Discovery

1. The Company existed a pplication and services

AsePay had launch of own product in Australia. It supports only **simple money transfer from bank to account** and **may issue virtual debit cards and make payments**. Company is planning to **support cryptocurrencies** in the future.

2. User Onboarding and KYC

A good onboarding screen should include the following characteristics:

1. Long user tutorials should be avoided. The tutorial's purpose is to explain why the user requires the program.
2. Bring the consumer up to speed gradually, and don't expect them to recall everything right once.
3. Use UI suggestions to guide new users through the app. Such indications should be presented to the user at the precise moment when they are required.
4. While keeping the application screen visible, highlight essential portions of the program. Users will be able to quickly locate the functionality they require in this manner.

Know Your Customer (KYC)

regulations in South American countries. Aim for a process that can be **completed within 5 minutes**, accommodating users with limited internet access.
KYC refers to the process of verifying the identity of customers and understanding their business activities. Financial institutions are required by law to implement KYC procedures, which are designed to:

- Ensure customers are not involved in **illegal activities, such as money laundering or terrorism financing.**
- Mitigate risks associated with **non-compliant customers or false identities.**
- Comply with regulatory **requirements and avoid sanctions or fines from regulators.**

KYC typically involves the following steps:

1. **Customer Identification:** Collecting basic information about customers, such as their name, date of birth, address, and identification number:
   1.1. **Identification Document:** A valid government-issued identification document, such as a **national ID card, passport, or driver's license**. The document **should contain the individual's full name, photograph, date of birth, and a unique identification number.**

1.2. **Proof of Address:** A document verifying the customer's address, such as a recent **utility bill (gas, electricity, water, phone)**, **property tax receipt, or bank statement.** The document should display the individual's name and residential address and be issued **within the past 3-6 months.**
1.3. **Tax Identification Number (TIN)**: A Taxpayer ID number or equivalent, such as **Brazil's CPF (Cadastro de Pessoas Físicas) or Argentina's CUIT (Código Único de Identificación Tributaria)**, which helps in tracking financial transactions and tax compliance.
1.4. **Proof of Income or Occupation:** Documents that demonstrate the individual's **source of income, employment, or occupation, such as recent payslips, tax returns, or an employment contract.** For self-employed individuals, **business registration documents or licenses might be required.**

2. **Identity Verification:** Validating the identity of customers by checking their provided information against reliable, independent sources (e.g., government-issued ID or identity database).
3. **Risk Assessment:** Analyzing the potential risks associated with customers based on their background, occupation, transactional behavior, and other factors. This step may involve assigning risk ratings to customers and applying different levels of due diligence based on these ratings.
4. **Ongoing Monitoring:** Continuously monitoring customer relationships and transactions to ensure that they remain consistent with their risk profile and to detect any potential red flags or suspicions of illicit activities.

For corporate clients or businesses, additional documents might include:

1. **Company Identification Number:** A government-issued registration number that identifies the legal entity, such as a National Taxpayer Registry Number or an equivalent identifier from the respective country.
2. **Certificate of Incorporation:** A document issued by the responsible local authority that confirms the registration of the legal entity.
3. **Articles of Association or Bylaws:** These legal documents outline the company's structure, objectives, and governance rules.
4. **Shareholder and Beneficial Ownership Information:** Documentation of the company's shareholders, board members, and ultimate beneficial owners.
5. **Power of Attorney or Authorization:** If a company representative is acting on behalf of the business, a valid power of attorney or authorization document should be provided.

Know Your Transaction (KYT)

KYT refers to the process of monitoring, analyzing, and understanding the transactions made by customers within the financial system. The objective of KYT is to:

- Detect suspicious transaction patterns, anomalies, or inconsistencies that may indicate **money laundering, terrorist financing, or other illicit activities.**
- Enable efficient reporting of s**uspicious transactions to relevant authorities.**

- Aid in building a more comprehensive risk assessment of customers based on their transactional behavior.

KYT typically involves the following steps:

1. **Transaction Monitoring:** Continuously monitoring transactions conducted by customers and comparing them against established baselines, thresholds, or expected behavior.
2. **Red Flag Identification:** Identifying red flags or unusual patterns in customer transactions, such as **unusually large or frequent transactions, round-dollar transactions, transactions involving high-risk countries**, or sudden deviations from typical behavior.
3. **Investigation and Reporting:** Conducting further investigations in case of suspicious or unusual transactions and reporting them to the appropriate **regulatory authorities**, as required by law.

Data protection/privacy laws

Argentina: Argentina's "Ley de Protección de los Datos Personales No. 25.326" (Personal Data Protection Law) is similar to the GDPR, governing the collection, processing, and use of personal data. Argentina's law is one of the strictest in the region, offering a high level of data protection.

Brazil: The "Lei Geral de Proteção de Dados" (LGPD) is Brazil's data protection law, which came into effect in August 2020. It shares many similarities with GDPR, such as requiring a legal basis for processing personal data, appointing a data protection officer, and implementing appropriate security practices.

