

Work In Progress-embargoed Not For Circulation Or Citation



Security Standards for the Financial Technology Sector in India

October, 2019

By **Vipul Kharbanda, Prem Sylvester**

The Centre for Internet and Society, India

Work In Progress-embargoed Not For Circulation Or Citation

Introduction

Information security standards provide a framework for the secure development, implementation and maintenance of information systems and technology architecture. Regulatory policies often cite several information security standards as a baseline that is to be complied with in order to ensure the adequate protection of information systems as well as associated architecture. Information security standards for the financial industry provide consideration to the specific risks and threats that financial institutions may face, making them an integral part of the process of ensuring business and operational sanctity.

There is an urgent economic interest in ensuring robust security of the financial technology sector within the country. This interest is amplified considerably due to the policy push seeking to shift India towards the realisation of a 'cashless society'. This recent policy push has in part led to the ubiquitous adoption of technology-centric financial services such as PayTM, PhonePe, Mobikwik and others. The current landscape with respect to security standards for financial institutions in India appears to be multi-pronged; with multiple standards in place for companies to implement.

One of the major stumbling blocks when dealing with the Fintech sector is the lack of a universally accepted definition of the term. FinTech is generally understood as an amalgamation of "finance" and "technology," but there is divergence on whether the centre of gravity of FinTech is the former or the latter.¹

Definitions that focus on the financial services offered by FinTech describe technology as an enabler. Arner et al² simply state that "FinTech refers to technology enabled financial solutions, or the new marriage of financial services and information technology," or as Thakor puts it³, FinTech is the "use of technology to provide new and improved financial services." FinTech is often described in terms of the companies that offer such financial

¹ Fintech Literature Review - Forthcoming

² Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P., The Evolution of Fintech: A New Post-Crisis Paradigm? (October 1, 2015). University of Hong Kong Faculty of Law Research Paper No. 2015/047; UNSW Law Research Paper No. 2016-62. Available at SSRN: <https://ssrn.com/abstract=2676553> or <http://dx.doi.org/10.2139/ssrn.2676553>

³ Anjan V. Thakor, Fintech and banking: what do we know?, Journal of Financial Intermediation, 2019, 100833, ISSN 1042-9573, <https://doi.org/10.1016/j.jfi.2019.100833>.

Work In Progress-embargoed Not For Circulation Or Citation

services, combined with “modern, innovative technologies⁴.” Magnuson⁵ emphasizes FinTech as a “new breed” of companies “that specialize in providing financial services primarily through technologically enabled mobile and online platforms.” Varga expands definitions of FinTech by noting⁶ that the goal of such companies is to develop “novel, technology-enabled financial services” whose ultimate aim is to “transform current financial practices.” The Financial Stability Board (FSB) summarizes FinTech as “technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions, and the provision of financial services.”⁷

Other definitions describe FinTech in terms of the technological innovations that interact with financial services in a variety of ways - specifically, digital innovations and technology-enabled business model innovations⁸ and novel technologies adopted by financial institutions which are ultimately used to improve the quality of financial services⁹. Drasch et al. expect FinTech companies to bring these technology solutions and innovations to the financial sector to provide more effective financial products and services that bring the sector into the digital age¹⁰. Others refer to FinTech as an industry that uses (mobile-centered IT¹¹) technology to enhance the efficiency of the financial system¹².”

Arner et al. note that the term “FinTech” is not confined to specific sectors of the existing financial industry (e.g. financing) or business models (e.g. peer-to-peer (P2P) lending), but instead covers the entire scope of services and products traditionally provided by the

⁴ Dorfleitner, G., Hornuf, L., Schmitt, M., & Weber, M. (2017). Definition of FinTech and Description of the FinTech Industry. *FinTech in Germany*, 5–10. doi:10.1007/978-3-319-54666-7_2

⁵ Magnuson, William J., *Regulating Fintech* (August 26, 2017). Vanderbilt Law Review, Forthcoming; Texas A&M University School of Law Legal Studies Research Paper No. 17-55. Available at SSRN: <https://ssrn.com/abstract=3027525>

⁶ Varga, David. (2017). Fintech, the new era of financial services. *Vezetéstudomány / Budapest Management Review*. 48. 22-32. 10.14267/VEZTUD.2017.11.03.

⁷ *Financial Stability Implications From Fintech*. 2017. Ebook. Financial Stability Board. <https://www.fsb.org/wp-content/uploads/R270617.pdf>.

⁸ Philippon, T. (2016). The FinTech Opportunity. doi:10.3386/w22476

⁹ Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. *Journal of Network and Computer Applications*, 103, 262–273. doi:10.1016/j.jnca.2017.10.011

¹⁰ Drasch, B. J., Schweizer, A., & Urbach, N. (2018). Integrating the “Troublemakers”: A taxonomy for cooperation between banks and fintechs. *Journal of Economics and Business*. doi:10.1016/j.jeconbus.2018.04.002

¹¹ Kim, Yonghee & Park, Young-Ju & Choi, Jeongil & Yeon, Jiyoung. (2015). An Empirical Study on the Adoption of “Fintech” Service: Focused on Mobile Payment Services. 136-140.

¹² McAuley, Daniel. 2015. “What Is Fintech?”. *Medium*. <https://medium.com/wharton-fintech/what-is-fintech-77d3d5a3e677>.

