Investor Guidelines – Comprehensive Risk Assessment Matrix – draft version 1.0
Annex 2 - Guidelines for Investing in Responsible Digital Financial Services

Objective: To provide a comprehensive summary of emerging risks in digital financial services, their sources and impacts and proposed actions or policies to mitigate such risks across constituents or stakeholders in DFS ecosystems. These initial risks were identified based on current projects and recent evidence.

Table 1. Risks arise from internal and external sources which impact the following constituents or stakeholders, for example:

<table>
<thead>
<tr>
<th>Risk Source</th>
<th>Impact on Consumers</th>
<th>Impact on Providers</th>
<th>Impact on Financial System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks result from: (1) internal risks from inadequate or failed internal processes, people, and systems; and (2) external risks or events.</td>
<td>Consumers should be able to understand the products and services they are offered, to use them as intended, and to get redress in case something does not work. Impact on consumers can include direct loss of money, the cost of getting redress (in terms of money and time), or the incremental cost of using a second-choice alternative, such as sending cash by bus from an urban to rural area.</td>
<td>Providers can be impacted through direct losses, regulatory fines, costs to remediate issues, and forgone current or future revenue when users cannot or choose not to use a product or service</td>
<td>Impact to the financial system at large can include macroeconomic effects when business is halted or harmed (e.g., if many businesses are unable to transact). It can also include consequences when the digital payment system is exploited to facilitate criminal activity (e.g., money laundering or moving funds to fund terrorist activities). We note that risk to the financial system at large is various and complex, and we offer this simplified schematic way to consider it.</td>
</tr>
</tbody>
</table>

Risk Definitions: The following summarizes key risks and are mapped across impacts on constituents or stakeholders:

1. Systemic: A risk that could cause collapse of, or significant damage to, the digital financial system or a risk which results in adverse public perception, possibly leading to lack of confidence and worst case scenario, a "run" on the system

2. Operational: A risk which damages the ability of any of the stakeholders to effectively operate their business or a risk which results in a direct or indirect loss from failed internal processes, people, systems or external events

3. Reputation: A risk that distorts and damages the image of any of the stakeholders, the digital financial system, the financial system, or of a specific product being offered to the consumer by the DFS provider

4. Legal: A risk which could result in legal cases which are not envisioned, judgment or contracts that could disrupt or affect DFS business practices

5. Liquidity: A risk that lessens the ability of a bank or DFS provider/agent to meet cash or transaction completion obligations upon demand

6. International: A systemic risk (as defined above) that could have cross-border effect in terms of non-compliance etc.

Actions and Mitigants: The above sources/definitions of internal and external risks further impact DFS investments, as shown in Table 2, and proposed are actions to mitigate them. Tables 3a-c follows with the same, analyzed across: (a) policies and procedures; (b) people; and (c) systems, along with proposed actions. Similarly, Table 4 provides a summary for sources of risks due to external events and proposed actions to mitigate them in line with Global Principles.

1 Investment/advisory projects in portfolio and pipeline. Key references include IFC-MCF Handbooks for (1) ADCs; (2) DFS Risks; (3) Data Analytics; IFC Consumer Risk Assessment/Due Diligence; WBG, CGAP policy and focus notes on DFS and consumer protection; RFF 2015-2017; Smart Campaign Client Protection Principles; SPTF; G20/GPFI policy/events.
## Table 2. Investment Risks and Mitigants

<table>
<thead>
<tr>
<th>Investment</th>
<th>Risk Descriptions/Definition</th>
<th>Risk Objective/Overview</th>
<th>Risk and Policy Options</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>
| Strategic risk | Strategy cannot be implemented due to  
1. Geo political situation in the service area  
2. Regulatory Guidelines  
3. Challenges with religious beliefs and social taboos  
4. Strategy does not cater to market needs which could be implemented but will not have business returns | The Strategy has to be aligned to the regulatory framework and guidelines for DFS in the country/area/region. It should also be designed in a way which does not conflict with the social norms and religious beliefs of the market. The strategy needs to also ensure that it caters to market needs which will be tapped by the DFS and has enough business potential for the DFS. | Strategy is devised after analysis and study of the following:  
1. Understanding of the political, security and stability of the government policies in the country/ geography  
2. Regulatory framework and guidelines in the country/ geography  
3. Evaluation of inconsistencies in the governing regulations in the country/geography  
4. The strategy should also be designed after ensuring that it does not conflict or create a concern for the customers because of the social norms or religious beliefs  
5. Strategy needs to be developed after obtaining empirical data through market research and analysis.  
6. DFS can hire independent consultants to validate or create a strategy according to the market and regulatory environment | x | x |     |     |     |     |
| Team Risk | Setting up incompetent/inexperienced/irrelevant management and project team to execute the strategy | The management and Project team  
1. Understands the regulatory environment  
2. Understands the geo political, social and religious sentiments of the country/ geography  
3. Has relevant experience and knowledge to implement the strategy | The team is hired after complete scrutiny of the experiences, references and capabilities. The team or at least some of the members devising the have knowledge of the local sentiments especially on the religious beliefs and social norms. | x | x |     |     |     |     |
## Investor Guidelines – Comprehensive Risk Assessment Matrix – draft version 1.0

