**Prepared for FinTech Infrastructure Working Group**

**COMMENTARY**

* Should we harmonize with the ‘NICE' Framework (US standards)?
* This can underpin the UK standards, as the latter are compact.

**Fintech Markets**

Based on the nature of sensitivity of data being passed among users, standards and best practices are recommended per category.

Measures that should be taken into consideration for any start-up branching in this space are:

1) Creation of Continuity | Contingency Plan

2) Layers of Security in Each Segment/Layer

3) Storage and Back Up of Data

4) Data Captured and Usage

5) Protection of Data

6) Defining External / Third- Party Integration

7) Risk Management and Planning

8) Compliance

9) Terms and Conditions

10) Discussion Between Your Start Up and Network Provider | Telecommunications

11) Documentation

12) Data Handling in open networks (if applicable)

13) Cyber security

|  |  |
| --- | --- |
| **Type** | **Best Practice / Standards** |
| **Payment Specification** | PCI DSS  ISO 27001  ISO 8583  PA – DSS  SOC2  Standards for MasterCard using IP-based or Wireless Communication |
| **Web Servers** | SSL/ TLS and firewall  OWASP top 10  Prevention mechanisms for cross site scripting  Implementation of key pair Public and Private Keys / Cryptographic Keys  DDOS Prevention  Back Ups  Network Monitoring  Anti Virus Malware Scanning  Access Restriction  User Permissions  Use of SSH Keys to access servers  Measures to Prevent Database Injections  Strong Passwords (Generated keys)  Server and Web application Updates ( especially concerning Security)  Disaster Recovery |
| **Hardware for Payment POS Transactions** | EMVco Certification  EMV Module Version 8.1.0  POI (Point of Interaction) V4  Approval Class PED (Pin Entry Device)  Tripe DES (TDES) Master Key encryption – fixed  DUKPT format  SSL v3 (minimum)  TLS v1.2 (recommended)  Tamper Evidence |
|  |  |
|  |  |

**1) Lending (Lend Tech) - CP, TC**

The process of using online platforms/digital platforms to assess borrowers’ credit worthiness quickly based on the information submitted online and automate the underwriting process.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** | **Certification Level** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**2) Consumer Banking (Bank Tech) - CP, SF,**

Digital bank accounts can be created for underbanked consumers who are unable to access banking services or get approval for credit card or prepaid cards.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** | **Certification Level** |
| **Payment Specification** | PCI DSS  ISO 27001  ISO 8583  PA – DSS  SOC2  Standards For MasterCard using IP-based or Wireless Communication |  |  |
| **Web Servers** | SSL/ TLS and firewall  OWASP top 10  Prevention mechanisms for cross site scripting  Implementation of key pair Public and Private Keys / Cryptographic Keys  DDOS Prevention  Back Ups  Network Monitoring  Anti Virus Malware Scanning  Access Restriction  User Permissions  Use of SSH Keys to access servers  Measures to Prevent Database Injections  Strong Passwords (Generated keys)  Server and Web application Updates ( especially concerning Security)  Disaster Recovery |  |  |
| **Hardware for Payment POS Transactions** | EMVco Certification  EMV Module Version 8.1.0  POI (Point of Interaction) V4  Approval Class PED (Pin Entry Device)  Tripe DES (TDES) Master Key encryption – fixed  DUKPT format  SSL v3 (minimum)  TLS v1.2 (recommended)  Tamper Evidence |  |  |

**3) Payments (PayTech) - GL, SM**

The management of assets and processing of various payment transactions is made secure and easy.Types of technology being developed for consumers to facilitate better digital connectivity and consumer identity protection are:

a) Wearable technology

b) Smart Technology

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** | **Certification Level** |
| **Message Specification** | ISO 8583 |  |  |
|  |  |  |  |
|  |  |  |  |

**4) Mobile Payment GL, SM**

Mobile wallets and other integrated payment solutions are being used widely by business models and individuals to facilitate and conduct payment operations through the use of technology.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** | **Certification Level** |
| **Message Specification** | ISO 8583 |  |  |
|  |  |  |  |
|  |  |  |  |

**5) Insurance (Insur Tech) - GL**

This includes everything from online policy handling, data protection and providing tailored insurances.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** | **Certification Level** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**6) International Money Transfer - AZ**

This area makes the whole process more streamlined, secure, faster, and easier for the consumers and business models.Sending money overseas through the use of Peer-to-Peer networks helps in reducing fees incurred normally by traditional means.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** | **Certification Level** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**7) Personal Finance (Wealth Tech) - MD**