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

financial services industry¹³. Gomber et al.¹⁴ refer to FinTech companies as both start-ups and established IT companies (often without a history in banking and/or financial services) entering the financial domain and evolving at the intersection of information and communication technology, specifically via the Internet and automated information processing, thereby disrupting the financial sector. Eickhoff reiterates that these companies operate at the intersection of (i) financial products and services and (ii) information technology, and they are usually (iii) relatively new companies (often startups) with (iv) their own innovative product or service offerings¹⁵. FinTech, therefore, is constructed such that it has three dimensions¹⁶: an input (namely the combination of technology, organization and money flow), mechanisms (create or improve or change, disrupt, apply technology to finance, create competition on the market) and an output (creation of new services or products or processes or business models). Milian et al. employ Christensen's (2003) theory of disruptive innovation to categorize these outputs of FinTech as "Sustainable Fintechs," for established financial service providers that work to protect their market positions by using IT through incremental innovations, and "Disruptive Fintechs" that are new companies and start-ups that challenge established providers by offering new technological products and services.¹⁷ We are thus presented with a mixed bag of definitions of FinTech. While the breadth of approaches in the literature to defining FinTech offers us a broad range of factors to consider, it also complicates attempts to create a comprehensive definition of the same. We agree with Dorfleitner et al.¹⁸ who note that it is not possible to construct a restrictive definition of "FinTech" that applies to all of the entities traditionally associated with the term. The area has an amorphous and evolving shape, and it is uncertain if and/or when its boundaries may set. However, for the purpose of laying a foundation for understanding its functions and regulatory responses, we summarize the reviewed definitions to arrive at the

¹³ Arner et al. (2015).

¹⁴ Gomber, P., Koch, J.-A., & Siering, M. (2017). *Digital Finance and FinTech: current research and future research directions*. *Journal of Business Economics*, 87(5), 537–580. doi:10.1007/s11573-017-0852-x

¹⁵ Eickhoff, M., Muntermann, J., & Weinrich, T. (2017). What do FinTechs actually do? A Taxonomy of FinTech Business Models. *ICIS*.

¹⁶ Zavolokina, Liudmila; Dolata, Mateusz; Schwabe, Gerhard (2016). FinTech – What's in a Name? In: Thirty Seventh International Conference on Information Systems, Dublin, Ireland, 11 December 2016 -14 December 2016

¹⁷ E.Z. Milian, M.d.M. Spinola, M.M. de Carvalho, Fintechs: A Literature Review and Research Agenda, *Electronic Commerce Research and Applications* (2019), doi: <https://doi.org/10.1016/j.elerap.2019.100833>

¹⁸ Dorfleitner et al.(2017).

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

following: FinTech describes a broad range of companies who develop technology-centred products that enhance the functionality of financial services as were typically offered by incumbent financial institutions (including banks & non-banking financial companies). We do not incorporate in this definition the form such enhancements may take, or the motivations for such enhancement, for reasons we will explain in later sections.

Need for these Rules

There may be an assumption amongst some that all Fintech entities are governed by the Reserve Bank of India which has a number of detailed guidelines regarding security standards. However, not all Fintech entities come under the jurisdiction of the Reserve Bank of India, which only has the powers conferred on it specifically under the Reserve Bank of India Act, 1934. Similarly the Securities and Exchange Board of India as well as the Insurance and Regulatory Development Authority only have powers to regulate entities specific to their sectors.

The burden of regulation the security standards of Fintech entities which do not fall under the regulations issued by the abovementioned authorities falls on the Information Technology Act, 2000, (“IT Act”) and more specifically on the rules issued pursuant to section 43A of the IT Act, called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (“SPDI Rules”).

Section 43A of the IT Act requires body corporates to comply with ‘reasonable security practices and procedures’ in order to avoid liability for negligence in dealing with data causing wrongful loss or gain (which liability may go upto Rupees Five crores). The explanation to section 43A states that in the absence of a contract specifying the security practices adopted by the body corporate, reasonable security practices and procedures will be those as specified in the SPDI Rules. Unfortunately even the SPDI Rules do not lay down any specific security standards or protocols but say that entities would be assumed to have implemented reasonable security practices and procedures if they have undertaken

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

measures that are commensurate with the information assets being protected with the nature of business.

The only specific standards that the SPDI Rules prescribe or refer to are the ISO27001 (or any other standards developed by an industry body which have been duly notified by the Central government). This means that if a body corporate has implemented the ISO27001 standard they shall be deemed to have complied with reasonable security practices and procedures as long as such standards have been certified or audited on a regular basis. The financial sector in India has to date not developed any sectoral security standards that have been approved by the Central government (as required by the SPDI Rules), meanwhile, we have learned from conversations with FinTech startups that ISO 27001 is an expensive standard for small businesses to implement. Therefore there appears to be a need for a set of security standards or guidelines that Fintech entities can look to implement which are specific and detailed enough to perhaps form a checklist but easier and more economical to implement than the ISO27001 standard or even the industry specific PCI DSS standard. It is precisely to fulfil this need that the Center for Internet and Society, along with (any future partners) have prepared these Draft Information Technology (Fintech Security Standards) Rules (“Fintech Rules”) to ensure that not only the data of users is dealt with in a secure and safe manner but also that the smaller businesses in the Fintech industry have a specific standard to look at in order to limit their liabilities for any future breaches.

A question may arise as to why have such specific rules only for the Fintech industry and not for other entities which deal with sensitive and personal data or information. The answer to this is rooted in the structure of section 43A of the IT Act, which provides for monetary damages for negligence in dealing with sensitive and personal data. It is assumed that losses due to negligence in dealing with financial data would be easier to quantify in monetary terms, and perhaps would affect users in a more direct manner than other forms of data.