Chile: Chile has the "Ley No. 19.628 sobre protección de la vida privada" (Law No. 19,628 on the Protection of Privacy). This law regulates the handling of personal data in the country, protecting individual privacy rights. Although it shares some key principles with GDPR, Chile's law is less comprehensive than that of Brazil or Argentina.

Colombia: Colombia's main data protection legislation is "Ley Estatutaria 1581 de 2012" (Statutory Law 1581 of 2012), which covers the collection, processing, storage, and other uses of personal data. The law is built on data protection principles similar to GDPR, but it is less extensive.

Peru: Peru's "Ley No. 29733 – Ley de Protección de Datos Personales" (Law No. 29733 - Personal Data Protection Law) controls the handling and protection of personal data. While sharing some aspects with GDPR, the Peruvian law is less extensive and less detailed in its approach to data protection.

1. Develop and implement a data privacy policy: Create a comprehensive data privacy policy outlining the procedures and measures your organization will take to ensure the

protection of PII. The policy should align with the data protection regulations of the South American countries where you operate.

2. Identify all PII that your business processes: Locate and document all the PII your organization collects, stores, processes, and transmits, along with its sources and the purposes for which it is used.

3. Map the data flows: Identify and document how PII flows through your organization, including both internal and external data transfers. This documentation will help you effectively manage and secure PII.

4. Implement appropriate security measures: Implement physical, technical, and administrative security controls to protect PII and maintain compliance with local regulations. This includes access controls, encryption, secure disposal of data, and employee training.

5. Develop a data breach response plan: Create and test a response plan outlining the steps your organization will take in the event of a security breach that compromises PII. This should include timely notifications to affected individuals and regulatory authorities, as required by local laws.

6. Conduct regular risk assessments: Periodically assess your organization's information security risks to identify any potential vulnerabilities and make improvements to security practices, systems, and applications.

7. Establish data subject rights procedures: Implement processes enabling data subjects to exercise their rights under the applicable data protection laws, including access to their data, rectification, deletion, and data portability. Inform data subjects about these rights and how to exercise them.

8. Assign a privacy officer or team: Appoint a designated privacy officer or team responsible for managing your organization's data privacy efforts, ensuring compliance, and staying informed of any changes or updates to local data protection regulations.

9. Monitor and review compliance: Conduct internal audits and regular reviews to evaluate your organization's data privacy practices and adherence to the relevant data protection laws in South America. Implement any necessary changes to maintain compliance.

10. Obtain expert guidance: Coordinate with legal counsels or consult specialized data privacy professionals for guidance on navigating the complexities of the data protection laws in South American countries as they pertain to your organization.

3. Payment and Transaction Features

1. In South America, businesses dealing with payment card transactions must follow **PCI DSS** standards to ensure the security of the payment card data they handle.
   PCI DSS applies to businesses in South America as well, and they must comply with these standards when handling cardholder data to reduce the risks of card fraud and secure sensitive payment information.

   The **Payment Card Industry Data Security Standard (PCI DSS)** consists of **12 core requirements** organized into **six control objectives (goals)**. Here are the six control objectives, along with the corresponding requirements:

   1. **Build and Maintain a Secure Network and Systems**
      1.1. **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data.
      1.2. **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters.
   2. **Protect Cardholder Data**
      2.1. **Requirement 3:** Protect stored cardholder data.
      2.2. **Requirement 4:** Encrypt transmission of cardholder data across open, public networks.
   3. **Maintain a Vulnerability Management Program**
      3.1. **Requirement 5:** Protect all systems against malware and regularly update anti-virus software or programs.
      3.2. **Requirement 6**: Develop and maintain secure systems and applications.
   4. **Implement Strong Access Control Measures**
      4.1. **Requirement 7**: Restrict access to cardholder data by business need to know.
      4.2. **Requirement 8:** Identify and authenticate access to system components.
      4.3. **Requirement 9:** Restrict physical access to cardholder data.
   5. **Regularly Monitor and Test Networks**
      5.1. **Requirement 10:** Track and monitor all access to network resources and cardholder data.
      5.2. **Requirement 11:** Regularly test security systems and processes.
   6. **Maintain an Information Security Policy**
      6.1 **Requirement 12:** Maintain a policy that addresses information security for all personnel.
2. Propose a comprehensive set of payment features:
   1.1. peer-to-peer transfers
   1.2. bill payments
   1.3. mobile recharges
3. Consider supporting popular local payment methods:
   2.1. **Pix** in Brazil: Pix users can make transactions from one bank to another or between

different accounts at the same bank. Pix payments can also be used for offline and online purchases, for bill payments, and even for tax and government fees payments. To make a Pix transfer, users need either a key (a phone number, email address, tax ID number, or random key linked to their bank account)
2.2. **UPI** in Argentina (is not working). Suggested **"Transferencias Inmediatas (Immediate Transfers)"** or **"TI"** managed by COELSA (Cámara Electrónica de Compensación y Liquidación de Efectivo S. A). This system allows bank customers to make immediate interbank transfers electronically.

