Cerise+SPTF Annual Meeting 2022
Session Notes

Name of session	**DFS Standards Working Group Meeting**
Date	28 September 2022
Time	9:00 am – 5:00 pm
Facilitator	**Amelia Greenberg**, Deputy Director, SPTF
Guest Speakers	**Eric Duflos**, Deputy Director, CGAP **Gerhard Coetzee**, Capacity Development Associate, CGAP

Overview

We spent the entire morning and part of the afternoon breaking into small working groups to review the draft version of the DFS Standards as of 27-Sep-2022, included as an annex in this document. Each small group reviewed a specific section of the DFS Standards and discussed questions and ideas for further revisions. Each group also took notes on its discussion and submitted those notes to Cerise+SPTF, which we share below. In addition to the small group work on the draft DFS standards, we also as one large group discussed how to launch the DFS Standards, and heard from two guest speakers. Notes from those discussions are below as well, but presented after the notes from the small working groups.

Notes from the Small Groups Discussions on Revising the Draft DFS Standards

Agent management small-group discussion:

- Overall – seems like there will be a lot of pushback from partners/agents.
- In any agreement with a partner/agent must include a clause that says they have read and agreed to all applicable data privacy laws. This is missing and \very important because in the event of a data breach it is the FSP that will be held responsible even if done through a partner/agent.
- Indicator 3.B.3.7 in the Universal Standards says, “If the provider uses agents, it monitors agent liquidity and whether agents respect client protection practices, and has mechanisms to address problems as needed. Add to this: monitors liquidity and agent behavior, not just liquidity.
- Detail 4.B.1.4.1 in the Universal Standard says, “The provider publishes basic product information, including pricing, at branch or agent locations, or digitally as applicable.” Add to this: the provider also publishes basic information on the digital partner’s products, etc. and that the digital partner publishes the FSPs basic information in return.
- Question: How often can one put out the information, as digital services can change rapidly?

Complaints mechanism small-group discussion:

- Amend 4.E.2.3.3 of the Universal Standards ("The provider resolves at least 90% of complaints within one month. If the resolution takes longer than one month, the provider notifies the client of the reason for the delay"). The period before reporting back to a client/customer if a complaint is not resolved should be reduced from 1 month. We made no specific time but think it depends on the type of complaint.
- Indicator 4.E.3.3 of the Universal Standards ("If the provider partners with third parties, the provider helps its clients to resolve complaints they have with those third parties.") needs to mention the appropriate frequency for complaints resolution, based on the availability of data.
- The draft DFS Standards do not seem to be customer centric, and instead are more institution/provider centric. There is no mention of timing to resolve complaints, nor on when the institution will come back if the delay is taking more time than expected. They do not focus on clear communication on how to complain and what to expect, define the time. This is spelled out in the Universal Standards but not here.
- The reporting should be more frequent based on the availably of data. It could be daily for certain types of complaints, weekly for others, but monthly is too long.
- Many of these are about analyzing and not acting. Have standards for governance around unresolved complaints. Accountability must be built on actions and standards should highlight actionability.
- After analyzing need to define what actions will be taken/escalated to senior management/board
- Should add train agents on how to engage with and assist the partners to resolve the complaints and raise issues with their senior management/board as needed
- Perhaps where the partner is unresponsive something about taking our complaints to the national regulatory body to help address, this would be for serious issues and based on our institutions having strong working relationships with the regulators so that they see the importance of addressing these types of complaints
- Question: should a digital product have a more frequent reporting system than for non-digital products. We suggest yes.

Cybersecurity small-group discussion:

- The board should define a list of approved venders that can do cybersecurity projects so that the IT Department doesn't choose by itself. The board checks into the companies to make sure they are reputable.
- The head of the Administration sends the CEO a weekly report on how many hacks/attempted hacks there have been and any data that was lost or compromised.
- IT governance will also be important. However, the board doesn't act to fix the problem. The appropriate department needs to act to fix the problem.
- The board's risk committee should report to the full board and should receive monthly updates from the IT department.