Structure of the Rules

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

All industries or sectors may not necessarily need to be regulated through legal mandates and in some cases the goals of the legal mandate may be better achieved through self regulation rather than state regulation. Self-regulation can take many forms, but at a very basic level it involves a private organization assuming responsibilities for its own rules and practices and also overseeing the enforcement of these as against a government regulator doing the same under law. This can be done by way of each organization tailoring its own codes of conduct or any industry body (such as a trade association) establishing a common code or a set of principles and each individual firm modelling its policies for the implementation of such a code. Such a model of governance though has been criticized due to an overall lack of accountability and transparency, incomplete realization of the principles promulgated in common codes and weak oversight and enforcement.¹⁹ Though reverting back to a command and control regulatory model may not be the most efficient approach for many fledgling industries operating with new technologies as 1) the law would not be able to keep up with the latest developments and 2) excessive regulation could stifle the growth of such industries.

A middle path between the above two models is a co-regulatory framework which involves both the government and the industry coming together and sharing the responsibility of drafting and enforcing regulatory standards.²⁰ This allows the government and the industry body to negotiate proper regulatory goals, collaborate on the drafting of standards, and work in a cooperative manner to enforce the standards against firms which violate it. Furthermore, this approach may be better than the traditional regulatory regimes as 1) It draws on industry knowledge and expertise; 2) Yields rules that are more cost-effective, workable, and innovative; 3) It also creates a stronger sense of industry ownership over rules and thus better compliance; 4)The consultative process leads to rules that are more politically practicable and efficient.²¹ It is perhaps for this reason that the SPDI Rules also follow a co-regulatory mechanism, and these proposed Rules also seek to adopt a similar framework.

¹⁹ Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving beyond Voluntary Codes, 6 I/S J. L. POL. 355 (2011).

²⁰ Hans-Bredaw-Institut, Final Report: Study on Co-Regulation Measures in the Media Sector, 2006, (defining “co-regulation” as systems that “combine state- and non-state regulation” and contrasting it with self-regulation, which operates “without any state involvement”).

²¹ Hirsch, The Law and Policy of Online Privacy: Regulation, Self-regulation, or Co-regulation? 34 SEATTLE UNIV. L. REV. 439 (2011).

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

These Fintech Rules are not set up as a licensing requirement, i.e. Fintech Entities will not have to comply with these rules as a pre-condition to starting operations. They have been drafted in a manner similar to that of the SPDI Rules, i.e. as a measure to be implemented for Fintech Entities to absolve themselves of any liability against claims of negligence under section 43A of the IT Act. This means that there is no legal obligation on Fintech entities to comply with these rules, instead there is a commercial reason to do so, viz. if a Fintech entity adopts and implements the standards prescribed in these rules then they can legally absolve themselves from liability for damages on the grounds of negligence as specified under section 43A of the IT Act. Thus there is a business case for Fintech entities to implement these standards rather than a legal obligation; this approach should ensure that the data of users is well protected while at the same time ensuring that there is no unnecessary burden on the fledgling Fintech industry. If a Fintech entity believe that it is too small or deals with extremely small amounts of data, it can take a commercial decision (risk) on whether to comply with these standards at all or follow its own policies. If it chooses the latter, then in case of a data breach, it will have the obligation to prove in court that its policies comprise reasonable security practices and procedures.

The Rules have only a single set of standards which all Fintech entities would be required to follow, however if it is felt during stakeholder consultations that these standards may not adequately protect the interests of users in certain scenarios, perhaps Fintech entities which have an extremely large number of users, or large turnover, or are extremely data reliant, etc., then a classification may be made and Fintech entities which, it is felt, should comply with stricter standards could be required to comply with ISO27001 or other similar standards.

Work In Progress-embargoed Not For Circulation Or Citation

DRAFT MODEL FINTECH SECURITY STANDARDS

In exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely.--

1. Short Title and Commencement - (1) These Rules may be called the Information Technology (Fintech Security Standards) Rules, 2019.

(3) They shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

2. Definitions

(1) In Rules, unless the context otherwise requires,

(a) “body corporate” shall mean any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

Expl: This explanation has been adopted from section 43A of the Information Technology Act, 2000 since it is an expansive definition which covers almost all entities which would have a significant enough presence to require regulation while leaving out individuals working solely as individuals and not as a commercial venture.

(b) “cyber security incident” shall mean any real or suspected adverse event in relation to cyber security that violates an explicit or implied security policy resulting in unauthorized access, denial of service/ disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization;

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

Expl: This definition has been adopted from the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

- (c) “Data Protection Officer” shall mean the person so designated by a Qualified Fintech Entity under sub-clause (1) of Rule 4;
- (d) “Fintech Entity” means a body corporate which deals with technology-centred products that enhance the functionality of financial services as were typically offered by incumbent financial institutions (including banks and non-banking financial companies), and the term Fintech shall be construed accordingly.

Expl: Please refer to the Background note for more details on this definition.

- (f) “Offering services in India” shall mean (a) enabling legal or natural persons in India to use the Fintech services offered by it; and (b) having a substantial presence in India.

Explanation: The term “substantial presence in India” may be said to exist where the Fintech Entity has an establishment in India. In the absence of an establishment in India, the criterion of a substantial presence shall be determined on the basis of the existence of a significant number of users or the targeting of activities in India. The targeting of activities can be determined on the basis of relevant circumstances, including factors such as the use of Indian currency, providing local advertising, handling of customer relations such as by providing customer service in local languages generally used in India, etc.

Expl: These terms and the Explanation have been adopted from the new E-evidence Directive of the European Union since they provide a good balance between those offering services in India but excludes entities who have a miniscule presence or whose activities are not geared towards India so that compliance does not become a burden to commercial activity.

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

(g) “Qualified Fintech Entities” shall mean Fintech Entities offering services in India and possessing, dealing or handling any financial data or information of their customers.