### Annex 2 - Guidelines for Investing in Responsible Digital Financial Services

| Technology Selection Risk | Error in Technology Selection due to market feedback and existing deployments using a certain technology. | The selected technology evaluation fails to map the strategy requirements with the functional capability, scalability, and adaptability of the technology platform. The technology selection also needs to take into account that new technological evolution and developments are happening very frequently. The platform which needs to adapt to the technological developments and evolutions to support changing requirements. | The technology platform needs to be evaluated against the following parameters before the investment decision:  
1. **Adaptability**: The platform needs to be adaptable and configurable according to the evolving business requirements and technological evolution.  
2. **Scalability**: The platform needs to be scalable for which testing such as stress testing and evaluation of the maximum TPS (transaction per second) needs to be obtained as part of evaluations.  
3. **Capability**: The platform needs to have the capability to provide the functionality as required by the strategy.  
4. **Service and Support**: The technical platform needs to have strong service and support for technology operations and developments. |
| Delays in Decision Making | Delays in decision making can result in the change of environment making the well-designed strategy redundant | The decision making to be swift and validity of the strategy to be evaluated after regular intervals. | Strategy to be owned by an independent team which keeps evaluating the validity of the assumptions and decisions in the strategy based on changes in the assumptions. |
| Lack of funding for the business | The funding (investment) is not enough to implement the strategy approved for the DFS | Failure to evaluate the funding required for the implementation of the strategy. This carries the risk that since the strategy is devised in isolation the funding available could fall short of the investment required to implement the strategy. | Funding and strategy needs to be evaluated simultaneously to ensure that the strategy finalized can be implemented in the available funding. |
**Table 3a. Policies and Procedures – Risks and Mitigants**

<table>
<thead>
<tr>
<th>Policies &amp; Procedures</th>
<th>Risk Descriptions</th>
<th>Risk Objective</th>
<th>Risk Mitigants and Policy Options</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lax credit standards</td>
<td>DFS has relaxed policies to giving credit and to allocate too little resources to screening borrowers and too many resources to giving credit.</td>
<td>Periods of high credit volume due to lax credit standards are followed by increases in loan delinquencies due to inability of the borrowers to pay the credit</td>
<td>DFS needs to have increased customer screening for credit approvals. It is prudent to ensure that over lending to the same individuals are not done by analyzing the debt burden and payback capability. Capital requirements can achieve the optimal balances of screening and lending because they affect the fraction of each loan financed with outside funding. Since this funding is cheaper than bank’s own capital, the lower the capital requirements the lower the costs for the banks to fund their loans. And when these costs go down, so does the quality of the marginal borrower getting credit relative to the social optimum.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weak guarantees</td>
<td>Weak Guarantees are non-binding commitments against unsecured loans and financial support.</td>
<td>Weak Guarantees can result in financial losses, as the guarantees cannot be enforced in case of delinquencies/nonpayment of liabilities</td>
<td>The following steps needs to be taken to ensure the guarantees to the DFS are not weak 1. Legal Review of the guarantee 2. Underwriting services should be considered for large amounts. These services are provided by some large specialist financial institutions, such as banks, insurance or investment houses, whereby they guarantee payment in case of damage or financial loss and accept the financial risk for liability arising from such guarantee. An underwriting arrangement may be created in a number of situations including insurance, issue of securities in primary markets, and in bank lending, among others.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Investor Guidelines – Comprehensive Risk Assessment Matrix – draft version 1.0
Annex 2 - Guidelines for Investing in Responsible Digital Financial Services

| Little or no due diligence | Due diligence of the customers allows the DFS to assign a risk rating to the customers according to which the services to the customers is disseminated. | Lack of due diligence increases the chances for defaults, money laundering and illegal financial activities. | The due diligence should be in place to anticipate the risk levels for every customer
1. Credit Default Checks
2. Validation through international lists for unwanted individuals
3. Identity Verification and validation through National ID systems
4. Risk Rating policy and matrix to be implemented to define the risk of every individual | x | x | x | x |
| High default rates | High default rates could occur due to lax credit standards (customer over-indebtedness) and due to changing market situations | High default rates could occur due to lax credit standards which results in high default rates. High default rates can also be anticipated through regular market studies and default trends | 1. Stringent Credit Policy
2. Monitoring non-performing loans
3. Regular market scan to anticipate high default through market indicators | x | x | x | x |
| Solvency / Liquidity risks - | Solvency risks occurs when an institution cannot fully meet its debts as they come due, even by selling all its assets, Liquidity risk occurs when an institution does not have sufficient liquid assets (e.g., cash) to meet its debts | Liquidity Risks – Liquidity risk arises from the potential inability of any financial institution to generate additional liabilities to cope with the decline in its liabilities or increase in its assets. A financial institution would face liquidity issues if a substantial number of its customers suddenly decide to withdraw a large part of their deposits/investments from that institution or due to a sudden and sharp impairment in the value of its assets (increase in its non-performing assets).
Solvency – Inability to manage the liquidity risk can lead to solvency. While liquidity issues are more common, and in some cases cyclical in nature, solvency issues are, most often, deep-rooted and if left unattended could | 1. To meet the sudden outflow of funds and the consequent likely adverse impact on liquidity, financial institutions are mandated by the banking regulator in that country to maintain sufficient liquid assets. Almost all Central Banks mandate a reserve ratio i.e. the amount of cash to be maintained either as cash in the vault of the bank and/or as balances in its current account with the Central Bank and/or as investments in liquid instruments such as government securities. These reserve requirements reflect the amount of liquid assets to be maintained by the bank as a percentage of customer deposits in the bank’s books.
2. Solvency is managed using a well-defined method called Capital Adequacy Ratio (CAR) also known as Capital to Risk Assets Ratio (CRAR). It measures a bank's | x | x | x | x |
result in the eventual liquidation of the firm altogether. Liquidity issues that remain unresolved for an extended period could inevitably translate into solvency issues for that financial institution.

