings indicate a pressing need for advanced cybersecurity infrastructure and real-time threat detection capabilities to protect sensitive customer data and prevent financial losses. Regular system upgrades and comprehensive cybersecurity training can significantly reduce these vulnerabilities.

Internal process weaknesses, such as internal fraud (65.79%) and procedural inefficiencies (47.37%), further exacerbate operational risk. Addressing these issues requires robust internal controls, regular audits, and a strong organizational culture that prioritizes risk awareness and process integrity.

The challenges faced by universal banks, as outlined in Tables 13 and 14, include economic instability, regulatory pressure, and technological vulnerabilities. Overcoming these challenges requires a comprehensive risk management approach that integrates strategic planning, continuous training, and technological innovation.

Recommended Measures to Mitigate Financial and Operational Risks

Informed by the empirical findings, grounded theory analysis, and theoretical anchoring in the Fraud Dia

mond Theory (Cressey, 1953; Wolfe & Hermanson, 2004), this section presents actionable, evidence-based recommendations aimed at improving the risk management systems of universal banks in Albay. These recommendations respond to the identified financial and operational risks and integrate the core elements of opportunity, pressure, rationalization, and capacity that underpin fraud vulnerability.

To mitigate financial risks, the study proposed the following: In the area of credit risk, where high vulnerability during economic downturns was observed, banks should adopt dynamic credit risk models powered by artificial intelligence that integrate macroeconomic indicators and borrower behavior analytics. This must be aligned with Basel III guidelines on dynamic provisioning and stress testing. In terms of market risk, where exposure to interest rate and stock market volatility was significant, banks are encouraged to implement hedging strategies and apply Value-at-Risk (VaR) analysis. The integration of real-time market intelligence tools can further enable proactive responses to market fluctuations. On liquidity risks, moderate challenges in deposit fluctuations demand a robust liquidity contingency plan, predictive cash flow forecasting, and diversified emergency funding sources.

Operational risk mitigation is equally essential. For compliance and regulatory risks, the implementation of regulatory technology (RegTech) can automate compliance updates, reduce human error, and improve responsiveness to regulatory changes. This must be supported by continuous employee training programs focused on AML regulations and data privacy

standards. Technological and cybersecurity risks necessitate infrastructure upgrades to meet ISO/IEC 27001 standards and the deployment of integrated fraud detection systems capable of real-time threat identification and response. These measures are crucial, especially in the context of increasing phishing and ransomware attacks. Internal process risks, such as human error and procedural inefficiencies, require organization-wide enterprise risk management (ERM) training. Promoting a risk-aware culture and embedding incident response protocols are critical steps toward minimizing operational disruptions.

Based on the findings the following recommendations are proposed:

1. **Strengthening Credit Risk Management:**
   - Implement more stringent credit evaluation processes and adaptive credit scoring models.
   - Regularly adjust provisioning strategies to align with economic conditions.
   - Increase the frequency of risk assessments for early detection of emerging credit issues.
2. **Enhancing Market Risk Resilience:**
   - Adopt dynamic investment strategies and real-time market monitoring tools.
   - Utilize financial derivatives and hedging strategies to manage interest rate and currency risks.
   - Conduct scenario-based stress tests to evaluate market shock impacts.
3. **Improving Liquidity Management:**
   - Strengthen cash flow forecasting and liquidity stress testing.
   - Establish contingency funding plans to reduce reliance on volatile deposits.
4. **Advancing Cybersecurity and Technological Infrastructure:**
   - Invest in modern cybersecurity tools and continuous employee training.
   - Regularly update IT infrastructure to address evolving threats.
5. **Enhancing Compliance and Regulatory Risk Management:**
   - Implement automated compliance monitoring systems.
   - Conduct ongoing regulatory training for staff.
6. **Strengthening Internal Process Controls:**
   - Develop comprehensive internal control frameworks.

- Foster a risk-aware culture through continuous training.

These recommendations aim to enhance the overall risk management framework of universal banks, ensuring financial stability and operational resilience in a rapidly changing economic landscape.