Expl: This definition ensures that only entities which satisfy two conditions have to comply with the security standards prescribed in this regulation; (i) they should be offering services in India; and (ii) they should be possessing, dealing or handling “vital data or information”. This dual qualification ensure that (i) not all Fintech entities around the world get covered by this legislation unless they have a significant presence or interest in India; and (ii) Fintech entities which do not possess or deal with vital information are not required to comply with the potentially strict data protection.

(g) “Sensitive personal data or information” shall have the same meaning as ascribed to it in Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Security Standards

(1) Notwithstanding anything contained in any other law for the time being in force, a Qualified Fintech Entity shall have an obligation to maintain confidentiality in relation to any Sensitive personal data or information of its users that is dealt with, handled by or in its possession.

Expl: This is a generic obligation to maintain confidentiality in relation to the financial data of their users.

(2) All Qualified Fintech Entities shall have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.[1] These information security policies shall be updated and upgraded from time to time as may be necessary to ensure that the vital data and information is safe.[2] Subject to the provisions of sub-section (3) below, a Qualified Fintech Entity shall be

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

deemed to have put in place reasonable security practices and procedures if it has implemented such security practices and standards as prescribed in the Schedule to these Rules notified under this section.

Expl: This is the main section providing an obligation to put in place adequate and documented security systems which should be commensurate with the nature of the business of the entity. This requirement of the systems being commensurate with the nature of the business has been adopted from Rule 8 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 which automatically puts an obligation on the entity to ensure that the security systems for sensitive information are more stringent than for other information. There is an added obligation to ensure that the systems are upgraded from time to time to ensure that they are capable of meeting the latest challenges. The way these Rules are structured, Fintech Entities that believe they are too small to be able to spend any resources on data security have an option to not put in place the security systems provided herein, but if they do not then they expose themselves to the risk of paying damages of upto Rs. 5 crore under section 43A of the IT Act.

(3) Any industry association of Fintech Entities or an entity formed by such an association, which has developed codes of best practices for data protection shall get its codes of best practices duly approved and notified by the Central Government for effective implementation. All Qualified Fintech Entities in the relevant sector, whether registered with the industry association or not, shall be required to implement any such codes notified by the Central Government within a reasonable time.

Expl: This sort of a co-regulation mechanism has been adopted from the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 with the added requirement that once such codes are notified by the Government all Fintech Entities in the relevant sector will have to follow those codes, whether they are a member of the industry body (whose code has been approved) or not. This sentence has been

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

added to ensure that Fintech Entities do not escape their obligation by not joining industry bodies or in case a particular sector has more than one industry body.

4. Breach Notification to CERT-In

(1) A Fintech Entity offering services in India which experiences a cyber security incident, shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the incident to the Indian Computer Emergency Response Team (CERT-In) as per the requirements of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

(2) The incident notice by the Fintech Entity above shall (a) describe the nature of the cyber security incident including where possible, the categories and approximate amount of the data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the cyber security incident; (d) describe the measures taken or proposed to be taken by the Fintech Entity to address the cyber security incident, including, where appropriate, measures to mitigate its possible adverse effects.

Expl: This clause reiterates the obligation to report incidents which is contained in the CERT-In Rules. The clause has been included here for the purpose of clarity and in order to not cause any confusion it refers back to the CERT-In Rules. The extra requirement of what the notice should contain has been adopted and modified from the EU GDPR. The reporting obligation here is to all Fintech Entities offering services in India whether dealing with personal information or not, which is why the term Qualified Fintech Entities is not used here.

5. Breach Notification to Users

(1) A Qualified Fintech Entity which experiences a cyber security incident which is likely to result in a high risk to the rights and freedoms of its users or is likely to cause any loss or damage

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

to such users, the Qualified Fintech Entity shall communicate such incident to the users without undue delay.

(2) The incident notice by the Qualified Fintech Entity above shall (a) describe the nature of the cyber security incident including where possible, the categories and approximate number of users concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the cyber security incident; (d) describe the measures taken or proposed to be taken by the controller to address the cyber security incident, including, where appropriate, measures to mitigate its possible adverse effects.

Expl: This clause has been adopted and modified from the EU GDPR. The obligation to report the incident is only upon Qualified Fintech Entities, i.e. those which deal in vital data and only kicks in if there is a likelihood of such breach causing a high risk to the rights and freedoms of its users. The safe harbor given in the GDPR which exempts data processors from reporting personal data breaches in certain circumstances such as encryption, etc. have not been included as of now since this sets a higher standard for reporting.

6. Exclusion

No provisions of these Rules shall apply to Bodes corporate which are under the regulatory supervision of the Reserve Bank of India, the Securities and Exchange Board of India or the Insurance and Regulatory Development Authority and are required to follow security standards specifically prescribed by said authorities.

Expl: The explanation clarifies that if a Fintech Entity is governed by security standards prescribed by the RBI, SEBI or IRDA, which may have their own security standards for entities regulated by them, then such entities do not have to comply with these guidelines.

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

SCHEDULE I

FINTECH SECURITY GUIDELINES

Every Qualified Fintech Entity shall put in place procedures and processes to ensure robust information security procedures as specified below:

1. IT Governance

IT governance should be overseen by senior members of the management, particularly the CEO and CIO. Every Qualified Fintech Entity must have a person designated as the Chief Information Officer (CIO). The person designated as CIO may also hold other designations. These members must oversee and manage IT strategy and policy with a strategic planning process.

IT policies and procedures must:

- lay down standards for hardware or software prescribed by the proposed architecture;
- lay down strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development;
- detail operational procedures for IT infrastructure, such as data centre operations;
- implement appropriate measures to ensure adherence to customer privacy requirements applicable to relevant jurisdictions;
- implement appropriate measures to comply with legislative, regulatory and contractual requirements on the use of systems and software where IPR, copyrights and on the use of proprietary software products are applicable;
- consider inter-dependencies between risk elements in the risk assessment process;
- ensure procedures to assess the integration and interoperability of complex IT processes (such as problem, change and configuration management) exists.