When implementing a new digital bank in countries like Brazil and Argentina, it is crucial to consider supporting popular local payment methods. This allows for easier adoption by the local population and helps ensure the bank's competitiveness in the market. Integrating these payment methods requires strategic planning, technical implementation, and compliance with local regulations. Here is an outline of key steps to consider while supporting Pix in Brazil and UPI in Argentina:

1. **Market Research and Strategy**: Begin by conducting extensive market research to understand the popularity and usage patterns of the local payment methods (Pix in Brazil and UPI in Argentina). Assess the feasibility and potential benefits of integrating these payment options into your digital bank.

2. **Partnerships and Collaborations**: Establish partnerships with local financial institutions, payment service providers, and payment processors that have expertise in the local payment methods. These partnerships can provide valuable insights, reduce implementation barriers, and facilitate smoother integration.

3. **Regulatory Compliance**: Familiarize yourself with the local legal and regulatory frameworks governing the use of these payment methods, including licensing requirements, transaction limits, anti-money laundering (AML) and know-your-customer (KYC) guidelines, and financial reporting.

4. **Technical Integration**: Develop and implement secure, reliable technical infrastructure that allows customers to use these local payment methods within your digital bank platform. This can involve integrating APIs provided by partner institutions or payment processors, implementing authentication and authorizing mechanisms, and ensuring all systems are aligned with the local payment standards.

5. **Testing and Quality Assurance**: Thoroughly test the functionality and performance of the local payment method integrations to identify and resolve any issues before launch. Perform end-to-end testing to validate the complete transaction flow and simulate real-world scenarios to ensure a seamless user experience.

6. **User Interface and Experience**: Design an intuitive and user-friendly interface that enables customers to easily access and use the local payment methods within your

digital bank application. Provide clear instructions, helpful guidance, and localized translations to make the process as seamless as possible.

7. **Customer Support and Education**: Offer dedicated customer support for users who may encounter difficulties using the local payment methods, and provide educational resources, such as guides, articles, or video tutorials, to help them become proficient users.

8. **Marketing and Promotion**: Leverage marketing and promotional campaigns highlighting the support of popular local payment methods to attract potential customers. This is particularly important in markets where these payment methods are widely used and expected by consumers.

By supporting popular local payment methods like Pix in Brazil and UPI in Argentina, your digital bank can significantly enhance its value proposition for users in these countries. Doing so requires a combination of in-depth market understanding, technical integration, and effective collaboration with local partners and authorities to ensure seamless experiences for your customers.

4. **Telegram** Integration (Telegram Wallet Bitcoin, USDT, TON)
5. **Coinbase, Buda.com, Bitso, or Mercado Bitcoin** integration
6. Aim for transaction completion within **10 seconds** for a smooth user experience.

4. Currency Exchange and Cross-Border Transactions

1. Develop a system for transparent and efficient currency exchange, allowing users to perform cross-border transactions easily. **Cross-banking transfers** or transfers between banks, involve a series of steps to move funds securely and accurately between customer accounts at different financial institutions. Here is an overview of the typical flow for a cross-banking transfer:

   1.1. **Transfer Initiation:** The customer initiates a transfer request through their bank's online portal, mobile app, or by visiting a branch. The customer provides the necessary details, including **the amount, recipient's name, recipient's bank, and the recipient's account number or IBAN (International Bank Account Number).**
   1.2. **Customer Authentication**: The sending bank verifies **the customer's identity and ensures they have sufficient funds or credit** in their account to complete the transfer.
   1.3. **Transaction Processing**: The sending bank processes the transfer request and prepares the transaction details to be sent to the recipient's bank. This may include applying **transfer fees** or **currency conversion**, if applicable.
   1.4. **Interbank Communication**: Transfers between banks often require communication through **interbank networks or systems**, such as **SWIFT (Society for Worldwide**

Interbank Financial Telecommunication) or **ACH (Automated Clearing House)** networks, depending on the country and transaction type. The sending bank **sends the transfer details to the recipient's bank through the chosen interbank network.**
1.5. **Recipient Bank Verification:** The recipient's bank **receives the transfer details and verifies the recipient's account information.** The bank also checks for any **issues related to fraud, sanctions, or compliance.**
1.6. **Crediting the Recipient**: Once the recipient's bank confirms the transaction details and performs necessary checks, it credits the transfer amount to the recipient's account. The time it takes to complete this step depends on factors such as the type of transfer, the banks involved, and the relevant interbank networks.
1.7. **Transaction Confirmation**: Once the recipient's bank has credited the funds, both the sending and receiving banks may generate a transaction confirmation, typically sent to the customer via email or visible in their online banking portal.
1.8. **Statements and Record-Keeping**: Both banks update their respective records and prepare the transaction information for inclusion in their account statements and reporting purposes.
1.9. Integration with Payment Gateways: Use international payment gateways like **PayPal, Stripe, Skrill, PayU, EBANX, or Mercado Pago.** These platforms offer robust APIs for integration with your systems, support multiple currencies, and handle currency conversion automatically.