Conclusion

This study comprehensively assessed the strategies employed by universal banks in the Province of Albay in managing financial and operational risks. The findings revealed that universal banks experience varying degrees of risk across different categories. Financial risks, particularly credit, market, and liquidity risks, were generally perceived to be low to moderate, with notable vulnerabilities emerging during economic downturns and periods of market volatility. Operational risks, including compliance and regulatory pressures, technological and cybersecurity threats, and internal process inefficiencies, also presented moderate challenges. These findings indicate that while current systems are functional under stable conditions, there are critical gaps during times of stress that warrant closer attention.

With regard to the strategies implemented, the study found that all universal banks maintain dedicated risk management departments and employ a range of tools, policies, and monitoring frameworks. However, the variation in staffing, frequency of risk assessments, and level of technological integration suggests disparities in risk management maturity among institutions. While some banks utilize real-time monitoring systems and maintain frequent committee meetings, others rely on manual processes and less frequent evaluations, potentially limiting their responsiveness to emerging risks.

The study also identified several challenges that hinder effective risk management.

Economic instability was seen as a major driver of loan defaults, while fluctuations in interest rates and inflation posed risks to financial planning. On the operational side, frequent regulatory changes, high compliance costs, cybersecurity vulnerabilities, and human errors were consistently highlighted. These challenges emphasize the need for more adaptive, technology-driven, and human-centered risk management approaches to strengthen institutional resilience.

In response to these findings, the study proposed several measures to mitigate financial and operational risks. Key recommendations include adopting dynamic credit scoring models that adjust to macroeconomic shifts, implementing market risk hedging strategies supported by real-time analytics, and enhancing liquidity planning through predictive cash flow forecasting and emergency funding strategies. On the operational side, the integration of regulatory technology (RegTech), continuous employee training, infrastructure upgrades, and the development of a risk-aware organizational culture were recommended to address compliance, cybersecurity, and internal process risks.

Recommendations for Further Study

1. **Comparative Study Across Regions:** Extend the scope beyond Albay to compare risk management practices across other provinces or regions.
2. **Post-Implementation Evaluation:** Conduct a follow-up study to assess how banks implement and benefit from the recommended strategies (e.g., RegTech, AI-based credit models).
3. **Impact of Digital Banking Transformation:** Explore how digitalization and fintech integration are reshaping risk landscapes in universal banking.
4. **Staff Competency and Culture:** Investigate how organizational culture and staff competencies influence risk awareness, reporting, and mitigation success.

5. **Cost-Benefit Analysis of Risk Mitigation Tools:** Assess the financial and operational returns on investments in cybersecurity infrastructure, training, or automated systems.