2. Information Security Governance

Information Security (or Infosec) governance as an area of IT governance, must consider information security as a critical strand of business strategy, with appropriate measuring, monitoring and reporting of InfoSec parameters, and the management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level.

A comprehensive security programme needs to include the following main activities:

- Development and ongoing maintenance of security policies;

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

- Sharing of roles, responsibilities and accountability for information security across the organization;
- Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures;
- Periodic risk assessments and ensuring adequate, effective and tested controls for people, processes and technology to enhance information security;
- Ensuring security is integral to all organizational processes;
- Processes to monitor security incidents;
- Effective identity and access management processes;
- Generation of meaningful metrics of security performance.

Chief InfoSec Officer (CISO)

A senior level official who has the necessary levels of access in the enterprise, working with the CIO, should be designated as Chief Information Security Officer, responsible for articulating and enforcing the policies that FinTech companies must use to protect their information assets apart from coordinating the security related issues/implementation within the organization as well as relevant external agencies.

3. Critical components of information security

1.Policies and Procedures

- A. In addition to those mentioned in section 1 extended to InfoSec, there are other specific considerations:
- i. Identification, authorisation and granting of access to IT assets (by individuals and other IT assets);
 - ii. Addressing the various stages of an IT asset's life to ensure that information security requirements are considered at each stage of the lifecycle;
 - iv. Management of technology solutions for information security like a firewall, anti-virus/anti-malware software, intrusion detection/prevention systems, cryptographic systems and monitoring/log analysis tools/techniques;
 - v. Clearly indicating acceptable usage of IT assets including application systems that define the information security responsibilities of users (staff, service providers and customers) in regard to the use of IT assets;
 - ix. Exception policy for handling instances of non-compliance with the information security policy;
 - x. Penal measures for violation of policies and the process to be followed in the event of violation.

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

2. Risk Assessment

The risk assessment for the enterprise must, for each asset - physical, informational, computer, and/or digital etc - within its scope, identify the threat/vulnerability combinations that have a likelihood of impacting the confidentiality, availability or integrity of that asset - from a business, compliance or contractual perspective.

4. Defining roles and responsibilities

All defined and documented responsibilities and accountabilities must be established and communicated to all relevant personnel and management.

5. Access Control

(i) Access to information assets needs to be authorised by an enterprise only where a valid business need exists and only for the specific time period that the access is required. The various factors that need to be considered when authorising access to users and information assets, inter-alia, include business role, physical location, method of connectivity, remote access, time, anti-malware and patch updation status, nature of device used and software /operating system.

[(ii) Among the important controls that Qualified Fintech Entities need to consider are:

(a) Implementation of (unique, auditable) role-based access control policies designed to ensure effective segregation of duties;

(b) Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment;

(c) Audit of logging and monitoring of access to IT assets by all users;

(d) Applying the four-eyes principle to very critical/sensitive IT assets.]²²

(iii) A mutual authentication system may be considered.

²² Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

Work In Progress-embargoed Not For Circulation Or Citation

(iv) Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures.

6. Design Controls

Planning and design level controls need to be in place to ensure that information security is embodied in the overall information systems architecture and the implemented solutions are in compliance with the information security policies and requirements of the enterprise.

7. Personnel security

[(i) Risk exposures from internal users include altering data, deleting production and back-up data, disrupting/destroying systems, misusing systems for personal gain or to damage the institution, holding data hostage and stealing strategic or customer data for espionage or fraud schemes.]²³

Personnel-driven risk must be mitigated through background checks and verifications, and verification of government ID. There also needs to be a periodic rotation of duties among users or personnel as a prudent risk measure.

8. Physical security

(i) Physical security risks are mitigated through zone-oriented implementations that are a function of the sensitivity of the data contained or accessible through the zone and the information technology components in the zone.

(ii) The requirements for each zone should be determined through the risk assessment. The risk assessment should include, but is not limited to, threats like chemical effects, dust, electrical supply interference, electromagnetic radiation, explosives, fire, smoke, theft/destruction, vibration/earthquake, water, criminals, terrorism, political issues (e.g. strikes, disruptions) and other threats based on the entity's unique geographical location, building configuration, neighboring environment/entities, etc.

(iii) An enterprise needs to deploy the following environmental controls with adequate protection measures:

- Secure location of critical assets providing protection from natural and man-made threats;

²³ Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

Work In Progress-embargoed Not For Circulation Or Citation

- Restrict access to sensitive areas like data centres, which also includes detailed procedures for handling access by staff, third party providers and visitors;
- Monitoring mechanisms for the detection of compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access log reviews, etc.

9. User Training and Awareness

There needs to be initial, and periodic, security and confidentiality training for all employees, appropriate to their roles and responsibilities. *[There needs to be a mechanism to track the effectiveness of training programmes through an assessment/testing process designed on testing the understanding of the relevant information security policies, not only initially but also on a periodic basis.]*²⁴

10. Incident management

- (i) Common incident types include, but not limited to, outages/degradation of services due to hardware, software or capacity issues, unauthorised access to systems, identity theft, data leakage/loss, malicious software and hardware, failed backup processes, denial of service attacks and data integrity issues.
- (ii) Major activities that need to be considered as part of the incident management framework include:
 - a. Developing and implementing processes for preventing, detecting, analyzing and responding to information security incidents
 - b. Establishing escalation and communication processes and lines of authority
 - c. Developing plans to respond to and document information security incidents
 - d. Establishing the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing, etc.
 - e. Developing a process to communicate with internal parties and external organizations (e.g., regulator, media, law enforcement, customers)
 - f. Organizing, training and equipping teams to respond to information security incidents
 - h. Periodically testing and refining information security incident response plans
 - i. Conducting post-mortem analysis and reviews to identify causes of information security incidents, developing corrective actions and reassessing risk, and adjusting controls suitably to reduce the related risks in the future

²⁴ Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

Work In Progress-embargoed Not For Circulation Or Citation

(iii) Incident management strategies would also typically assist in compliance with regulatory requirements. Institutions would also need to proactively notify CERT-In/IDRBT/RBI regarding cyber security incidents.