capital as a percentage of its ‘risk weighted assets’. If a financial institution maintains adequate capital (i.e. equity, retained earnings, etc.), it will lessen the chance of bankruptcy / insolvency even when its assets are stressed i.e. increase in non-performing assets that may have to be written off.

| KYC/ AML | Potential and existing customers cannot access DFS due to inability to prove his/her identity. | Know Your Customer (KYC)/Customer Due Diligence (CDD) guidelines to be set commensurate with the risk of the service. Subject to regulatory approval and verification of implementation. | 1. National ID systems  
2. Financial ID systems  
3. Regulated KYC requirements left for implementation by the DFS providers  
4. Ensure that appropriate risk based service access requirements are established at account opening |
|--------------------------|------------------------------------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Prevention of customers' over-indebtedness is crucial for both customers and business sustainability; therefore, investing considerably in the customer selection process | Over-indebtedness occurs when the pool of customers in the market is limited and are being tapped by multiple institutions for lending and in absence of proper lending policy and credit standards. | Customer selection needs to be governed by stringent lending policies and standards. | The following needs to be ensure prevention of over-indebtedness of customers  
1. Avoid Lax Credit Standards  
2. Debt Burden needs to be strictly adhered to in order to manage over-indebtedness |
| Ensure customers are not easily "black listed" | Blacklisting customers due to fraudulent or unethical practices is a normal practice in the financial services space to manage risks of frauds, money laundering and other malpractices | Blacklisting on the slightest suspicion of fraud and unethical practices to avoid losses can result in a lot of blacklisted customers. | The following steps can  
1. Fair and transparent Blacklisting policy.  
2. Blacklisting must be backed by evidence and proof of fraudulent activity. |

| x | x | x |
## Annex 2 - Guidelines for Investing in Responsible Digital Financial Services

| Protection of customer data and privacy | Customer data and privacy is sensitive and needs to be secured through policies and their implementation, i.e. through customer consent | Customer data and privacy can be compromised in the following  
   1. Unencrypted data.  
   2. Unrestricted access to data and systems of unauthorized users.  
   3. Data retention, transmission and communication is not managed through adequate data privacy and security policies. | The following policies should be in place for ensuring the protection of customer data and privacy  
   1. Data Encryption Policy  
   2. Data retention, transmission and communication security policy  
   3. Data and system Access authorization policy | x | x | x |

| Fair and transparent pricing | Pricing of services needs to be transparent and clearly communicated to the customers in advance. Fair Pricing means to avoid over-pricing the customers and disclosing costs for informed decisions | Pricing needs to be clearly communicated to the customers through all the touchpoints  
   1. Website  
   2. DFS Branches and Agents  
   3. Digital Channels  
   It needs be ensured that the customers of the services can easily view and understand the pricing.  
   The pricing needs to be just and according to the pricing policy or regulatory guidelines. | The following steps help in achieving the fair and transparent pricing.  
   1. No hidden charges  
   2. There is no set rule for fair pricing however the DFS can devise a pricing policy on its own or based on industry good practices in absence of regulatory guidelines.  
   3. Regulatory interventions are available in some markets to ensure fair pricing | x | x | x |
## Annex 2 - Guidelines for Investing in Responsible Digital Financial Services