References

1. AFC Ecosystem. (2024). Fortifying against financial crime. How to tackle the critical AML challenges in the philippines. https://www.afcecosystem.org /fortifying-against-financial-crime-in-the-philippines
2. ASEAN+3 Macroeconomic Research Office (AMRO). (2023, December 5) ASEAN +3 financial stability report 2023: Navigating high debt in low visibility. https://amro-asia.org/navigating-high-debt-in-low-visibility-in-asean3/
3. ARAI.(2024, August 8). Average data breach cost in ASEAN climbs to all-time high. Business World Online. https://www.bworldonline.com/technology/2024/ 08/08/612668/
4. Azba, S. (2024). From suspicion to trust: Evaluating banks' fraud management through customer lens: An Investigation of Meezan Bank in Pakistan.(Master's) Thesis. Uppsala University. 2024-04-29.
5. Balita, C. (2023, August 23). Number of phishing attacks Philippines 2021-H1 2022. Statista. https://www.statista.com/statistics/1349352/philippines-number-of-phishingattacks/#:~:text=The%20number%20of%20phishing%20attacks, 1.34%20million%20attacks%20in%202021.
6. Balita, C. (2023,December 21). Cybersecurity and cybercrime in the Philippines - statistics & facts. Statista https://www.statista.com/topics/11332/cybersecurity-and-crime-in-the-philippines/#topicOverview
7. Batalla, E. V.C. (2020, July 2). Grand corruption scandals in the Philippines. Public Administration and Policy: An Asia-Pacific Journal. ISSN: 2517-679X.
8. Bangko Sentral ng Pilipinas (BSP). (2025). ASEAN economic community (AEC) 2025:
9. Financial integration in ASEAN. https://www.bsp.gov.ph/Media_and Research/Primers
10. Bangko Sentral ng Pilipinas (BSP). (2021). 1st semester 2021 banking sector outlook survey. Supervisory Policy and Research Department, Financial Supervision Sector,https://www.bsp.gov.ph/Media_And_Research/PBSOS/PBSOS_ 1s2021.pdf
11. Bangko Sentral ng Pilipinas (BSP). (2018). 101 classifications, powers, and scope of authorities of banks, Manual of regulations of banks.https://www.bsp.gov.ph
12. Bangko Sentral ng Pilipinas (BSP).(2018) 101-classifications-powers-and-scope-of-authorities-of-banks/https://mor.bsp.gov.ph.
13. Braithwaite, J. (2022). Macrocriminology and freedom: Why incapacitation trumps deterrence. ANU Press. https://www.jstor.org/stable/j.ctv2bks5gq.15
14. Capule, E.O. (Ed). (2023). Banking laws of the Philippines: The laws on secrecy of bank deposits, a legal primer. https://www.bsp.gov.ph/Media_and_Research/Primers%20Faqs/Primer_on_Bank_Secrecy.pdf
15. Carpio, J. (2019, January 16). Bank of the Philippine Island and Ana C. Gonzales, petitioners, vs. Spouses Fernando V. Quiaoit and Nora L. Quiaoit, respondents. (G.R. No. 199562).Official Gazette, 115 (3) 845-857.https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/1/64895
16. Corporate Finance Institute, (2024). What are major risks for banks? https://corporatefinanceinstitute.com/resources/career-map/sell-side/risk-management/major-risks-for-banks.

17. Casucian, J. A. C. (2024)/ AMLC to probe Alice Guo's alleged P23-M downpayment for Baguio Property. GMA Integrated News. https://www.gma network.com/news/topstories/nation/921045/
18. De Vera, B. O. (2022, January 18). P2 billion feared lost to scams, fraud – BSP. Philippine Daily Inquirer. https://business.inquirer.net/338991/p2b-feared-lost-to-scams-fraud-bsp
19. FICO Proprietary Research. (2023). 2023 scams impact survey: Philippines Exploring the consumer impact of unauthorized push payment scams. https://www.fico.com/en/latest-thinking/ebook/2023-scams-impact-survey-philippines
20. Fisher, K. (2015). The psychology of fraud: What motivates fraudsters to commit crime? (Graduate thesus, Texas Women University. https://download.ssrn.com/ 15/04/20/ ssrn_id2596825_code2218697.pdf
21. Gabordi, J.M.C., Razote, R.B.C. (2020). Systemic risk of the Philippines: Application of the SRisk risk measure to top Philippine banks. https://www.researchgate.net/publication/358128324
22. Bangko Sentral ng Pilipinas(BSP). (2025). ASEAN Economic Community (AEC) 2025:
23. Financial integration in ASEAN. https://www.bsp.gov.ph/Media_and_Research/Primers
24. Hermanson, D.R., Wolfe, D.T. (2024, June 10). The fraud diamond: A 20-Year retrospective. The CPA Journal: The Voice of the Profession. .https://www.cpajournal.com/2024/06/10/the-fraud-diamond/
25. Hussain, A. and Anees, A. (2022, December 31). Impact of fraud risk management on bank performance with moderating role of risk culture. Journal of Business Education and Management. ISSN (Online): 2790-81.
26. Institute of Internal Auditors(IIA. (2015). Mitigating fraud in Philippine organizations: Best practices, challenges and opportunities. https://iia-p.org/wp-content/uploads/2020/02/White_Paper_ Mitigating Fraud _Philippines-v4.pdf
27. Indrianto, D., Young, J.A., Ng, N. (2022). Fraud risk management approach to deterrence fraud at banks in Indonesia. Sinomics Journal, Vol. 1 (5). https:www.sinomicsjournal.com
28. Kital. (2024). Understanding cyber security in the banking sector. https://www.kital.com.ph/ cybersecurity -in-banking/
29. Laila, N. N., Prasetyo, D., & Winarno. (2024) ASEAN banking industry performance analysis. Diponegoro International Journal of Business, 6, (2), 128-141.
30. Leonen. S.A.J.(2022,June) G.R. No. 207078. Supreme Court E-Library. https://elibrary.judiciary.gov.ph/search
31. LogicManager (2023 September 19). Risk management in banking: Introduction, risk management in banking [Complete Guide]. https://www. logicmanager. com /resources/erm/risk-management-in-banking/
32. Mabior, M.M. & Wanyama, K.W. (2024). Role of forensic investigations in reduction of financial fraud among commercial banks in South Sudan. International Journal of Finance and Accounting, Volume 3,(1). https://doi.org/10.37284/ iijfa.3.1.1645
33. Machado, M.R.R., & Gartner, I.R. The Cressey hypothesis (1953) and an investigation into the occurrence of corporate fraud: An empirical analysis conducted in Brazilian banking institutions.https://doi.org/: 10.1590/1808-057x201803270
34. Moore, J. (2020). Occupational fraud models: A comparative analysis and proposed expanded model. International Journal of Accounting Research, 8:203. doi:10.35248/2472-114X.20.8.203
35. Noble, L. W. T, (2022, April 29). Central bank sanctions BDO, UnionBank over online fraud incident. Business World. https://www.bworldonline.com/top-stories/2022/04/29/445420/