(iv) All security incidents or violations of security policies should be brought to the notice of the CISO.

[12. Migration controls

(i) There needs to be a documented Migration Policy indicating the requirement of roadmap / migration plan / methodology for data migration (which includes verification of completeness, consistency, confidentiality, continuity and integrity of the migration activity and pre and post migration activities along with responsibilities and timelines for completion of same).

Explicit sign offs from users/application owners need to be obtained after each stage of migration and after complete migration process. Audit trails need to be available to document the conversion, including data mappings and transformations.]²⁵

13. Encryption

(ii) Typical areas or situations requiring deployment of cryptographic techniques, given the risks involved, include transmission and storage of critical and/or sensitive data/information in an ‘un-trusted’ environment or where a higher degree of security is required, detection of any unauthorised alteration of data/information and verification of the authenticity of transactions or data/information.

(iii) Since security is primarily based on the encryption keys, effective key management is crucial. Effective key management systems are based on an agreed set of standards, procedures, and secure methods that address key generation, storage, confidentiality, and recovery. *[It is recommended that there is no human intervention in the generation and management. It is expected that Qualified Fintech Entities will properly evaluate security requirements associated with their systems and adopt an encryption solution that is commensurate with the degree of confidentiality and integrity required and adherent to strong security standards.]²⁶*

14. Data security

²⁵ Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

²⁶ Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

Work In Progress-embargoed Not For Circulation Or Citation

i. Qualified Fintech Entities need to define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives, as indicated throughout.

ii. Policies regarding media handling, disposal, and transit should be implemented to enable the use of protection profiles and otherwise mitigate risks to data.

*[iii. There should be secure storage of media, with adequate access, as well as physical and environmental controls. More sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimize the distribution of sensitive information through non- or less-secure means.]*²⁷

iv. Appropriate disposal techniques for both electronic and physical media should be applied to sensitive data like physical destruction, overwriting data, degaussing etc.

*[v. Qualified Fintech Entities should maintain the security of media while in transit or when shared with third parties. Policies should include contractual requirements that incorporate necessary risk-based controls, restrictions on the carriers used and procedures to verify the identity of couriers.]*²⁸

vi. Qualified Fintech Entities should encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.

vii. Data leak prevention (DLP) software solutions may be implemented to:

- Locate and catalogue sensitive information stored throughout the enterprise;
- Monitor and control the movement of sensitive information across enterprise networks;
- Monitor and control the movement of sensitive information on end-user systems.

15. Vulnerability Assessment

a. Automated vulnerability scanning tools need to be used against all systems on enterprise networks on a periodic basis.

b. Qualified Fintech Entities should ensure that vulnerability scanning is performed in an authenticated mode (i.e., configuring the scanner with administrator credentials) at least quarterly.

c. Vulnerability assessments must generally accept a low level of business risk.

²⁷ Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

²⁸ Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

Work In Progress-embargoed Not For Circulation Or Citation

d. The security function should have updated status regarding numbers of unmitigated, critical vulnerabilities, plan for mitigation and should share vulnerability reports indicating critical issues with senior management to provide effective incentives for mitigation.

16. Establishing on-going security monitoring processes

i. Common monitoring processes include activity logging (including exceptions to approved activity), for example, device, server, network activity, security sensor alerts; monitoring staff or third-party access to sensitive data/information to ensure it is for a valid business reason, scanning host systems for known vulnerabilities, checks to determine if information security controls are operating as expected and are being complied with, checking whether powerful utilities / commands have been disabled on attached hosts, environment profiling, checking for the existence and configuration of unauthorised wireless networks by using automated tools, discovering the existence of unauthorised systems by using network discovery and mapping tools and detecting unauthorised changes to electronic documents and configuration files by using file integrity monitoring software.

[ii. Qualified Fintech Entities would need to establish a clear allocation of responsibility for regular monitoring, and the processes and tools in this regard should be in a position to manage the volume of monitoring required, thereby reducing the risk of an incident going undetected.

iii. Highly sensitive and/or critical IT assets would need to have logging enabled to record events and monitored at a level proportional to the level of risk.

iv. Qualified Fintech Entities should regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.]²⁹

v. On a periodic basis, say monthly or quarterly basis, entities should require that managers match active employees and contractors with each account belonging to their managed staff. Security/system administrators should then disable accounts that are not assigned to active employees or contractors.

vi. Qualified Fintech Entities must implement audit logging and should validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries.

[vii. System administrators and information security personnel should consider devising profiles of common events from given systems, so that they can tune detection to focus on unusual activity, reducing

²⁹ Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

Work In Progress-embargoed Not For Circulation Or Citation

false positives, more rapidly identify anomalies, and prevent overwhelming the analysts with insignificant alerts.

viii. *Technologies/factors that provide capabilities for effective attack detection and analysis may include Security Information and Event Management (SIEM), Intrusion Detection and Prevention System (IDS and IPS), Network Behaviour Analysis (NBA), and Managed Security Service Provider (MSSP).]*³⁰

ix. Qualified Fintech Entities also need to pro-actively monitor various authentic sources like CERT-In, security vendors, etc. for any security related advisories and take suitable measures accordingly.

