FinTech in the Modern Philippines: A Financial Regulation Adequacy Analysis

Espejo, Abigael C.

MS Finance 296 – Financial Regulation and Ethics | September, 2017

Abstract

The global trend of the financial markets towards the use of FinTech has already caught up in the Philippines. The activities of FinTech start-ups in the nation's emerging market have already reached a significant transaction volume that raises different types of risks. Cyber threat and data privacy issues are the major concerns in this internet-reliant industry, especially since the government has experienced major cyber-threats within the past year. These issues, among others, demand a regulatory framework from the government financial arms for risk mitigation and at the same time, promotion of the FinTech trade. The Bangko Sentral ng Pilipinas has issued two circulars in relation to FinTech early this year as a respond to this demand. Additionally, laws such as the E-commerce Act, Data Privacy Act and Cybercrime Protection Act have pushed the country towards accepting the modernization brought about by technology in regulatory terms. This policy paper also presents a comparison between the domestic regulations against the FinTech policies of other countries, and identifies the regulatory lapses in the Philippine's current framework.

I. Introduction

In a digital age where information is power, the protection of data shared within the cyber landscape needs to be a major concern for government regulators and financial institutions. The Philippines has been dubbed as the *social media capital of the world*, pushing world records on internet activity from as simple as supporting local TV shows, to expressing political opinions, down to personal causes and even cyber bullying. However, beyond the staggering number of hours spent online and the international fame the Filipino internet addiction that ensued is the dependency and reliance of a nation on the new-age information and communications technology.

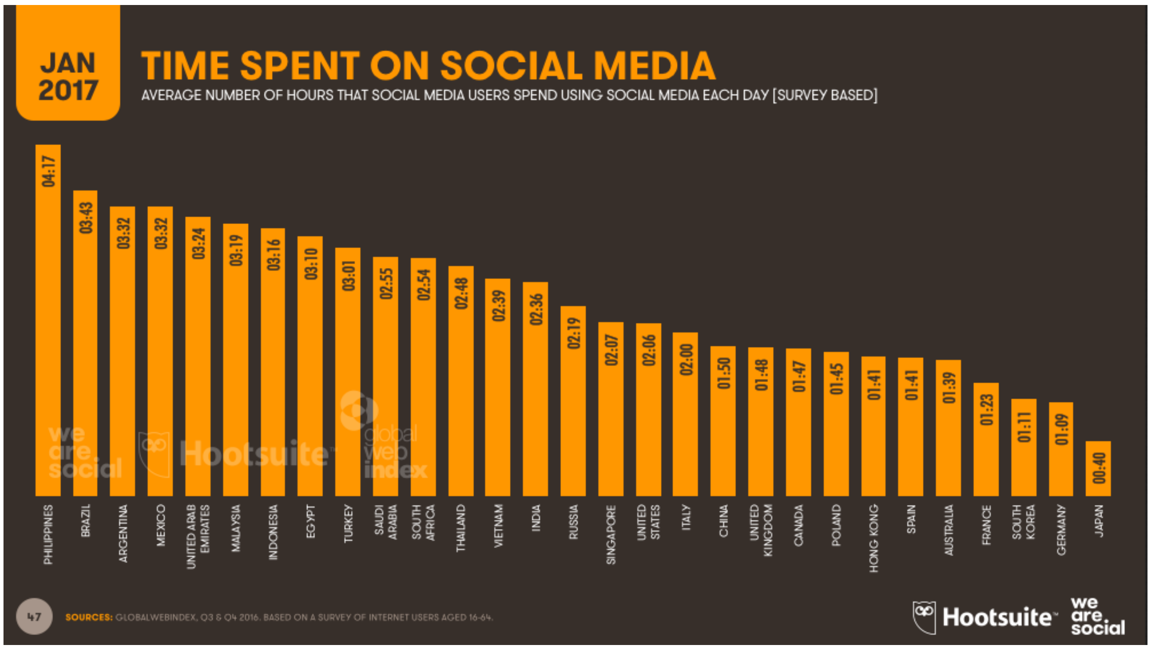


Figure 1 Philippines ranks #1 on the time spent on social media *(Source: https://wearesocial-net.s3.amazonaws.com/uk/wp-content/uploads/sites/2/2017/01/Slide047.png)*

Activities on the internet are not limited on social media alone, financial institutions have caught up with the internet age and have been using the internet for efficiency, greater market reach and additional product variability.