This area offers advice and help with budgeting. Consumers can get personal finance advice anywhere, at any time. Some consumers create budgets, while others help consumers save or plan and give retirement or investment advice.WealthTech aids the simplification of the investment process, whereby investors can manage their investment portfolios.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** | **Certification Level** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**8) Equity Financing – CF, MD (e.g Start Engine)**

This area makes it easy for businesses to raise money. Some companies work to connect accredited investors with vetted startups. Others use a crowdfunding model and let anyone invest in new businesses.These companies simplify the fundraising process for businesses. Virtual fundraising is also easier for investors, since everything can be done online.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards/ Best Practice** | **Description** | **Certification Level** |
| **Third Party Usage** | Analyze :   1. Data security 2. Privacy Compliance 3. Cyber Insurance 4. Access They have(if they do, get a risk assessment annually) |  |  |
| **Application and Infrastructure** | Implementation of Cybersecurity  \*Web Servers  ISO 27001  ISO 27002 |  |  |
| **Transactions/ Payment Management** | PCI DSS  PA-DSS  ISO 8583 |  |  |

**9) Trading (Trade Tech) - GL, TC, CP**

This area encompasses the application of information technology in an effort to reduce the information costs of international trade, facilitate trade finance, and increase transparency in trading operations for business models and consumers alike. International coordination is highly needed for the full potential and benefits to be realized.

TradeTech is used to facilitate and support cross-border trading through the use of IT systems in supply chain finance and asset distribution platforms.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** | **Certification Level** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**10) Accounting - BD**

The use of technology in this area of finances has helped improve the access and analysis of data through the use of software and tools.

The time accountants’ need to process operations like invoice management, cash flow forecasting, and other accounting services has been reduced through the use of financial technology and software.

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** | **Certification Level** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**11) RegTech** - LK, SF

RegTech is used to standardize and facilitate transparent regulatory processes that automate the whole compliance system. Regulatory reporting, risk management, transaction monitoring, and compliance.

- this area seeks to help financial service firms meet industry compliance rules, especially those covering Anti-Money Laundering and Know Your Customer protocols which fight fraud.RegTech can create sustainable and scalable ways for institutions to conduct a variety of compliance functions:

* + - * Automation of customer onboarding
  + Customer identity verification and management(KYC)
  + Real-time transaction monitoring
  + Improved fraud control
  + Secure financial information
  + Control over internal business processes
  + Tracking, analytics and scanning of regional and country regulatory changes
  + Proactive identification and reporting of regulatory risks
  + Automated mapping of regulatory risks to key business processes
  + Leveraging big data to extract market and customer insights

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Standards** | **Description** |  |
| **Data Security** | ISO 27001, 27002 | Cloud processing data security | Self cert, 3rd party |
| **Data security** | SOC2 | US CPA equivalent of ISO27001 - covers security, privacy, confidentiality, availability, and process integrity | Type I, Type II |
| **Data security** | ISO 31000 | Provides a level of reassurance in terms of economic resilience, professional reputation and environmental and safety outcomes. In a world of uncertainty, ISO 31000 is tailor-made for any organization seeking clear guidance on risk management. |  |
| **Data security / Biometrics** | ISO 24745 | Specific standards for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, ISO/IEC 24745:2011 provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information. |  |
| **Customer Due diligence** | FATF 40 | Foundation of CBTT, FIU regulations |  |
| **Customer Due diligence** | FATF recommendations on Digital Identity (2020) | Extension of FATF 40 for modern era |  |
| **Customer Due Diligence** | CBTT, FIU guidelines on AML/CFT | Defines regulations for T&T entities to conduct risk based due diligence |  |

Technologies Involved in Fintech Market

**Blockchain – provides more private, secure, and transparent means of tracking the complete lifecycle of financial transactions.**

**Cryptocurrency - is digital cash for the digital age. It’s similar to regular money — think $$ — but it’s digital-only, so there are no bills or coins to carry around.**

**Robot-Advisors -has disrupted the asset management sector by providing algorithm-driven recommendations and a customized portfolio management which does not necessarily demand human supervision.utilize algorithms to automate investment advice to lower its cost and increase accessibility.**

**Automated Assistants - can perform tasks, or services, on behalf of an individual based on a combination of user input, and location awareness. It has the ability to access information from a variety of online sources**

**AI - wide-ranging branch of computer science concerned with building smart machines capable of performing tasks that typically require human intelligence.**

**Machine Learning - the study of computer algorithms that improve automatically through experience.**

**Big Data - a combination of structured, semistructured and unstructured data collected by organizations that can be mined for information**

**Data Analytics - a process of inspecting, cleansing, transforming and modeling data with the goal of discovering useful information, informing conclusion and supporting decision-making**

**Cloud Computing - the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change.**

**Cyber Security - the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.**