2. Implement real-time currency conversion rates and support transactions in local currencies.
3. Provide users with **clear information on fees**, and aim for a conversion time of less than **3 seconds.**

5. Security and Fraud Detection

Multifactor Authentication

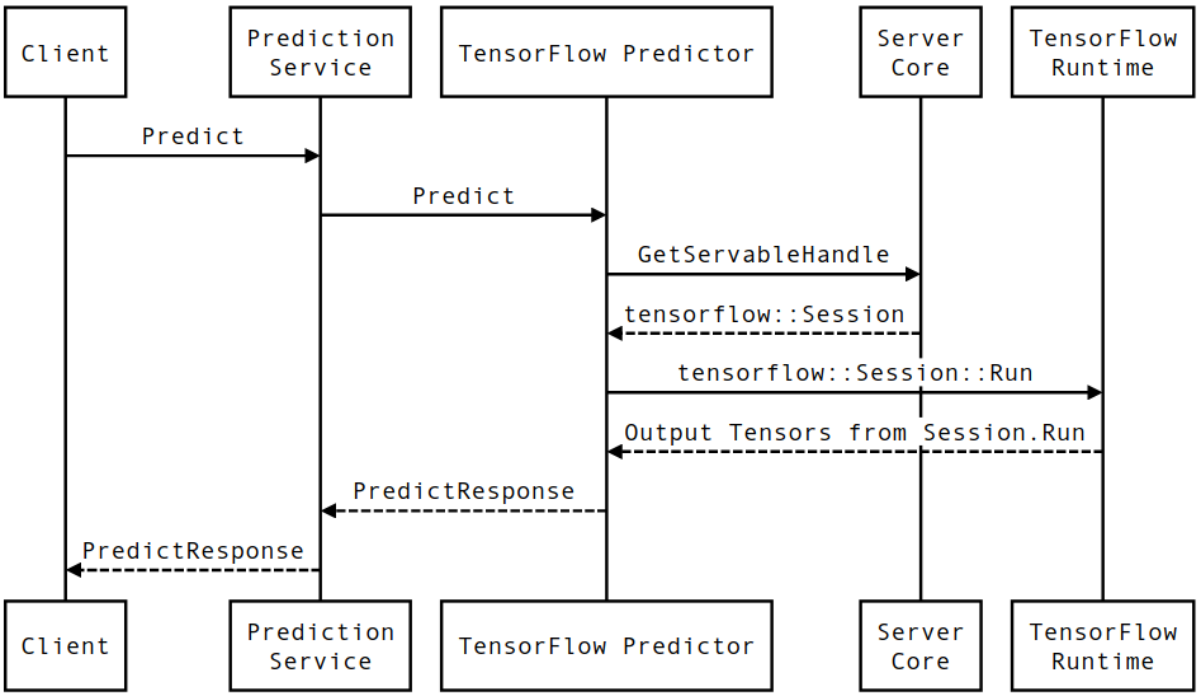
Common factors include something the user knows (e.g., a **password**), something the user has (e.g., a **physical token, a smartphone (Microsoft Azure AD**), and something the user is (e.g., biometric characteristics, like **fingerprints or facial recognition**).

Fraud Detection Systems

Implementing a fraud detection system involves using various techniques, tools, and strategies to identify suspicious activities and prevent financial fraud. Here's an outline of the steps to implement a fraud detection system:

1. **Define fraud types and risks:** Begin by identifying the various types of fraud that may impact your business, such as identity theft, credit card fraud, account takeover, or insider fraud. Assess the risks and potential impact of each fraud type on your organization.

2. **Data collection and preparation:** Collect and aggregate relevant data from multiple sources, including transaction details, customer profiles, and historical fraud cases. Ensure data quality and integrity, cleansing and normalizing the data for analysis, if needed.
3. **Feature engineering:** Extract and create relevant features or attributes from the data, which will help build models to detect fraud patterns. Features can include transaction amounts, frequency, time, and behavioral or contextual information.
4. **Choose fraud detection techniques:** Determine which fraud detection techniques best suit your organization's needs and available resources. Some common techniques used for fraud detection include:
   4.1. **Rule-based systems:** Define a set of rules or heuristics based on known fraud patterns, which can be adjusted over time. These systems are relatively simple to implement but may require regular adjustments to keep up with evolving fraud schemes.
   4.2. **Machine learning algorithms:** Use supervised and unsupervised learning techniques like Logistic Regression, Neural Networks, Decision Trees, or clustering algorithms to analyze data and detect anomalies, outliers, or patterns indicative of fraud.
   4.3. **Artificial Intelligence (AI) and deep learning:** Employ more advanced AI and deep learning techniques like recurrent neural networks (RNN) or long short-term memory (LSTM) networks for fraud detection, particularly when dealing with complex patterns or large volumes of data.
5. **Develop and train models:** Develop fraud detection models using selected techniques, feeding them with historical data for training and validation. Fine-tune the models to optimize their performance and strike a balance between false positives and false negatives.
6. **Integrate with existing systems:** Implement the fraud detection models within your organization's existing infrastructure and IT systems, such as payment processing, customer relationship management, or risk management systems.
7. **Real-time monitoring and alerting:** Monitor transactions and other activities in real-time to detect potential fraud cases, using the trained models. Set up alert mechanisms and notification systems to inform relevant personnel when suspicious activities are detected.
8. **Continuous model evaluation and improvement:** Assess the performance of your fraud detection system regularly, using metrics like precision, recall, F1-score, or the area under the receiver operating characteristic (ROC) curve. Update the models as needed, incorporating new data and feedback to maintain accuracy and effectiveness.
9. **Invest in employee education:** Train employees to recognize potential fraud scenarios and their roles in preventing and responding to fraud. Encourage a culture of vigilance and emphasize the importance of adhering to company policies and compliance procedures.
10. **Review and adjust:** Continuously review your organization's fraud detection processes, adjusting rules or models as necessary to respond to evolving fraud patterns and technology advancements.