Traditional banking has restricted access to the financial services of the country's emerging economy, mainly due to the country's geographical landscape, language differences, and economic distribution, among others. While around 55% of the total population uses the internet, only 30% of the population has bank accounts. The untapped market is a huge potential for the financial wealth of the country, and the move towards internet and mobile flexibility will open the doors for additional monetary sources, promoting a more robust financial economy.

Since the integration of technology and finance is inevitable, financial regulations need to cope with the innovatory behavior of the industry. This policy paper shall present an analysis of the financial regulations in the Philippines in relation to the FinTech start-ups and movements in the market, as demanded by the latest and upcoming technological trends in finance.

II. *FinTech in the Philippines*

FinTech, the use of technology to deliver financial solutions, has been picking up in the Philippines as a response to the market demand of technology-based financial products and services. The trend towards innovation has been supported by the following Philippine demographics data:

- Millennials top the internet users of the country, with a median age of 24. This young population is more receptive to new ways to do things and places a high value on efficiency.
- Mobile internet penetration rate is growing at a rate of 1.5 times per year. More and more people use their mobiles as a substitute to daily activities.
- Increasing number of e-commerce shoppers (29% of the total internet-users population) validates the users' trust on online sale transactions.
- An increasing number of Overseas Filipino Workers (OFW) with needs of managing financial transactions across borders.

The expansions through technological applications have been started in the following sectors:

Sector	**Activities**	**Leading Start-ups**
Lending	▪ matchmaking between loan seekers and banks or private finance establishments ▪ financial consultancy and assistance to borrowers	Lendr LendMe.ph LoanSolutions.ph Leverage
Block chain / Cryptocurrencies	▪ purchasing and selling of cryptocurrencies ▪ digital payment technology using digital currencies	Satoshi Citadel Industries Rebit.ph Bitmarket.ph
Online Wealth Management	▪ online pawning ▪ investment assessment assistance	PawnHero Robur
Crowdfunding	▪ funding projects or ventures via monetary contributions	The Spark Project Cropital PhilCrowd GoGetFunding
Personal Finance Management	▪ financial services to the unbanked ▪ mobile money solutions	Mynt iMoney Philippines
Data Management	▪ Cloud-based data storage and software solutions ▪ Credit analytics platform	Salarium Lenddo Myfinb
Money Transfer	▪ Seamless money transfer via digital payment in cash, credit or cryptocurrencies	Coins.ph E-peso Weepay
Digital Payment	▪ Digital wallet via mobile applications ▪ Bills payment	TagCash BPI Globe BanKO GCash/Smart Money PayMaya/Pitaca DragonPay/Peso Pay
Comparison Sites	▪ Small business investment through rewards and points	PaidUp Zap

Table 1. Different sectors of FinTech start-ups in the Philippines

How big is FinTech in the Philippines?

Investors have been flocking the FinTech industries, with an approximated US$4.9 billion worth of transaction value in 2016. This amount is projected to grow annually at a rate of 20%, ballooning up to US$11 billion by 2020. The largest market share goes to the digital payment sector, which covers almost 98% of this value.

In 2016, around 70 million FinTech users have been recorded. This number is expected to sum to 82million by 2020. The average transaction value per user is US$65 in 2017.

III. Potential Risks Associated with FinTech

The trend towards technology-based financial instruments and services do not come off without certain risks such as:

a. Cyber threat – financial institutions are exposed to sophisticated and evolving cyber threats that require constant awareness and timely defenses.
b. Data protection and privacy – the storage of data in the internet and cloud landscape radically increase the amount of risk in keeping the data protected. A strong authentication, end point software, and malware detection is highly necessary to protect data.
c. Reliance on third-party providers are increasing – financial institutions are employing external firms to develop the latest possible technological version of their products and services. This increased reliance on third party institutions may increase compliance risk.
d. KYC – know-your-customers rule become more complicated as FinTech companies are still required to meet the traditional KYC rules.
e. Anti-trust/Monopoly – financial institutions may create private networks for exclusive trading and product offerings
f. Credit risk – a seamless credit system relies on algorithms to assess the credit worthiness of borrowers.