### Table 3b. People – Risks and Mitigants

<table>
<thead>
<tr>
<th>People (HR/Training)</th>
<th>Risk Descriptions</th>
<th>Risk Objective</th>
<th>Risk Mitigants and Policy Options</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>
| Human errors                          | Human errors are mistakes made by the individuals due to the manual nature of the processes /activities in place | In absence of automated processes and 4 eye principle human errors are possible. This could result in operational challenges and customer dissatisfaction. | 1. Automation - automation of processes can avoid human errors  
2. 4 eye principle – The manual process should be broken in the way where the initiator of the activity and completion of the activity are two individuals. This enables a dual check on every manual activity. | x |   |   |   |   |   |
| Money sent to the wrong account because of user error | Users of the DFS can send the funds to the wrong account in absence of validation of the account ownership. | The money sending functionality needs to be supported through an identity fetch (inquiry transaction) before the funds are transferred. In case the customer even after the inquiry fails to rectify the mistake and transfer funds it needs to be backed up by customer facilitation policy and documented reversal process. | The following needs to be implemented to manage the user error for money transfers.  
1. Title fetch  
2. Reversal processes  
3. Customer facilitation policy | x |   |   |   |   | x |
| Agents may perform small acts of abuse without detection, such as inflating a surcharge and pocketing the excess; agents may also become targets of theft, as they accumulate and must deliver a day’s or weeks’ worth of cash deposits made by customers to banks each day | Agents are entities, retailers and mom & pop shops providing financial services on behalf of the DFS under an agreement.  
Agents can abuse their position as the intermediary between the DFS and its customers and also can be susceptible to security risks on ground. | The agents can be the ones abusing customers as they are the ones interacting with the customers as the front end of the DFS educate the customers for the services and its pricing.  
Agent exploiting the customer by over-charging is a common complaint.  
The agent can also be susceptible to risk of theft or burglary as the liquidity management at the agents can result in security risk for the agent. | The following needs to be ensured in order to manage and monitor the agent for his activities.  
1. Scheduled Field visits  
2. Surprise visits  
3. Mystery Shopping  
Agent having large business volume also needs to be provided security in form of cash management solutions on their door step. Alternatively providing them insurance for average cash balances can also give them confidence to increase business volumes. | x | x |   |   |   | x |
| Fraud | Frauds mean the unauthorized activity to deprive the customer of his finances. It is the use of potentially illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution | Fraud Management Policies should be in place with the element of mitigation in all the operational processes of the DFS. Fraud can never be eliminated however; it could be minimized through proper controls and policies. Fraud Investigations for any fraud are key to finding the root cause and act to ensure that the same does not occur again. | The following needs to be ensured by the DFS  
1. Fraud Policies  
2. Fraud investigation unit to be in place  
3. Fraud Reporting |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>x x x</td>
</tr>
</tbody>
</table>
### Table 3c. Systems – Risks and Mitigants

<table>
<thead>
<tr>
<th>Systems</th>
<th>Risk Descriptions</th>
<th>Risk Objective</th>
<th>Risk Mitigants and Policy Options</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>
| New/ untested technology      | Technology selections should be an extensive exercise. New/untested technology increases the risk of technology vulnerabilities.                                                                                       | The technology platforms mature overtime after they are deployed in the market based on experiences, feedback and vulnerability identification through ethical and unethical interventions.                             | It is prudent to not select new/untested technology unless  
1. There is no tested options which can perform the same function.  
2. The application has been extensively tested / studied to ensure that it will be the right choice for the business.  
However, DFS can never be certain of the performance of the new / tested | x | x | | | | |
| Cyber-attacks/ Hacking        | The DFS services being digital in nature are susceptible to cyber-attacks and hacking.                                                                                                                             | A cyberattack is any type of offensive maneuver employed by hackers that targets technology infrastructures by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. | The technological infrastructure should be validated through white hat hackers/ethical hackers to perform the following  
1. Vulnerabilities Testing  
2. Penetration Testing  
3. Web Application Testing  
4. Monitoring and Responding to Cyber Security Events | x | x | x | | | |
**Data security**
Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to systems, applications, databases and websites. Data security also protects data from corruption.

The fundamental data security requirements and elements which needs to be ensured for data security:
1. **Confidentiality**
   a. Privacy of Communication
   b. Secure Storage of Sensitive information
   c. Authenticated Users
   d. Granular Access Controls
2. **Integrity**
3. **Availability**

The following Data Security dimensions are recommended to be implemented as a policy.

- **Physical** - Systems must be physically inaccessible to unauthorized users. This means that you must keep them in a secure physical environment.

- **Personnel** - The people responsible for system administration and data security at your site must be reliable. You may need to perform background checks on DBAs before making hiring decisions.

- **Procedural** - The procedures used in the operation of your system must assure reliable data. It is recommended to separate out users' functional roles in data management.

- **Technical** - Storage, access, manipulation, and transmission of data must be safeguarded by technology that enforces your particular information control policies.

**The following policies should be in place for ensuring the data security**
1. Data Encryption Policy
2. Data retention, transmission and communication security policy
3. Data and system Access authorization policy
4. Backup and Business Continuity Policies
5. Data Center access policy
In this digital data-driven world, system downtime poses a significant threat towards an organization’s business operations. Business continuity and disaster recovery plans should be in place, regardless of the size of the DFS provider. These are there as a last resort, but not having a plan to handle downtime could create a bigger headache than the downtime itself.

Whilst it is widely accepted that downtime in some form will sometimes happen, it is important that efforts are made to reduce it. No matter how good your disaster recovery plans may be, most DFS providers would rather never have to use them.

When critical systems go down, the risk of losing data is significantly increased – documents, data, communications and information can all disappear. DFS can be left unable to return to normal capacity, with key information missing.

Downtime can be caused by issues as simple as overloaded servers, so making sure they are properly provisioned and maintained needs to be high up on the agenda.