36. PCIEERD. (2023). DOST-PCIEERD highlights 11 completed data science and analytics R & D projects for good governance. https://pcieerd.dost.gov.ph/news /latest-news/541-dost-pcieerd-highlights-11-completed-data-science-and-analytics-r-d-projects-for-good-governance
37. Phiri, J., Lavhengwa, T. & Segooa, M.A., (2024), 'Online banking fraud detection: A comparative study of cases from South Africa and Spain', *South African Journal of Information Management* 26(1), a1763. https://doi.org/10.4102/sajim.v26i1.1763
38. Pociumban, A. (2023). Moldova's vulnerabilities – the targets of hybrid attacks: A learning-by-doing strategy. Hague Centre for Strategic Studies.https://www.jstor.org/stable/resrep34686
39. PwC. (2020). Fraud and economic crime: Are we prepared enough for a new decade? https://www.pwc.com/ph/en/consulting/consulting-publications/fraud-and-economic-crime-survey.html
40. Quadir, S. (2019, January 30). Bangladesh to sue Manila bank over $81million cyber heist: Central bank governor. Reuters January 30, 2019. https://www.reuters.com/article/technology/bangladesh-to-sue-manila-bank-over-81-million-cyber-heist-central-bank-governor-idUSKCN1PO19F/
41. Rastogi, V. et al.(2022) Journal of vulnerabilities. Journal Studies, 8(1):28 https://doi.org/10.1186/s43093-022-00146-4
42. Sánchez-Aguayo, M.; Urquiza-Aguiar, L.; Estrada-Jiménez, J. (2021) Fraud detection using the fraud triangle theory and data mining techniques: A literature review.*Computers* , *10*, 121. https:// doi.org/10.3390/computers10100121
43. Setyarini, E. et al. (2024). Evaluation of risk management strategies in profit optimization in the banking sector. International Journal of Social and Education (INJOSEDU), 1(6) 1555-1567 .https://hal.archives-ouvertes.fr/hal-04162475
44. ` ``````````````````
45. Suryandari, N. N. A., Yadnyana, I. K., Ariyanto, D., & Erawati, N. M. A. (2023). Implementation of fraud triangle theory: A systematic literature review. Journal of Governance & Regulation, 12(3), 90–102. https://doi.org/10.22495/jgrv12i3art10
46. Statista. (2024). Average cost of a data breach in the United States, 2006-2024. https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/
47. Statista. (2024, September 18). Online data breach density APAC 2021-2022, by country. Statista Research Department, https://www.statista.com/statistics/ 1400323/apac-online-account-breach-density-by-country/
48. Syadullah, M. (2018). ASEAN banking efficiency review facing financial services liberalization: The Indonesian perspective. Asian Development Policy Review. 6(2), https://. www.aesaweb.com
49. Tijam, J. (2018). Bank of the Philippine Islands, Petitioner, Vs. Land Investors and Developers Corporation, Respondent(G.R. No. 841 Phil. 534) Supreme Court e-Library, ***https://elibrary.judiciary.gov.ph/thebookshelf /showdocs/1/64811***
50. Tirumalaraju, N. (2024). Analyzing the fraud tendency in the Indian banking sector. Journal of Management Research and Analysis, 11(3):168-175.
51. Tsang, A. (2022). Stress testing Philippine bank resilience in the post-pandemic era. Asean Macroeconomic Research Office. https://amro-asia.org/stress-testing-philippine-bank-resilience-in-the-post-pandemic-era/
52. Tupas, E. (2023, December 20). Online scams top list of 2023 cybercrimes. The Philippine Star, https://www.philstar.com/headlines/2023/12/20/2320172/online-scams-top-list-2023-cybercrimes