IV. Overview of the Philippine Regulations related to FinTech

FinTech thrives on innovation. Hence, a regulatory framework that encourages innovative business solutions and products is essential towards the advancement of this market sector. This section highlights the existing regulations and the government initiatives, in relation to FinTech enterprises.

Bangko Sentral ng Pilipinas Regulations and Initiatives

The BSP has relaxed banking norms to make regulations relevant to the changing financial environment:

- allowed telecom companies to offer mobile money services
- lowered remittance rate for external and internal payments
- created a separate unit for innovative digital technologies

- KYC norms - allowed financial institutions to rely on third-party verification of KYC. The ID requirements for opening a bank account have also been relaxed. This has enabled banks to outsource some of their verification processes to financial technologies.

Additionally, it has issued two circulars in the beginning of 2017 that targets companies engaged in remittance services, e-money, digital currency, and other FinTech businesses. Both circulars amended the BSP Manual of Regulations for Non-Bank Financial Institutions.

BSP Circular No. 942 (issued on January 20, 2017)

This circular applies to remittance and transfer companies (RTCs), which include e-money issuers and remittance platform providers, remittance sub-agents, and money changers/forex dealers (MCs/FXDs). The circular contains the following rules and guidelines:

- RTCs and MCs/FXDs need to register in BSP. Existing ones should re-register within six months from the circular effectivity (February 10, 2017).
- Covered entities need to register with the Anti-Money Laundering Council Secretariat.
- RTCs and MCs/FXDs must seek the approval of BSP for any change in control of the corporation. Control refers to any transaction involving voting shares that will transfer, or result in, the ownership or control by a person of at least 20% of the voting shares, or which will enable such person to elect, or be elected as, a director of the covered entity.
- Foreign RPPs can only conduct business through a locally incorporated subsidiary. Existing foreign RPPs have a two year deadline in incorporating a subsidiary. They should appoint a resident agent in interim.

BSP Circular No. 944 (issued on February 6, 2017)

This circular oversees the operations and reporting obligations of digital/virtual currency (VC) exchanges in the country. It covers all institutions that offer services in relation to trading, conversion or fiat currency to VC or vice versa.

This circular describes virtual currencies as any type of digital unit used as a medium of exchange or form of a digitally stored value that may be:

- with a centralized depository or administrator.
- decentralized and have no centralized repository or administrator.
- created or obtained by computing or manufacturing effort.

Virtual currencies do not include:

- e-money.
- digital units solely used within online gaming platforms that are not convertible to fiat currency or actual goods or services.
- digital units that are redeemable exclusively in goods and services and are limited to transactions involving a defined merchant (like rewards programs).

Virtual currencies must be registered in BSP to operate as a remittance and transfer company. They must also register with the Anti-Money Laundering Council.

Moreover, the BSP recognizes that FinTech firms are beyond the straightforward oversight of their authority and other financial sector regulators, hence, two options are currently being reviewed as a solution to this

- an Application Programming Interface (API) system that would streamline the reporting requirements between the BSP and its regulated entities. This API system would consolidate the data under one warehouse that would enable them to access information in a significantly shorter period of time.
- An Automated Complaint Handling Portal that would directly link the BSP with the customers of the regulated entities.
- A National Retail Payment System (NRPS) framework that will convene financial institutions to enable the electronic credit transfer scheme among the members within the framework

Electronic Commerce (E-commerce) Act of 2000

Republic Act 8792 or the Electronic Commerce Act of 2000, is an act providing for the recognition and use of electronic commercial and non-commercial transactions and documents. The Act aims to provide a secure legal framework and environment for e-commerce, and to protect the integrity of electronic documents and electronic signatures, including its transmission and communication.

This act has the following provisions:

a. Provides the legal recognition of electronic data messages, electronic documents and electronic signatures
b. Legalizes the formation of contracts in electronic form
c. Makes the banking transactions done through ATM switching networks absolute once consummated
d. Allows parties to have the right to choose the type and security methods depending on their respective needs
e. Provides the mandate for electronic implementation of transport documents to facilitate carriage of goods.
f. Provided the guidelines on when a service provider can be liable
g. Makes all existing laws, such as the Consumer Act of the Philippines, applicable to e-commerce transactions.