- All staff members need IT training and should be informed about the principles of responsible DFS.
- Identify the financial harm that can be caused by cybersecurity breaches and prepare some scenarios to address this risk.
- Maybe there should be an assessment of insurance options for the FSPs in the country to manage the cybersecurity risks. It's possible to buy insurance to cover the cost of ransomware/restoring lost data/recovering from a hack etc. In Egypt at least there is this kind of insurance, but it is very expensive.
- The FSP should appoint a head of cybersecurity as a staff position.
- Add an audit process for the third-party partners so the FSP has the right to audit its third-party providers for security risks. You can't just assume the partners are doing all they should be. We have had cases where that has not turned out well.
- Build a database of all the problems and solutions related to cybersecurity issues in 3 different markets – capital markets, finance, and insurance. There could be a role for the network to facilitate information sharing about the types of hacks that have been tried lately in a market and the solutions that can be used against them.

Data rights and privacy small-group discussion:

- Confidentiality is not enough. Systems need to be better because of risks of hacking.
- It is good to make customers aware of benefits of sharing their data because customers take a risk by sharing their data.
- It is good to have consent of consumer as conscious opt-in.
- Indicator 4.D.2.1 in the Universal Standards says this, "The provider explains to clients how it will use client data, with whom it will share the data, and how third parties will use the data. The provider receives clients' consent before using or sharing their data." The group discussed its support for this indicator. It is important to specify when the data is used by third parties, and how.
- Regarding "Opt-in," what does is really mean? Is it feasible? Clarify in the wording what is meant by "opt-in." We might define "opt-in" as deciding to share, but it is not really an option because the customer does not have the choice. If they do not share their data, they will not get the loan.
- Agreement to share information for access to financial services is not the same as sharing data for marketing purposes.
- The suggested DFS Standards talk about defining the minimum data needed by the FSP and collecting only that. But who would be able to do PPI for example? Would collecting those data be prohibited under this standard, because the FSP does not use those data to make a decision about approving or rejecting an application for a product or service. Tricky to define "minimum". It should be justified somehow why you collect specific information. Also, the minimum amount of data may change over time.
- Need to specify the need to properly dispose of discarded data when there is a change in the minimum set.

- All countries have data rights and privacy rights law. Law specifies how you use the information, transfer of data, security… The DFS is maybe too "soft". Need to add something specific about protection from hackers.
- When an FSP transforms digitally, it is an expensive process. Need to do it right.
- Nicaragua recently added in the law the need to explain reasons for denial to customers. This helps customers realize when there is something wrong with their data, and also what actions they can do to improve their chances of having their applications to use a financial product be accepted.
- Similarly, when an FSP denies an application because of algorithm scoring, it is important to inform customer so they can know when it is an issue with their data and the FSP can know if there is an issue with the algorithm.
- Does this concept of explaining why an application was denied belong in the Data Rights section? It is more due to respectful treatment of clients.
- Question: if they deny the application, what will the FSPs do with the data? What is the process for the data of denied customers.
- Rephrase: Inform the customer specifically which specific information is the cause for denial.
- ADD this idea: When working with third parties, specify the requirement to safeguard client data by 1) third parties are not allowed to use the data for other purposes; 2) when changing third party making sure that client data is safeguarded (need to erase the data, making sure that there is no data that remains at the old third party).
- ADD: How long can you use the data of people that are not your client anymore.

Fair and respectful treatment of customers small-group discussion:

- Have an easy to reach call center. Use IVR and/or chatbots in a limited way. Make it very easy for customers to use the call center to ensure efficient access.
- In the standards, use positive wording instead of phrases like "top risks they incur" or "bad behaviors," both of which are in the current draft of the DFS Standards. Translate these concepts instead into positive words. For example, use "customers' rights."
- Define customers' right and inform customers. Inform all complaint channels.
- Digital tools should have clear messaging that helps customers to choose a course of action. All interactions are understandable, and specific to the problem.
- Further define what is currently the first standard in this section: "Inform your customers of the top risks they incur if they use the products or services offered via a partner." It is not understandable. Do not expose clients to risks of partners.
- The current standard #4 in the DFS Standards, "As part of the agent selection criteria, consider whether the personality, culture, and language(s) spoken will appeal to your target customers," is a concept already included in the Universal Standards.
- The audit department should be involved in the review of controls in place regarding the treatment of customers.