The system availability cannot be guaranteed but the unavailability can be minimized with the following steps:

1. SLA’s with vendors and partners
2. Use Active – Active Clustering for all core technology systems
3. Deploy load balancing and scalable infrastructure
4. Deploy simple structures and avoid multiple processing
**Design** — security may not be part of the initial functional design, creating significant security flaws that enable fraud.

A design is a blueprint of an application; it lays a foundation for its development. It illustrates the layout of the application and identifies different application components needed for it. It is a structure that determines execution flow of the application.

The design of the technical platform/infrastructure needs to be evaluated for technical stability and significant security flaws that enable fraud.

The developers and technical implementation rush the design phase which leaves flaws which can be exploited by fraudsters.

Design level flaws are lesser known concepts but their presence is a very big risk to the applications. Such flaws are hard to find in static or dynamic application scans and instead require deep understanding of application architecture and layout to uncover them manually. With increasing business needs the complexities in application design and architecture are also increasing. There is a rise in the use of custom design techniques and diverse technologies in the applications today, which makes the need for design reviews imperative.

Design review should be an integral part of secure software development process. If the application is reviewed for security at the design level many inherent backdoors can be uncovered. Design reviews also help to implementing the security requirements in a better way.

The design is thoroughly studied mainly with respect to the data flow, different application components and their interactions, data handling etc. This is achieved through manual analysis and discussions with the design or technical architect’s team.

The design and the architecture of the application must be understood thoroughly to analyze vulnerable areas that can lead to security breaches in the application.

The key areas of the design that must be considered during threat analysis are given below.

1. Data Flow/Code Layout
2. Access control
3. Existing/Built-in Security controls
4. Entry points of non-user inputs
5. Integrations with external services

| Design | A design is a blueprint of an application; it lays a foundation for its development. It illustrates the layout of the application and identifies different application components needed for it. It is a structure that determines execution flow of the application. The design of the technical platform/infrastructure needs to be evaluated for technical stability and significant security flaws that enable fraud. | The developers and technical implementation rush the design phase which leaves flaws which can be exploited by fraudsters. Design level flaws are lesser known concepts but their presence is a very big risk to the applications. Such flaws are hard to find in static or dynamic application scans and instead require deep understanding of application architecture and layout to uncover them manually. With increasing business needs the complexities in application design and architecture are also increasing. There is a rise in the use of custom design techniques and diverse technologies in the applications today, which makes the need for design reviews imperative. Design review should be an integral part of secure software development process. If the application is reviewed for security at the design level many inherent backdoors can be uncovered. Design reviews also help to implementing the security requirements in a better way. The design is thoroughly studied mainly with respect to the data flow, different application components and their interactions, data handling etc. This is achieved through manual analysis and discussions with the design or technical architect’s team. The design and the architecture of the application must be understood thoroughly to analyze vulnerable areas that can lead to security breaches in the application. The key areas of the design that must be considered during threat analysis are given below. | x | x | x | x |
**Investor Guidelines – Comprehensive Risk Assessment Matrix – draft version 1.0**

**Annex 2 - Guidelines for Investing in Responsible Digital Financial Services**

<table>
<thead>
<tr>
<th>Source code — malicious code and/or flaws in the code (e.g. Cryptography) may assist future attacks on the application</th>
<th>Source Code flaws can create risks / vulnerability for the technology platform which make it susceptible to attacks</th>
<th>The following Source Code vulnerability needs to be assessed at the time of technology selection</th>
</tr>
</thead>
</table>
| **1. Information Leakage:** The DFS should ensure that sensitive or confidential information such as cryptographic keys, account details, passwords, system configurations and database connection strings are protected. Hence, the DFS should scrutinize potential sources of information leakages like verbose error messages and banners, hard-coded data, files and directories operations for accidental information disclosure. | **2. Resiliency Against Input Manipulation:** One common security weakness in applications is the failure to properly validate inputs, from a user or system interface. Malformed inputs can spawn major vulnerabilities such as script injection and buffer overflows as well as cause erratic system behavior. The DFS should ensure that data validation includes the following steps: | **Source Code Review needs to be conducted for the following vulnerabilities:**

1. Information Leakage
2. Resiliency Against Input Manipulation
3. Unsafe programming practices
4. Deviation from design specifications
5. Cryptographic Functions
6. Exception Handling
7. Business Logic
8. Authorization
9. Logic |

6. Location of configurations file and data sources
7. Add-ons and customization present (in case of built-in design framework)

This will help in identifying the trust boundaries for an application and thus aid in taking decisions about the vulnerabilities and their risk levels posed to the application.
### Annex 2 - Guidelines for Investing in Responsible Digital Financial Services

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>i.</td>
<td>all inputs to an application should be validated;</td>
</tr>
<tr>
<td>ii.</td>
<td>all forms of data (such as text boxes, select boxes and hidden fields) should be checked;</td>
</tr>
<tr>
<td>iii.</td>
<td>the handling of null and incorrect data input should be verified;</td>
</tr>
<tr>
<td>iv.</td>
<td>content formatting should be checked; and</td>
</tr>
<tr>
<td>v.</td>
<td>maximum length for each input field should be validated.</td>
</tr>
</tbody>
</table>

All input validation routines should be reviewed and tested to assess their effectiveness against known vulnerabilities.