Data Privacy Act of 2012

Republic Act 10173, also known as the Data Privacy Act of 2012, aims to protect individual personal information in the information and communications systems in the government and in the private sector. The act defines personal information as "any information, whether recorded in material form or not, from which the identity of an individual is apparent or can reasonably and directly ascertained by the entity holding the information.

This act has the following aspects:

a. Definition of the procedures to be followed in the collection, processing, and handling personal information
b. The rights of data subjects to be informed and to have a reasonable access to the information being processed

c. The creation of the National Privacy Commission, an independent body that will administer and implement the provisions of this act.
d. Appointment of a personal information controller for the implementation of appropriate measures for the protection of personal information against unlawful use and processing.

Violations are penalized with fines from Php500 thousand to Php2million, and 3 to 6 years of prison terms.

Cybercrime Prevention Act of 2012

Republic Act 10175, known as the Cybercrime Prevention Act of 2012, defines cybercrime, aims to address the legal issues concerning online related activities. This is the first law in the Philippines that criminalized technology-related crime incidences including:

a. Offenses against the confidentiality, integrity and availability of computer data and systems such as illegal access, illegal interception, data interference, system interference, misuse of devices and cyber squatting
b. Computer-related offenses such as forgery, fraud and identity theft
c. Content related offenses such as cybersex, child pornography unsolicited commercial communications, and libel

Imprisonment of prisión mayor (6 years and one day to 12 years) and fines shall be imposed as penalties against individuals upon commitment of the abovementioned criminal acts. Corporate liability is equivalent to at least double the fines imposed on individuals up to a maximum of Php10 million.

V. National Cybersecurity Plan 2022

The National Cybersecurity Plan of 2022 was created to establish an environment that will promote confidence in everyone while using ICT tools, and ensure that the Philippines is self-reliant and able to protect its interests, particularly in national security. In pursuant of RA 10844, the DICT shall protect the security of critical infrastructure, including information assets and data of the government, individuals and businesses.

The National Cybersecurity Plan 2022 is a five-year process of implementation of the National Cybersecurity Strategy Framework which aims to adopt and implement the global Information Security Governance and Risk Management. The primary goals of this plan are: (1) assuring the continuous operation of our nation's critical infrastructure and public military networks; (2) implementing cyber resiliency measures to enhance our ability to respond to threats before, during, and after attacks; (3) effective coordination with law enforcement agencies; and a cybersecurity-educated society.

In order to accomplish these goals, the following mission objectives have been determined:

a. To systematically and methodically harden the Critical Information Infrastructure (CII) Resiliency;
b. To prepare and secure the government infrastructure;
c. To raise awareness in the business sector on cyber risk and the use of security measures among businesses to protect, respond and recover from attacks; and

d. To raise awareness of individuals on cyber risks among users as they are the weakest links.

The National Cybersecurity Strategy Framework is guided by the principles of the following:

a. Rule of Law – apply the rule of law in the cyberspace as much as it is applied in the physical world.
b. Autonomy and Self-governance – government intends to continue respecting the self-governance that cyberspace has developed.
c. Collaboration with Multi-Stakeholders and International Cooperation – building a layer of defense among citizens, businesses, education providers and governments.
d. Balance between Free Flow of Information and Privacy Rights of Individuals – balance must be made between protecting the privacy of the individual against securing protection of information and data of the users.
e. Risk Based Management Approach – formulation of a Risk Treatment Plan that the government and other relevant sectors will undertake as it evaluates the types of risk appetites of the stakeholders.

The government, through the DICT shall provide the formulation of policies, guidelines and strategic direction for cybersecurity. The National Cybersecurity Strategy Framework may be found in *Appendix 1.*

VI. Cyber Attacks

With the progressing trend towards the use of technology in financial transactions, the issue of cyber security is of the highest importance to ensure the continuous development of the industry. FinTech is founded on the customers' trust, hence, cyber-attacks, especially on government agencies, are crucial and may be an impediment to the emerging FinTech market.