Fraud mitigation small-group discussion:

- In the implementation guide, be more specific about fraud types: an annex to the standards may include a list of DFS-related frauds (in all cases, FSPs run behind fraudsters so it cannot harm to have taken stock of known ones).
- The standards may benefit from some structure in terms of fraud types / source / impact, that may have an impact on how FSPs handle them:
    - Impact:
        - Frauds affecting customers and the FSP is liable (specifically, FSPs should be liable for agent fraud)
        - Frauds affecting customers and the FSP is not liable
        - Fraud affecting primarily the FSP with no immediate financial harm to the client
    - Source
        - Technical (IT related)
        - Internal & human (equivalent of loan officer fraud in MFIs)
        - External: friends and family, agents. External frauds are probably new and specific to DFS because key steps of the customer journey take place outside of the financial institution and may not be digital steps hence not remotely detectable through digital tools.
- Proactivity about collecting customer feedback should be emphasized, especially considering the threat of outside risks mentioned above. Customer research should take place before launching and while running a digital products, in order to identify potential risks (for example workarounds at agents that don't match the theoretical customer journey and introduce new risks) as well as these that materialized, talking to a larger sample of clients than the one that will reach out to customer service with complaints.
- Make the need for digital literacy training more explicit (in addition to customer training, public communication on fraud attempts).
- Point 1 of the standards may benefit from being reworded in terms that are more aligned with the usual risk management vocabulary (risk assessment, appetite, matrix, etc) as this is in fact the application of risk management processes to DFS.
- Different departments may be able to collect information on fraud risk (marketing, customer service, risk, audit) and FSPs should see how these different players coordinate (maybe through the risk committee).
- Refer in the USSEPM to "digital" frauds.

Managing algorithm bias small-group discussion:

- Clarify for what purpose algorithms are used (mostly credit, maybe also insurance).

- Provide a better definition of fairness (is segmentation / adaptation of loan amounts considered unfair) ?
- Restate in DFS standards that the first criteria upon which the algorithm's performance is assessed is the prediction of financial capacity: this should ideally not only be assessed through effective repayment but also the level of financial stress experienced by customers: are algorithms able to encompass an assessment of a customer's financial stress, beyond his actual repayment history?
- How to handle "root" discrimination causes such as the lack of data for some sub-groups that may result in their exclusion?

Outcomes small-group discussion:

- Collect data – why? What type of data?
- Limit check to digital data- add human check. Consider whether these data are external data, social objectives / internal data, or supply side data on customer.
- Consider working with the mobile service provider on outcomes data analysis, if data privacy allows it. There is much lower use of mobile services by women.
- When gathering data on the customer journey, do you mean the end-to-end flow of activities or the emotional and behavioral side? The latter can help with prediction of customer behavior.

Partnerships small-group discussion:

- The Universal Standards for SEPM already have this section:

4.C.3	EP	The provider protects clients' rights to respectful treatment during the loan collection process.
4.C.3.1	Indicator	The provider's collections policy includes the following:
4.C.3.1.1	Detail	A list of appropriate and inappropriate debt collections practices, including collateral seizing practices.
4.C.3.1.2	Detail	A schedule for the collections process that allows time for the debt collector to determine the reasons for a client's default and for the client to find solutions.
4.C.3.1.3	Detail	The provider informs the client prior to seizure of collateral, allowing the client to attempt to remedy the default.
4.C.3.1.4	Detail	A prohibition on sales of the clients' collateral to the provider, the staff of the provider, to their relatives, or to third parties involved in the seizing process.

- Add to 4C3 (see above) the need to cover external debt collections partners under the third-party providers listed there.
- It is good to treat the third-party providers like employees or it will be a failure.
- The document says that the FSP should have annual meetings with its third-party providers to discuss the partnership. However according to the type of business the provider is doing, the FSP should meet with them quarterly, but never less

than semi-annually. It's too long to go a year between meetings, especially for partnerships related to digital services because it is a fast-paced industry.
- The FSP needs a relationship manager for each third-party provider.
- If the FSP uses third-party providers and doesn't ensure that they have the proper cybersecurity measures in place, it's the client who loses in the end. There needs to be a designated person to manage the partnerships.

Prevention of over-indebtedness small-group discussion:
- What does "aggressive" mean in this first point?
    - Does this mean a concept like: "you have 5 mins before offer closes"
    - Customer may be tempted to get loan without explanation of repayments or price? This is linked to transparency
- Cooling off period
    - Does this imply after disbursement or before?
    - Does this cause operational strain? Would be a system strain?
    - What is definition of nano/micro loan? Term or Size
    - Based on client profile (like new customer)
- What does "use" mean?
    - Many customers don't have digital footprint
    - Reliant of MNO partnerships
- Loan size graduation is linked to affordability, not purely previous loan amount
- Strict policy on parallel loans, review of mandatory pauses or rather offer credit facility
- Better (longer term) product should be available and recommended to customers
- Focus wording on financial literacy rather than around "unscrupulous lenders"
    - Goal here is for customers to work this out for themselves
    - Is this covered in other sections like fraud (for non-lending products)
- Reminding customers of their obligations related to loan repayment should be built into the digital customer journey
- Asking customers for feedback should be built into digital customer journey, including into the new loan application process,
- Use data to set flags for potentially "engineering" of behavior by clients/ gaming
- Missing : use of call center as channel to customer info gathering
- Mention that for DFS the point 4.A.1.1.2 in Universal Standards ("("Loan approval decisions are made by at least two people, one of whom does not interact directly with the client") doesn't apply.