11. 

6. Financial Education and inclusion

Daily, Weekly, Monthly reports for clients (regarding the possible perspective investments, exchange rates differences, and analysis of it type of blog).

Fundación Capital (Regional): Fundación Capital is a regional social enterprise present in several South American countries, focusing on financial inclusion, economic citizenship, and poverty reduction. Through initiatives like financial education programs, digital innovations, and **public-private partnerships**, they aim to empower marginalized populations and foster socio-economic development. Website: https://fundacioncapital.org/en/

7.Local Partnerships and Integration

Mercado Libre:

Mercado Libre, headquartered in Argentina, is the largest e-commerce platform in Latin America, dominating the market in countries like Argentina, Chile, Colombia, and Peru. Mercado Libre offers an extensive range of product categories, including electronics, fashion, home and garden items, and automotive parts. It provides various services such as **Mercado Pago (its payment platform), Mercado Envíos (its shipping service), and Mercado Crédito (its credit service).**

B2W Digital:

B2W Digital is a leading e-commerce company in Brazil that operates through multiple online retail platforms, including Americanas.com, Submarino.com, and Shoptime.com. These platforms offer a wide variety of product categories, ranging from household items to electronics. B2W Digital also provides **payment solutions through Ame Digital and a seamless shopping experience for customers.**

Magazine Luiza:

Magazine Luiza is another prominent e-commerce player in Brazil. Besides its extensive online presence, Magazine Luiza also has a vast network of physical stores across the country. They offer various product categories, including electronics, home appliances, furniture, and fashion. Magazine Luiza is known for its investments in digital innovation, logistics, and an omnichannel strategy that integrates online shopping with physical stores.

8. Regulatory Compliance

Argentina: Argentina's financial system is regulated by the Central Bank of Argentina (BCRA). Money laundering, terrorist financing, and other illicit activities are overseen by the Financial Information Unit (UIF). Financial institutions such as banks and insurance companies must comply with capital adequacy and risk management requirements.

Brazil:
Brazil's principal financial regulatory body is the Central Bank of Brazil (BACEN). There is also the Securities and Exchange Commission of Brazil (CVM) overseeing the securities market, and the Superintendence of Private Insurance (SUSEP) regulating the insurance market. Financial institutions need to comply with AML/CFT regulations, capital requirements, consumer protection norms, and data reporting requirements. In Brazil, capital adequacy requirements for financial institutions are regulated by the Central Bank of Brazil (Banco Central do Brasil, or BACEN).

Chile: In Chile, the Financial Market Commission (CMF) and the Central Bank of Chile oversees financial regulations. They ensure that financial institutions adhere to regulations concerning risk management, capital adequacy, corporate governance, and anti-money laundering.

Colombia: The Financial Superintendence of Colombia oversees banking, securities, and insurance sectors. Financial regulations cover a broad range of areas, including prudential regulations, AML/CFT norms, risk management, corporate governance, and consumer protection.

Peru: The Superintendence of Banking, Insurance and Pension Fund Administrators (SBS) regulates and supervises the financial system in Peru. Regulations cover aspects such as capital adequacy, risk management, AML/CFT standards, and data protection laws.
Given the complexities and variances between countries, entities are encouraged to work with local consultants or legal experts to ensure they accurately understand and comply with financial regulations and requirements. Remember, non-compliance can result in heavy penalties and damage to the reputation of the organization.

Observing capital adequacy and risk management requirements is essential for maintaining the financial health and stability of financial institutions. Here are some steps to ensure compliance with these requirements:

Understand the regulatory framework: Stay updated on the capital adequacy and risk management requirements set by the relevant regulatory authorities in your jurisdiction. These may include guidelines from central banks, financial supervisory authorities, or other regulatory bodies.

Develop a robust risk management framework: Establish a comprehensive risk management framework that identifies, assesses, and mitigates various risks such as credit risk, market risk, operational risk, and liquidity risk. Ensure that the framework includes processes for risk identification, risk assessment, and risk response.