Several incidents of cyber-attacks have been recorded in the country, some of the most notable incidents are:

- Anonymous Philippines claimed the attack on the server of the Philippine Voter's Database on March 2016 in which around 54 million sensitive data was leaked online. In 2016, at least 68 government websites have been subject to attacks including hacking attempts and defacement.
- Finland-based security firm, F-Secure, has reported that a malware may be spying on the Philippines as a form of cyber-espionage in 2016. It was found targeting confidential information of the government and private institutions.
- In May 2017, a ransomware called WCry has affected several countries, including the Philippines reportedly. This ransomware encrypts files in the infected computer and demands payment of $300 worth of Bitcoin in exchange for the recovery of files.

VII. Global Jurisdiction in FinTech

Governments of huge market economies have taken a much more proactive role in building their domestic FinTech initiatives through regulatory support. The FinTech industries of UK, Australia, Hong Kong and Singapore have been analyzed to come up with these general regulatory trends among FInTech intensive nations.

a. Creation of a FinTech focused structure within the regulator – focused groups within the nation's financial regulatory bodies have been created to focus on FinTech.
b. Sandbox – regulatory sandboxes have been created by regulators for FinTech firms to be able to experiment their new business models.
c. Innovation Hubs – serves as the financial regulatory bridge to FinTechs, shortening times for them to obtain licenses.
d. Guidance on different areas of FinTech – including secure cloud computing, digital finance and insurance, marketplace lending, cyber resilience measures, e-payments.
e. RegTech – promotion of the active use of technology to continually catch up with the latest FinTech trends.

VIII. FinTech Regulatory Concerns – Recommendations

The current landscape of Philippine regulations in line with FinTech is still substantially under par as compared to other countries. The following regulatory changes and initiatives are recommended to safeguard the financial stakeholders against the inherent risks due to FinTech, while at the same time, promoting the innovative spirit in the market.

a. *Establish a regulatory body within the Bangko Sentral ng Pilipinas that focuses on FinTech.*
   A technologically inclined regulatory arm within the BSP is needed to be able to track all these FinTech groups. This regulatory body should be focused on developing regulatory compliance requirements in relation to FinTech firms, monitoring of FinTech performance and compliance, and should have penalizing power for noncompliant firms.
b. *Standardize application and reporting requirements for FInTech companies.*
   A standard process should be established for a seamless application process of FinTech firms, non-restrictive of the products and/or services that they offer. Standard reporting requirements should also be imposed to make sure that stakeholders are aware of the financial status and performance of these firms.
c. *Maintain some financial indices.*
   Levarage, cost of capital, and required asset base, are just some of the financial measures that need to be restrictively followed by FinTech companies. While the investment on physical assets may be low in these industries, it must be ensured that there is enough capital and earnings to keep the company afloat.
d. *Create a FinTech Sandbox and assess risks of new technologies via this portal.*
   Setting up a sandbox environment would incur costs to the government. However, this is a way for FinTech start-ups to test their products before launching it in the market. This can be used by the regulatory bodies to assess the risk and tailor-fit some policies, depending on the product/service offered. This solution will answer the huge risk variance among different FinTech firms due to its innovative nature.
e. *Move towards RegTech.*
   A regulator for technology based firms should be able to catch up with the technology itself. Hence, the move towards RegTech of the FinTech regulator would promote a proactive approach towards

this segment, reduce risks due to increased regulatory knowledge on the latest technological advancements and use FinTech on their own.

f. *Provide tax incentives to FinTech companies.*

Tax incentives would promote more players in the FinTech market.