53. Villanueva, J. (2022, May 12). Fraud monitoring system for financial institutions now required. https://www.pna.gov.ph/articles/1174309
54. Wang, Y., et al. (2024, July 15). What explains the operational efficiency of listed commercial banks in China? Evidence from a three-stage DEA-tobit modeling analysis. Heliyon, 10(13), e337161
55. Weber, O. (2024, February). Climate stress testing in the financial industry. Current Opinion in Environmental Sustainability. 66, 101401
56. Yoganandham, G. (2024). Economic consequences of cyber fraud in online banking and credit card transactions – A theoretical assessment. https://www.researchgate.net/publications/385012122
57. ASEAN +3 Macroeconomic Research Office (AMRO). (2023, December 5). ASEAN+3 financial stability report 2023: Navigating high debt in low visibility. . https://amro-asia.org/navigating-high-debt-in-low-visibility-in-asean3/
58. Bangko Sentral ng Pilipinas (BSP). (2021). 1st Semester 2021 banking sector outlook survey. Supervisory Policy and Research Department, Financial Supervision Sector,https://www.bsp.gov.ph/Media_And_Research/PBSOS/PBSOS_ 1s2021.pdf
59. Bangko Sentral ng Pilipinas (BSP). (2025). ASEAN Economic Community (AEC) 2025:
60. Financial integration in ASEAN.https://www.bsp.gov.ph/Media_and_
61. Research Primers.
62. Greenberg, S., & Travis M. (2025). How good is Elon Musk at predicting the future? And what would it take to become an accurate predictor, yourself? Clearer Thinking.Org. https://www.clearerthinking.org /post/how-good-is-elon-musk-at-predicting-the-future-and-what-would-it-take-to-become-an-accurate-predict
63. Gregory, J. (2025). Making smart cybersecurity spending decisions in 2025. IBM.https://www.ibm.com/think/insights/making-smart-cybersecurity-spending-decisions-in-2025
64. Laila, N. N., Prasetyo, D., & Winarno. (2024) ASEAN banking industry performance analysis. Diponegoro International Journal of Business, 6 (2), 128-141.
65. LogicManager (2023, September 19). Risk management in banking: Introduction, risk management in banking [Complete Guide]. https://www. logicmanager. com /resources/erm/risk-management-in-banking/
66. Syadullah, M. (2018). ASEAN banking efficiency review facing financial services liberalization: The Indonesian Perspective. Asian Development Policy Review. l. 6(2), 88-99. https://www.aesaweb.com
67. Tsang, A. (2022). Stress testing Philippine bank resilience in the post-pandemic- era. ASEAN Macroeconomic Research Office. https://amro-asia.org/stress-testing-philippine-bank-resilience-in-the-post-pandemic-era/
68. Wang, Y., et al. (2024, July 15). What explains the operational efficiency of listed commercial banks in China? Evidence from a three-stage DEA-tobit modeling analysis. heliyon, 10.(13), e337161