Implement strong internal controls: Develop and maintain a system of internal controls that ensure the accuracy and integrity of your financial reporting, compliance with laws and regulations, and the effectiveness and efficiency of your organization's operations.

Maintain sufficient capital levels: Capital adequacy ratios, such as the Basel III framework, require financial institutions to maintain a minimum amount of capital relative to their risk-weighted assets. Continuously monitor your capital levels and ensure that you meet the regulatory requirements for capital adequacy.

Risk-weighted assets assessment: Regularly assess your organization's risk-weighted assets (RWAs) to ensure accurate risk measurement and capital adequacy calculations. RWAs are a measure of an institution's assets, adjusted for their associated risks.

Stress testing: Perform stress testing and scenario analyses to assess the potential impact of adverse market conditions on your capital levels and risk exposure. Use the results of these tests to enhance your risk management practices and ensure adequate capital buffers.

Monitor and report compliance: Establish a system for monitoring and reporting compliance with capital adequacy and risk management requirements. This may include regular reporting to senior management and the board of directors, as well as periodic reporting to regulatory authorities, as required.

Ongoing training and education: Provide ongoing training and education to employees responsible for risk management and compliance. This ensures that they remain up-to-date with the latest regulatory changes and best practices.

External consultation: Consider engaging external consultants or auditors to review your organization's adherence to capital adequacy and risk management requirements. This can provide valuable insights and recommendations for improvement.

Continuous improvement: Regularly re-evaluate your approach to capital adequacy and risk management to identify areas for improvement, enhance risk mitigation strategies, and ensure ongoing compliance with regulatory requirements.

Compliance with capital adequacy and risk management requirements is a critical aspect of maintaining financial stability. By implementing these steps, financial institutions can effectively monitor, manage, and mitigate risks while ensuring they meet their regulatory obligations.

Basel III

Capital adequacy requirements in Brazil, Peru, Chile, Colombia, Argentinal are based on the Basel III framework with adjustments according to government regulations.

The Basel III framework, established minimum capital requirements for banks to ensure financial stability and minimize the risk of insolvency. The framework sets three primary capital ratios that banks must observe:

1. Common Equity Tier 1 (CET1) Ratio: CET1 capital includes common shares, retained earnings, and other reserves. The CET1 ratio is the bank's CET1 capital as a percentage of its risk-weighted assets (RWAs). In Brazil, the minimum CET1 ratio requirement for banks is 4.5%.

RWAs are typically classified into three main categories: credit risk, market risk, and operational risk.

Risk-weighted assets (RWAs) are a measure of a financial institution's assets weighted by the risk associated with them. In the context of capital adequacy calculations, RWAs are used as a denominator to estimate the capital ratios to evaluate the financial health and stability of a financial institution.

The primary purpose of RWAs is to help regulators and financial institutions to account for the underlying risk exposure associated with different types of assets. By assigning risk weights to assets, regulators can ensure that banks maintain adequate capital to cover potential losses in case of default or other adverse events.

RWAs are typically classified into three main categories: credit risk, market risk, and operational risk.

Credit risk-weighted assets: Credit risk arises from the possibility that borrowers or counterparties may default on their financial obligations, leading to losses for the bank. To calculate credit risk-weighted assets, regulators assign different risk weights to loans, securities, and other debt instruments based on the creditworthiness of the borrowers or counterparties involved.

Market risk-weighted assets: Market risk includes the risk of losses stemming from fluctuations in market prices, such as interest rates, exchange rates, and equity or commodity prices. To measure market risk-weighted assets, banks use various approaches, such as Value-at-Risk (VaR) models or regulatory standardized models, to estimate their exposure to potential market losses.

Operational risk-weighted assets: Operational risk arises from the possibility of losses resulting from failures in internal processes, systems, people, or external events. Banks may use different methods (Basic Indicator Approach, Standardized Approach, or Advanced Measurement Approach) to assess their operational risk and determine the corresponding operational risk-weighted assets.

By using risk-weighted assets as a denominator in capital adequacy ratios, regulators can ensure that banks hold a minimum level of capital in proportion to their risk exposure, thereby enhancing the stability of the financial system and minimizing the risk of bank failures.

2. Tier 1 Capital Ratio: Tier 1 capital comprises CET1 capital and Additional Tier 1 capital (AT1, which includes instruments like preferred shares and contingent convertible bonds). The Tier 1 capital ratio is the bank's Tier 1 capital as a percentage of its RWAs. In Brazil, the minimum Tier 1 capital ratio requirement for banks is 6%.

3. Total Capital Ratio: Total capital includes Tier 1 capital plus Tier 2 capital (subordinated debt and other instruments that have loss-absorbing capacity). The total capital ratio is the bank's total capital as a percentage of RWAs. In Brazil, the minimum total capital ratio requirement for banks is 10.5%.

It is important to note that these requirements may be subject to changes from time to time, and banks should stay updated on the latest regulations from the Central Bank of Brazil. Additionally, banks may face additional capital buffer requirements based on their size, systemic importance, or current economic conditions, such as the countercyclical capital buffer and capital conservation buffer.