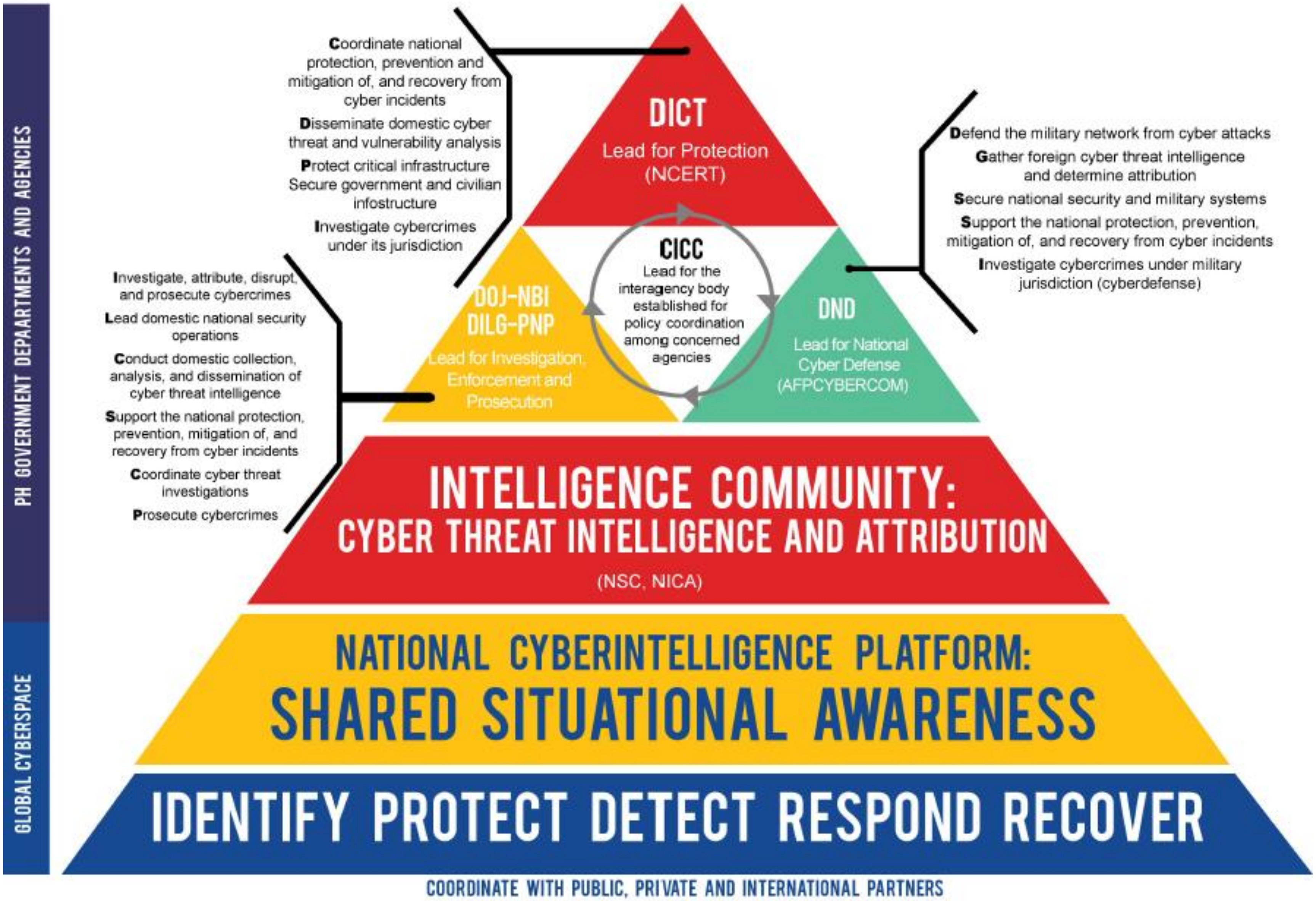
g. *Stricter licensing requirements for cryptocurrency trading and ICOs.*

With the recent decision of China to ban the trade of cryptocurrencies as they are seemed to be illegal, a more cautious approach should be applied in the Philippine market. The highly volatile nature of digital currencies posts a higher risk among investors, especially to the return riders who are not very familiar with their investments. To be able to mitigate the risks of virtual currency trading, stricter licensing requirements may be imposed. Additionally, to promote information symmetry among all investors, an information campaign must be initiated before allowing the firm to proceed in launching their ICO.

h. *Regulate crowdfunding initiatives.*

Crowdfunding initiatives have already started to pick up in the local market. While this model is socially inclined, the stakeholders are high susceptible to fraud. Policies may be imposed to crowdfunding initiatives of a certain amount (for instance, if raised money would total of more than Php500 thousand) and would involve a certain number of investors (for example, if 20 or more people contributed to the fund, it should be registered),