#### 3. Unsafe Programming Practices

The DFS should ensure that the source code review enables it to identify unsafe programming practices such as the use of vulnerable function calls, poor memory management, unchecked argument passing, inadequate logging and comments, use of relative paths, logging of passwords and authentication credentials, as well as assignment of inappropriate access privilege.

#### 4. Deviation From Design Specifications

Implementation oversight is one of the common causes of system vulnerabilities. The DFS should review critical modules such as those containing authentication and session management functions for any deviation from its design specifications. Testing of authentication functions should cover
the verification of security requirements (such as credential expiry, revocation and reuse) and the protection of cryptographic keys. The DFS should test session management to ensure that:

i. sensitive or confidential information that is stored in cookies is encrypted;

ii. the session identifier is random and unique; and

iii. the session expires after a pre-defined length of time.

5. **Cryptographic Functions** The strength of cryptography depends not only on the algorithm and key size, but also on its implementation. The DFS should evaluate cryptographic implementation and ensure that only cryptographic modules based on authoritative standards and reputable protocols are installed. The DFS should review cryptographic algorithms and crypto-key configurations for deficiencies and loopholes. The choice of ciphers, key sizes, key exchange control protocols, hashing functions and random number generators should be thoroughly assessed. Rigorous testing should be conducted on all cryptographic operations (encryption, decryption, hashing, signing) and key management procedures (generation, distribution, installation, renewal, revocation and expiry).

6. **Exception Handling** When exception or abnormal conditions occur, the DFS
should ensure that adequate controls are in place so that resulting errors do not allow users to bypass security checks or obtain core dumps. The DFS should also ensure that sufficient processing details are logged at the source of the exception to assist problem diagnosis. Robust exception/error handling that facilitates fail-safe processing under various exception conditions should be implemented. Leakage of sensitive or confidential information due to improper error handling should be prevented.

### 7. Business Logic:

The DFS should test its business logic to ensure that a user cannot perform an unauthorized function or transaction. It is imperative that negative testing be included in the testing to determine the response of a system when an unexpected input is received.

### 8. Authorization:

After a user has been authenticated and gains access into the system, authorization helps to ensure that the user is only allowed to view, write, execute, modify, create and/or delete data and invoke the functions that he is permitted to do so. DFS should perform tests to confirm that the actual access rights granted to a user in the system conform to the approved security access matrix.

### 9. Logging:

Logging is implemented to facilitate follow-up investigation and troubleshooting when a system
An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application. Once an attacker has found a flaw, or application vulnerability, and determined how to access it, the attacker has the potential to exploit the application vulnerability to facilitate a cybercrime. These crimes target the confidentiality, integrity, or

<table>
<thead>
<tr>
<th>Application vulnerabilities — common vulnerabilities (e.g., developer ‘back doors’) may be overlooked in the haste to get to market</th>
<th>incident occurs. The DFS should build the following requirements and specifications into the tests:</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. sensitive or confidential information such as passwords, authentication credentials, cryptographic keys, confidential business data should not be recorded in system logs;</td>
<td></td>
</tr>
<tr>
<td>ii. the maximum data length for logging is pre-determined;</td>
<td></td>
</tr>
<tr>
<td>iii. successful and unsuccessful authentication attempts are logged; and</td>
<td></td>
</tr>
<tr>
<td>iv. successful and unsuccessful authorization events are logged.</td>
<td></td>
</tr>
</tbody>
</table>

The application vulnerabilities are usually ‘Just Enough’ Coding which means that in order to meet deadlines and rush to finish a project or program, application developers may code just enough to make it functional without allocating enough time to evaluate and mitigate potential security problems. Lack of security elements like type checking, improper error handling, vulnerability to SQL injections, and inefficient memory overflow handling are just some examples of insufficient coding that provides hackers with just enough information to sneak in and steal reams of data.

The technological infrastructure should be validated through white hat hackers/ethical hackers to perform the following:

1. Vulnerabilities testing
2. Penetration Testing (white box/gray box and black box)
## Application integration

— other systems that the application interacts with in the ecosystem may be insecure

<table>
<thead>
<tr>
<th>Availability (known as the “CIA triad”) of resources possessed by an application, its creators, and its users. Attackers typically rely on specific tools or methods to perform application vulnerability discovery and compromise.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application integration (sometimes called enterprise application integration or EAI) is the process of bringing data or a function from one application program together with that of another application program. Where these programs already exist, the process is sometimes realized by using middleware, either packaged by a vendor or written on a custom basis. An common challenge for an enterprise is to integrate an existing (or legacy) program with a new program or with a Web service.</td>
</tr>
</tbody>
</table>

### 1. Number of integration points

Projects that attempt to integrate everything at once, sometimes called “the big bang approach,” are prone to adverse results due to the extreme complexity and large number of interdependencies.