As a financial institution operating in South America, you'll need to manage various risks, comply with diverse regulations, and adhere to multiple standards across different countries. While this list is not exhaustive, it provides an overview of the key risks, regulations, and compliance requirements applicable to financial organizations in South America.

Risks

1. Credit risk: The risk of losses when borrowers or counterparties fail to meet their financial obligations.
2. Market risk: The risk of losses due to fluctuations in interest rates, exchange rates, equity prices, and commodity prices.
3. Operational risk: The risk of direct or indirect losses resulting from inadequate or failed internal processes, people, systems or external events.
4. Liquidity risk: The risk arising from the inability to meet financial obligations or fund asset purchases in a timely manner.
5. Reputational risk: The risk of damage to the institution's brand and standing, which may result from poor business practices, regulatory violations, or negative public opinion.
6. Legal and regulatory risk: The risk arising from non-compliance with applicable laws, regulations, and guidelines set by financial authorities.

Compliance and Regulations

1. Capital adequacy: Adherence to minimum capital ratio requirements, such as those set by the Basel Committee on Banking Supervision's Basel III framework, and any additional capital buffer requirements imposed by local regulators.
2. Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT): Design and implement an effective AML/CFT program in line with the requirements of the Financial Action Task Force (FATF) and local regulations in each country of operation.
3. Know Your Customer (KYC) and Customer Due Diligence (CDD): Implement KYC and CDD procedures to verify the identity of customers, understand their activities, and assess potential risks of money laundering or terrorist financing.
4. Consumer protection: Comply with local regulations regarding the transparency of financial products and services, fair treatment of customers, and dispute resolution.

5. Data protection: Implement robust data privacy and security measures to protect customer information and comply with data protection laws in respective countries, such as the General Data Protection Regulation (GDPR) and local data protection legislation.
6. Corporate governance: Establish a sound corporate governance framework, ensuring effective oversight, transparency, risk management, and accountability.
7. Taxation: Comply with all applicable domestic and international tax regulations, including reporting requirements, and cooperate with taxing authorities to combat tax evasion.
8. Credit reporting and information sharing: Adhere to local regulations regarding sharing customer credit information with credit bureaus or other financial institutions.
9. Foreign exchange and cross-border transactions: Comply with foreign exchange controls and restrictions on cross-border transactions as imposed by each country's central bank or financial authority.
10. Sector-specific regulations: If your financial institution operates in niches such as insurance, pensions, or securities, adhere to the regulations specific to those sectors, as enforced by each country's respective regulatory body.

9. Accessibility and Inclusivity:

Support English, Spanish and Portuguese languages

Supporting multiple languages in an application is essential in catering to a diverse user base and providing a seamless user experience. To build a multilingual application, follow these steps:

Internationalization (i18n): This is the process of designing your application to support various languages and regions without modifications. Ensure that your application is developed with internationalization in mind, accommodating different character sets, number formats, date/time formats, and potential variations in text length due to translations.

Localization (l10n): Localization is the process of translating and adapting your application to different languages and cultures. This includes translating text, modifying images or other media to reflect language-specific contexts, and adjusting the UI to display translated text and different formats correctly.

Externalize strings: Keep all text displayed in the application separate from the source code. Store text in dedicated external files or databases called "resource files" or "language packs." Each language should have its resource files containing the appropriate translations.

Language detection: Implement a mechanism to detect the user's preferred language based on their device settings, browser preferences, or in-app selection. Automatically set the application's language according to the user's preference upon launch. Also, provide an option for users to switch languages manually within the app.

Use language files: Load the appropriate resource files or language packs based on the selected language. When displaying text, fetch the translated strings from these files rather than hardcoding them in the application.

Format dates, times, and numbers: Use built-in or third-party libraries to present date, time, currency, and number formats in accordance with the user's language and regional preferences.

Font compatibility: Use fonts that support the character sets of the languages you plan to display, ensuring legibility and consistent presentation across different languages.

Testing: Rigorously test your application in all supported languages and on devices with different regional settings. This ensures translations and formatting are accurate, and the user experience remains consistent across languages.

Translation updates: Regularly update translations and incorporate changes into your application. Engage professional translators, language service providers, or use localization platforms like Transifex or CrowdIn to maintain high-quality translations.

Optimization

To optimize an app for users with low-end smartphones and limited data plans, it's essential to focus on performance, data efficiency, and user experience. Here are some strategies to achieve this:

Design a lightweight user interface (UI): Create a simple and clean UI with elements that require minimal data and computing resources. Use compressed image formats like WebP and SVG or opt for minimalistic icons instead of heavy graphics.

Optimize images and multimedia: Compress images without compromising quality, and use responsive images to serve appropriately sized images according to the device screen. For videos, ensure they are compressed and optimized for mobile viewing.

Reduce app size: Keep the app's download size as small as possible by removing unnecessary assets, using vector graphics wherever possible, and minimizing the use of third-party libraries.