Appendix I. National Cyber Security Framework (from the National Cyber Security Plan 2022)



References:

A Profile of Internet Users in the Philippines. (https://www.rappler.com/brandrap/profile-internet-users-ph)

Arellano Law Foundation. *Republic Act 10175.* (http://www.lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html)

Castro, Fleire. *Social Media and Digital Stats in the Philippines. 31 January 2016.* (http://fleirecastro.com/guides/social-media-and-digital-stats-in-the-philippines-2016-wearesocial-data/)

Dogwe, A., Eusebio, C., Gonzales, M., Tandoc, L., Tating, Al. *Study on Financial Technologies* (https://www.slideshare.net/MauriceGonzales/sector-study-of-financial-technology-in-the-philippines-64733032)

Financial Inclusion in the Philippines Dashboard, Bangko Sentral ng Pilipinas. 1st Quarter 2017. (http://www.bsp.gov.ph/downloads/Publications/2017/FIDashboard_1Q2017.pdf)

FinTech News Hong Kong. *ICOs are subject to Securities Law in Hong Kong: License Needed! 5 September 2017.* (http://fintechnews.hk/2033/blockchain/icos-subject-securities-law-hong-kong-license-needed/?utm_content=bufferab0ba&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer)

FinTech News Singapore. *3 Crypto Companies in the Philippines You Should Know. 18 August 2016.* (http://fintechnews.sg/4669/blockchain/3-crypto-companies-in-the-philippines-you-should-know/)

FinTech News Singapore. *MAS: 100 FinTech Problems to Solve for Singapore* (http://fintechnews.sg/3268/fintech/mas-100-fintech-problems-to-solve/)

FinTech Start-ups in the Philippines. 10 February2017. (https://aseanup.com/fintech-startups-philippines/)

Fintech Singapore. (http://fintechnews.sg/philippines/)

Higgins, Stan. *The Philippines Just Released New Rules for Bitcoin Exchanges. 7 February 2017.* (https://www.coindesk.com/philippines-just-released-new-rules-bitcoin-exchanges/)

Kong, Alex. *The State of FinTech in the Philippines. 17 October 2016* (https://yostartups.com/the-state-of-fintech-in-philippines/)

Lopez, Elyssa. *How PH banking will look like in 2020. 25 May 2016.* (http://www.entrepreneur.com.ph/startup-tips/ph-banking-fintech-2020-a746-20160525)

Mateo, Janvic. *DICT drafts Philippine cybersecurity plan. 28 December 2016.* (http://www.philstar.com/business/2016/12/28/1657255/dict-drafts-philippine-cybersecurity-plan)

Mateo, Janvic. *Spread of malware is the first big test for Philippine cybersecurity plan. 14 May 2017.* (http://www.philstar.com/headlines/2017/05/14/1699819/spread-malware-first-big-test-philippine-cybersecurity-plan)

Mobile finance innovation in the Philippines. 10 February 2017 (https://aseanup.com/mobile-finance-innovation-philippines/)

Nam Soon, Liew and Lee-Salas, Vicky. *The Digital Challenge from a Philippine Banking Perspective. 25 July 2016.* (http://asianbankingandfinance.net/banking-technology/commentary/digital-challenge-philippine-banking-perspective)

Palabrica, Raul. *Data Privacy Act of 2012. 31 August 2012.* (http://business.inquirer.net/79534/data-privacy-act-of-2012)

Republic Act 8792 of the Philippines. Electronic Commerce Act of 2000. (http://www.dict.gov.ph/wp-content/uploads/2014/10/images_ipenforcement_RA8792-E-Commerce_Act.pdf)

Statista. *Fintech Philippines.* (https://www.statista.com/outlook/295/123/fintech/philippines#)

SyCip Law TMT Bulletin: Philippine Cental Bank Issues New FinTech Rules. (http://www.syciplaw.com/documents/LegalResources/Philippine%20Central%20Bank%20issues%20new%20FinTech%20rules%2020170210.pdf)

The Future of FinTech in Hong Kong. FSCD Paper No. 29 (http://www.fsdc.org.hk/sites/default/files/FSDC%20Paper_FinTech_E.pdf)