### 2. Changing Requirements

When the use case has been poorly thought through, requirements can change frequently and create chaos in an application integration project. Make sure you spend enough time in the requirements gathering and process planning phases to gather the best possible set of requirements for your project.

### 3. Inadequate integration infrastructure

Avoid solutions that rely on manual programming or overly complex, heavy middleware software sets. Focus on single stack, single studio solutions with an integration platform for enterprise class integration projects.

### 4. Impossible Schedules

Set realistic expectations by establishing an accurate estimate of the integration efforts required for your project. If necessary, bring in...
<table>
<thead>
<tr>
<th>Program of another company.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The application integration can cause delays in the implementation if not managed properly. It also creates risks for the</td>
</tr>
</tbody>
</table>

6. **Inadequate Change Management Procedures.** Some organizations lack the formal methodology to handle change orders. In addition, changes to the application and other systems being integrated may not be locked down during the integration project. The result can be chaotic from a requirements, implementation and testing perspective.

7. **Lack of Staff and Management Experience.** APPLICATION integration may be new territory for your IT staff and management.

8. **New Business Processes**
   - Introducing change to an organization always carries with it the risk of institutional or market resistance.

9. **New integration infrastructure**
   - New or unproven integration infrastructure represents a risk factor.

10. **Inadequate testing plans.** Test plans should introduce testing early and often. Test scripts and automated testing may be able to help ensure accelerated and more complete discovery of problems early in the APPLICATION integration project.

11. **Inadequate testing plans.** Test plans should introduce testing early and often. Test scripts and automated testing may be able to help ensure accelerated and more complete discovery of problems early in the APPLICATION integration project.

12. **Inadequate testing plans.** Test plans should introduce testing early and often. Test scripts and automated testing may be able to help ensure accelerated and more complete discovery of problems early in the APPLICATION integration project.

5. **Staff Turnover:** Try to avoid turnover by gaining commitments from participants that they are available for the expected duration of the project.

6. **Inadequate Change Management Procedures.** The change management procedures needs to be properly in place and professionally managed.

7. **Lack of Staff and Management Experience**
   - Try supplementing your experience with proven consultants or consulting firms that can leverage experience across a wide array of APPLICATION integration projects.

8. **New Business Processes**
   - Make sure the processes have been vetted by stakeholders and customers and that they are introduced properly so as to gain maximum adoption and adherence.

9. **New integration infrastructure**
   - Make certain vendor experts are available to back up your team not only with technical bugs but with implementation
### Perimeter security devices — are normally inadequate and should not be relied on

<table>
<thead>
<tr>
<th>The perimeter security devices are required to provide security and protection to the technological infrastructure, databases, network, applications and web interfaces</th>
<th>The perimeter security devices implemented to provide security to the technological infrastructure have the following limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Signature based</strong>—A database of signatures and known bad elements can't keep pace with the sheer volume of new malware strains created daily. Even if perimeter defenses with rules and signatures are proactively managed and updated regularly, they are necessary, but are far too static for today's threats.</td>
<td></td>
</tr>
<tr>
<td>2. <strong>Lack scalability</strong>—Managing users/identities, all systems, all applications, and all data all at once, with products that have serious scalability limitations narrows the security analysis into a sub-set of event and log data.</td>
<td></td>
</tr>
<tr>
<td>3. <strong>Can’t support highly distributed environments</strong>—Today’s organizations consist of highly distributed environments. Most current solutions deploy appliances or collection agents to these locales. But this just</td>
<td></td>
</tr>
</tbody>
</table>

In order to perimeter security devices to be able to support the technology security it is important that the controls are implemented during the implementation in the following areas

1. **Design Phase**
2. **Application Development**
3. **Application Integrations**
4. **Integration through APIs**
5. **Network Security**

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
compounds analysis latency with limited data parsing and filtering at the collection point and requires inbound data to come to rest in a database before further processing.

4. **Forensic vs. Preemptive**—Current solutions are passive and lean heavily toward forensic analysis after attacks have long since occurred. We need the ability to be more preemptive and have the ability to react. The key to breaking the cycle lies in identifying an attack while it’s happening or even before it begins—when cybercriminals are profiling an organization.

5. **Focused on compliance**—Demonstrating compliance is a static event, and compliance regulations are reactive to technology. While demonstrating compliance is important, it’s not the same as being secure.

6. **Intrusion-centric**—In many respects, information security has mimicked physical security practices in deploying an intrusion-centric approach to threat protection. Cyberattackers take advantage of this lop-sided security model to provide command and control channels for on premise bots to access confidential data and intellectual property.