Enable data saving features: Offer settings that allow users to reduce data usage, for example, by turning off automatic image and video loading or enabling a functional offline mode.

Lazy loading: Implement lazy loading for images, videos, and other content to ensure that only the necessary elements are loaded when required, reducing the amount of data consumed on initial load.

Optimize network requests: Minimize the number of API requests, and use caching where appropriate to avoid redundant requests. Also, consider using data-efficient mechanisms such as GraphQL to minimize the payload of requests and responses.

Test on low-end devices: Actively test your app on low-end devices and slow network connections to ensure that it works effectively under various conditions.

Monitor and optimize performance: Utilize performance monitoring tools to measure the app's performance, identify bottlenecks, and optimize resource usage, such as CPU, memory, and network bandwidth.

Progressive Web App (PWA): PWA is an alternative solution that combines web technology with a native-like experience, offering lower data and resource consumption. Consider developing a PWA for potential gains in performance and data efficiency.

Educate and communicate: Inform users about the app's features and settings that help in managing data consumption and maximizing efficiency. Good communication helps establish trust that your app respects users' data limitations.

10. Scalability and Performance:

Create an architecture that can scale to accommodate a user base of at least **5 million within the first year**. Ensure the app remains responsive even **during peak usage times**, such as salary payment days. Implement **caching strategies** and **CDN integration to optimize performance**.

11. Delivery Center

To build a local delivery and engineering center that maximizes the value of received investments, follow these steps:

1. Strategic planning and research: Conduct comprehensive research and planning to identify the optimal location for your local delivery and engineering center. Consider factors like availability of skilled talent, proximity to customers, cost of real estate, infrastructure, and local business incentives.

2. Resource allocation: Allocate the required resources, such as funding, human resources, and equipment, for the establishment and operation of the local center. Secure necessary permits and licenses to ensure compliance with local regulations.

3. Talent acquisition: Develop a well-defined recruitment strategy to attract and retain skilled professionals in engineering, delivery management, project management, and other relevant roles. Collaborate with local universities or technical institutions to identify potential hires and establish partnerships for talent development.

4. Capacity building: Invest in employee training and development to ensure a high level of expertise and continuous improvement of your team. Encourage knowledge sharing, collaboration, and nurturing of innovation within the center to drive value creation.

5. Infrastructure development: Set up the necessary infrastructure for the local center, including office spaces, IT systems, labs, meeting rooms, and other facilities. Invest in modern equipment and tools to ensure efficient operations and foster a productive work environment.

6. Develop local collaborations: Establish partnerships with local businesses, suppliers, industry associations and government agencies to strengthen your presence in the community and enhance your value proposition.

7. Project management: Implement robust project management practices to ensure timely and efficient delivery of projects. Use agile methodologies and adapt them to the local context to drive continuous improvement and maximize customer satisfaction.

8. Quality assurance and control: Establish quality assurance and control processes to ensure consistent high standards for products and services delivered by the center. Implement regular reviews, audits, and continuous improvement mechanisms to maintain a culture of excellence.

9. Performance measurement and analytics: Develop and track key performance indicators (KPIs) to measure the effectiveness of the local center and gauge its impact on the overall business. Conduct regular reviews and analysis of the performance data to identify areas for improvement and make data-driven decisions.

10. Marketing and expansion: Leverage your local delivery and engineering center's capabilities to attract new clients and expand your customer base. Develop a strong promotional strategy highlighting your center's strengths, expertise and commitment to local economic development.

PROFIT

1. **Subscription Fees:** AsePay offers different tiers of account plans, including free and premium options. Premium plans, such as Silver, Gold, Platinum, Black, provide added benefits and features like higher ATM withdrawal limits, overseas medical insurance, and cashback rewards. Customers pay a monthly or annual fee for these premium account tiers.
2. **Interchange Fees:** When users make purchases with their AsePay cards, the merchant's bank pays a fee to the card issuer, known as an interchange fee. A portion of this fee is passed on to AsePay, providing another source of revenue.
3. **Foreign Exchange Fees:** For certain currency exchanges outside of the fee-free limit or outside market hours, AsePay charges a markup or a nominal fee. This fee contributes to their overall revenue stream.
4. **Trading & Investing Features:** AsePay offers trading and investment services, including access to stocks and cryptocurrencies. They charge fees for some transactions, like cryptocurrency exchanges or instant trades, and these fees contribute to their income.
5. **Lending and Credit Products:** AsePay may offer credit products, such as personal loans, overdrafts, or credit cards, and generate revenue through interest rates and fees associated with these lending services.
6. **Partner Commissions:** AsePay partners with third-party service providers like insurance companies, mobile phone service providers, and other financial service providers, offering their services or deals to its users. AsePay may receive commissions or referral fees from these partners.
7. **Business Banking:** AsePay also offers banking services to businesses, with features like multi-currency accounts, money transfers, and expense management. Businesses pay subscription fees for their AsePay Business accounts, and additional fees may apply for specific services or transactions.