17. Security measures against Malware

i. Typical controls to protect against malware use layered combinations of technology, policies and procedures and training. The controls are of preventive and detective/corrective in nature applied at the host, network, and user levels:

- At host level: The various measures at the host level include host hardening(including patch application and proper security configurations of the operating system (OS), browsers, and other network-aware software), considering implementing host-based firewalls on each internal computer and especially laptops assigned to mobile users.
- At network level: The various measures include limiting the transfer of executable files through the perimeter, IDS and IPS monitoring of incoming and outgoing network traffic, including anti-virus, anti-spyware and signature and anomaly-based traffic monitors, routing Access Control Lists(ACLs) that limit incoming and outgoing connections as well as internal connections to those necessary for business purposes, proxy servers that inspect incoming and outgoing packets for indicators of malicious code and block access to known or suspected malware distribution servers, filtering to protect against attacks such as cross-site scripting and SQL injection.
- At user level: User education in awareness, safe computing practices, indicators of malicious code, and response actions.

ii. In addition to system-wide antivirus/anti-malware software, logs from firewalls, intrusion detection and prevention sensors, DNS servers and proxy server logs should be monitored on a daily basis for signs of worm infections including but not limited to:

- Outbound SMTP connection attempts from anything other than a bank's SMTP mail gateways;
- Excessive or unusual scanning on TCP and UDP ports 135-139 and 445;

³⁰ Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

Work In Progress-embargoed Not For Circulation Or Citation

- Connection attempts on IRC or any other ports that are unusual for the environment;
- Excessive attempts from internal systems to access non-business websites;
- Excessive traffic from individual or a group of internal systems;
- Excessive DNS queries from internal systems to the same host name and for known “nonexistent” host names.

iii. Qualified Fintech Entities should configure laptops, workstations, and servers so that they do not auto-run content from USB tokens, USB hard drives, CDs/DVDs, external SATA devices, mounted network shares, or other removable media and conduct an automated antimalware scan of removable media when it is inserted.

iv. Qualified Fintech Entities can also consider deploying the Network Access Control (NAC) tools to verify security configuration and patch level compliance of devices before granting access to a network.

v. Email Attachment Filtering - Qualified Fintech Entities should filter various attachment types at the email gateway, unless required for specific business use.

18. Patch Management

i. A Patch Management process needs to be in place to address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising with documented standards / procedures.

ii. Organizations should measure the delay in patching new vulnerabilities and ensure the delay is not beyond the benchmarks set forth by the organization, which should be less for critical patches, say not more than a week

iii. Critical patches must be evaluated in a test environment before being updated into production on enterprise systems. If such patches break critical business applications on test machines, the organization must devise other mitigating controls that block exploitation on systems where the patch is difficult to be deployed because of its impact on business functionality.

19. Change Management

i. A change management process should be established, which covers all types of change. For example, upgrades and modifications to application and software, modifications to business information, emergency ‘fixes’, and changes to the computers/networks that support the application.

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

[ii. The change management process should be documented, and includes assessing potential risk impacts of changes, approving and testing changes to ensure that they do not compromise security controls, performing changes and signing them off to ensure they are made correctly and securely, reviewing completed changes to ensure that no unauthorised changes have been made.

iii. Changes to the application should be performed by skilled and competent individuals who are capable of making changes correctly and securely and signed off by an appropriate member of the management.]

31

20. Audit trails

i. Qualified Fintech Entities need to ensure that audit trails exist for IT assets satisfying business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. This could include, as applicable, various areas like transaction with financial consequences, the opening, modifications or closing of customer accounts, modifications in sensitive master data, accessing or copying of sensitive data/information; and granting, modification or revocation of systems access rights or privileges for accessing sensitive IT assets.

ii. Audit trails should be secured to ensure the integrity of the information captured through encryption, including the preservation of evidence. Retention of audit trails should be in line with business, regulatory and legal requirements.

[iii. Network and host activities typically must be recorded in a central logging facility which may process the logging data into a common format, in a 'normalization' process.

iv. Other aspects related to logging to be considered include:

- a. All remote access to an internal network, whether through VPN, dial-up, or other mechanism, should be logged verbosely;*
- b. Operating systems should be configured to log access control events associated with a user attempting to access a resource like a file or directory without the appropriate permissions;*
- c. Security personnel and/or administrators designated in this regard should identify anomalies in logs and actively review the anomalies, documenting their findings on an ongoing basis;*
- d. Network boundary devices, including firewalls, network-based IPSs, and inbound and outbound proxies may be configured to log verbosely all traffic (both allowed and blocked) arriving at the device.]*

³¹ Portions that have been italicised may be deleted unless it is felt that they are absolutely essential for data protection in a small scale Fintech start-up.

Work In Progress-embargoed Not For Circulation Or Citation

21. Network Security

i. Defense in depth (multiple layers of defenses) for most organizations should at least consider the following two areas:

- (a) Protecting the enclave boundaries or perimeter;
- (b) Protecting the computing environment.

ii. The enclave boundary is the point at which the organization's network interacts with the Internet. To control the flow of traffic through network borders and counter attacks and evidence of compromised machines, boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based Intrusion Prevention Systems and Intrusion Detection Systems.

iii. Effective security deployment relies on carefully configured boundary defenses that separate networks with different threat levels, different sets of users, and different levels of control. Effective multi-layered defenses of perimeter networks help to lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

iv. An effective approach to securing a large network involves dividing the network into logical security domains.

v. Organizations can determine the most effective deployment of protocols, filtering routers, firewalls, gateways, proxy servers, and/or physical isolation to restrict access with a clear understanding of network connectivity. Some applications and business processes may require complete segregation from the corporate network. Others may restrict access by placing the services that must be accessed by each zone in their own security domain, commonly called a Demilitarized Zone.