7. **Difficult to deploy and manage**—To provide the needed protection against sophisticated attacks, it is essential to collect more data from more devices.
Investor Guidelines – Comprehensive Risk Assessment Matrix – draft version 1.0
Annex 2 - Guidelines for Investing in Responsible Digital Financial Services

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Risks and Challenges</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| **Application Programming Interfaces (APIs)** | Open up digital assets to a broader ecosystem of partner and customers, but they also increase digital risk through, identity, parameter and man in the middle attacks | Weak points in an API construct can expose customer data, backend server appliances, and even monetary systems to unauthorized access, putting the API (and more often than not, the business) at risk. | The API security can be weak because of the following reasons  
1. **Developer Responsibility**: The API security needs to be developed by the API developer, however the security of the API needs to be ensured by the API provider according to the utilization of the API  
2. **Insufficient Coding**:  
   In order to meet deadlines and rush to finish a project or program, API developers may code just enough to make it functional without allocating enough time to evaluate and mitigate potential security problems. Lack of type checking, improper error handling, vulnerability to SQL injections, and inefficient memory overflow handling are just some examples of insufficient coding that provides hackers with just enough information to sneak in and steal reams of data. |
| **Partnerships / ecosystems e.g. system down time/ unavailability** | Technical integration with partners and external ecosystems to facilitate services and payments is an important element of | When critical systems go down, the risk of losing data is significantly increased – documents, data, communications and information can all disappear. DFS can be | The system availability of external ecosystems cannot be guaranteed but the unavailability can be minimized with the following steps:  
1. SLA’s with vendors and partners |
| Network Security | Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other | Types of attacks on the network level include  
- Passive  
  - Network  
  - Wiretapping  
  - Port scanner  
  - Idle scan  
  - Encryption  
  - Traffic Analysis  
- Active:  
  - Virus  
  - Eavesdropping  
  - Data Modification  
  - Denial-of-service attack  
  - DNS spoofing  
  - Man in the middle  
  - ARP poisoning  
  - VLAN hopping  
  - Smurf attack  
  - Buffer overflow  
  - Heap overflow | Network security starts with authentication, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a fingerprint or retinal scan). Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>x x x</td>
</tr>
</tbody>
</table>
| authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a | • Format string attack  
• SQL injection  
• Phishing  
potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wire shark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account. Communication between two hosts using a network may be encrypted to maintain privacy. Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual |
| corresponding password. | network being protected by the honeypot. A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots. |
### Table 4. External Events – Risks and Mitigants

<table>
<thead>
<tr>
<th>External Events</th>
<th>Risk Descriptions</th>
<th>Risk Objective</th>
<th>Risk Mitigants and Policy Options</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>
| Settlement      | Settlement risk is the risk that a counterparty (or intermediary agent) fails to deliver a security or its value in cash as per agreement when the security was traded after the other counterparty or counterparties have already delivered security or cash value as per the trade agreement. The term covers factors incidental to the settlement process which may suspend or prevent a trade from completing, even though the parties themselves are in agreement, are acting in good faith, and otherwise competent to perform. | Settlement risk poses financial threat to the DFS incase the entity expected to settle the funds is not able to settle funds. It is not necessary the inability to settle is the fault of the entity rather it could be due to external uncontrollable factor such as policy changes at the country level. | 1. Real time Settlement – Instant settlement of all stakeholders.  
2. Settlement through clearing houses or entities which have securities from both entities.  
3. Settling foreign exchange via a special-purpose entity, such as the CLS Group. | x |   |   |   |   |   |
| Increasing competition | **Competitive risk** is the chance that competitive forces will prevent you from achieving a goal. It is often associated with the risk of declining business revenue or margins due to the actions of a competitor. | There is not much a DFS can do to the competition but can work to stay ahead of the competition to avoid the risk. The risk has the potential for reduced revenue or declining margins due to the price, product, promotion or distribution actions of a competitor. | The following steps can be put in place to manage the | x |   |   |   |   |   |
|                    |                   |                | 1. Setup a team which performs market analysis and identifies competitive risk  
2. Invest in research and development to keep innovating new ideas to ensure to stay ahead of the competitors  
3. Create unique positioning in the market to avoid competition | | | | | |
### Annex 2 - Guidelines for Investing in Responsible Digital Financial Services

<table>
<thead>
<tr>
<th>Failing to have DR/BCP</th>
<th>Disasters cannot be predicted but can happen at any time. Regardless of all the controls that are put in place the business continuity can only be ensured if proper disaster recovery is planned, tested</th>
<th>Business continuity and disaster recovery plans should be in place, regardless of the size of the DFS provider. These are there as a last resort, but not having a plan to handle downtime could create a bigger headache than the downtime itself.</th>
<th>The DFS should ensure to have the following in place</th>
</tr>
</thead>
</table>
|                       | While it is widely accepted that downtime in some form will sometimes happen, it is important that efforts are made to reduce it. No matter how good your disaster recovery plans may be, most DFS providers would rather never have to use them but will have no choice in case of disasters where business Impact is analyzed to be larger than acceptable. | 4. Focus heavily on customer experience to retain existing customers  
5. Seven elements needs to be focused to avoid competition risk as these elements are also the points that increase risk.  
a. Pricing  
b. Innovation  
c. Location  
d. Resources  
e. Promotion  
f. Distribution  
g. Intellectual Property |
|                       |                                                                                                |                                                                                                  | x x x x |

<table>
<thead>
<tr>
<th>Business Impact Analysis</th>
<th>Disaster Recovery Policy</th>
<th>Business Continuity Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>