vi. Perimeter controls for security domains may include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as DNS. The perimeter controls may exist on separate devices or be combined or consolidated on one or more devices. Consolidation on a single device could improve security by reducing administrative overhead. However, consolidation may increase risk through a reduced ability to perform certain functions and the existence of a single point of failure.

vii. Network protection devices that may be implemented include

- firewalls (packet filter/stateful inspection/proxy-server/application-level) with the requisite firewall policies. Given the importance of firewalls as a means of access control, good firewall related practices include:
 - Using a rule set that disallows all inbound and outbound traffic that is not specifically allowed

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

- Using NAT and split DNS to hide internal system names and addresses from external networks
- Using proxy connections for outbound HTTP connections and filtering malicious code
- Hardening the firewall by removing all unnecessary services and appropriately patching, enhancing, and maintaining all software on the firewall unit
- Restricting network mapping capabilities through the firewall, primarily by blocking inbound ICMP (Internet Control Messaging Protocol) traffic
- Backing up firewalls to internal media and not backing up the firewall to servers on protected networks
- Logging activity, with daily administrator review and limiting administrative access to few individuals
- Using security monitoring devices and practices to monitor actions on the firewall and to monitor communications allowed through the firewall
- Administering the firewall using encrypted communications and strong authentication, accessing the firewall only from secure devices, and monitoring all administrative access
- Making changes only through well-administered change control procedures.
- Network Intrusion Detection Systems (NIDS) and Network Intrusion Prevention Systems (NIPS)
- Quarantines
- Optimal DNS placement (such as split DNS)

viii. In addition to the above, the following are among the factors that need to be followed for improving the security of networks:

- a. Establishing strong controls over any medium that is used as a backdoor into the critical network. If backdoors or vendor connections do exist in critical systems, strong authentication must be implemented to ensure secure communications.
- b. Establishing critical "Red Teams" to identify and evaluate possible attack scenarios. There is a need to feed information resulting from the "Red Team" evaluation into risk management processes to assess the information and establish appropriate protection strategies.
- c. Documenting network architecture and identifying systems that serve critical functions or contain sensitive information that require additional levels of protection.
- d. Network control functions should be performed by individuals possessing adequate training and experience, and the duties should be rotated on a regular basis, where possible. Network control software must restrict operator access from performing certain functions (e.g., the ability to amend/delete operator activity logs) outside desired access level.

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

- e. Network control software should maintain an audit trail of all operator activities.
- f. Another important security improvement is the ability to identify users at every step of their activity.

22. Remote Access

- i. Good controls for remote access include the following actions:
 - a. Disallowing remote access by policy and practice unless a compelling business need exists. Here, management approval would be required for remote access;
 - b. Regularly review remote access approvals and rescind those that no longer have a compelling business justification;
 - c. Appropriately and in a timely manner patching, updating and maintain all software on remote access devices;
 - d. Using encryption to protect communications between the access device and the organization and to protect sensitive data residing on the access device;
 - e. Using VLANs, network segments, directories, and other techniques to restrict remote access to authorized network areas and applications within the institution;
 - f. Maintaining strong audit mechanisms for remote access actions;
 - g. Requiring a two-factor authentication process for remote access (e.g., PIN based token card with a one-time random password generator, or token based PKI);
 - h. Implementing controls consistent with the sensitivity of remote use.
- ii. While using TCP/IP Internet-based remote access, organizations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Using VPNs, however, has its own set of challenges. The encrypted traffic can hide unauthorized actions or malicious software that can be transmitted through such channels. IDSes/virus scanners able to decrypt the traffic for analysis and then encrypt and forward it to the VPN endpoint should be considered as preventive controls. Use of VPN concentrators may also be beneficial

23. Wireless Security

- i. Alongside extensive use of encryption to authenticate users and devices and to shield communications, wireless networks are recommended to use additional controls such as:
 - Treating wireless networks as untrusted networks, allowing access through protective devices similar to those used to shield the internal network from the Internet environment;

Work In Progress-embargoed Not For Circulation Or Citation

Work In Progress-embargoed Not For Circulation Or Citation

- Using end-to-end encryption in addition to the encryption provided by the wireless connection;
 - Using strong authentication and configuration controls at the access points and on all clients;
 - Using an application server and dumb terminals;
 - Shielding the area in which the wireless LAN operates to protect against stray emissions and signal interference;
 - Monitoring and responding to unauthorized wireless access points and clients.
- ii. All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by Information Security functionary of the enterprise. These Access Points / Base Stations need to be subjected to periodic penetration tests and audits. Access points/Wireless NIC should not be installed /enabled on a bank's network without the approval of information security function.
- iii. Each wireless device connected to the network must match an authorized configuration and security profile, with a documented owner of the connection and a defined business need, or be denied access
- iv. Network vulnerability scanning tools should be configured to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.
- v. Qualified Fintech Entities should use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromise. In addition to WIDS, all wireless traffic should be monitored by a wired IDS as traffic passes into the wired network.
- vi. For devices that do not have an essential wireless business purpose, organizations should consider disabling wireless access in the hardware configuration (BIOS or EFI), with password protections to lower the possibility that the user will override such configurations.
- vii. Organizations should ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection, with authentication protocols such as EAP/TLS or PEAP, which provide credential protection and mutual authentication.
- viii. Qualified Fintech Entities should disable peer-to-peer wireless network capabilities and peripheral access (such as through Bluetooth) on wireless clients, unless such functionality meets a documented business need.

Work In Progress-embargoed Not For Circulation Or Citation