Product design & delivery small-group discussion:
- Feels like a how-to guide rather than a set of standards
- Focuses on how to design the products, rather than a set of standards around their design
- Could rather be worded around assessing if the methodology of design and delivery meet a required standard, rather than a guide
- At times, seems too prescriptive (like testing for 3 months)

- Unclear why so much detail on this for DFS, when pitched at higher level in the Universal Standards
- Role of FinTech partnerships in the product design is not a strong theme, for example often new product development will be led by the FinTech, and the MFI/FSP would then access if this product is a priority/add value to their target customer base
- In FinTech partnerships, the standards must outline that the FSP has the technical capability to manage all aspects of the product- like technology/scoring etc.
- More detail on standards around testing, like agile approach and customer sampling
- Role of staff on advisory role. Protect people less financially literate.
- Restructure DFS Standards content in this area by phase of project development. Make it easy to read and make the sub-topics more actionable.
- Remember that digital product delivery happens not only with Smart phones but also with old phones.
- Design products with the purpose in mind – how will this help customers – not on what is not working.
- Product design is not always bottom up. There are opportunities to build top-down based on purpose.

Responsible pricing small-group discussion:

- Pricing strategy could also be included in standard 1A of the Universal Standards ("The provider has a strategy to achieve its social goals.") It is important that board and management develop and update the pricing strategy.
- Have simple fees - simple enough for customers to understand.
- The time dimension (before the fee is charged, when product is being selected) is important.
- Costs may differ according to market. Digital financial services are supposed to facilitate efficiencies in FSPs' systems that allow them to limit costs (e.g., chatbot, call center). But in some areas, such as rural areas, the FSP must implement a higher-cost model such as having a physical person/credit officer to give information to clients.
- 6.B.2.3 of the Universal Standards says, "Arrears interest and penalties do not compound debt; they are calculated based on the principal amount only." It is unclear why for DFS "late fees" comes in addition to 6.B.2.3.

Transparency small-group discussion:

- Include a clause that all the DFS should follow the same wording in each of the digital contract --> standardization of the messaging across the country. Visual image is important --> standard visuals. Key Facts Document (KFD) could be standardized.
- How to transfer the KFD and contract with all the necessary information virtually? It can be hard for the client to receive a contract of 20 pages digitally. Propose an alternative at branch level so they can pick it up and having a paper copy?

- Add to indicator 4.B.1.1. in the Universal Standards, which lists information that must go in a key facts document. Maybe add to this list the hotline/contact of the DFS + complaint handling number.
- We totally agree with the suggested indicator, “Give customers an option to speak to a live person.” The option to speak to a live person and what phone number or channel to use to contact this person should be disclosed in the KFD, especially if there are not a lot of branches, meaning the client cannot directly visit the institution easily, and the officer can be only contacted via phone.
- Unsubscribe option - link in the KFD or contract? Maybe comes more into privacy part.
- Regarding spot checks to test whether customers understand terms and conditions, the standard is written so broadly that a loan officer could be the one doing the spot check on his or her clients, but it would better for this to be done by an internal audit or call center team. The standards could be more specific about who is or is not the right person to do spot checks.
- Regarding the suggestion that a credit officer should receive confirmation of a transaction going through on his/her electronic devise after each transaction is conducted, the wording is a bit confusing. Why should the credit officer receive a confirmation? Is it necessary? They should already be following their portfolio on a daily basis to monitor delinquency. They already have a dashboard.
- We disagree with the suggested standard of, “If the provider is working with a third-party partner provide payments, each time the customer makes a digital payment, both the third-party partner and the FSP must provide the customer with a receipt.” We think that a joint receipt should be enough: like third-party on behalf of FSP, in order not to send too many messages to the client.
- Customers who are not digitally literate may not be able to apply for loans digitally and lack of digital literacy makes it challenging for clients to understand the process. Train loan officers on how to communicate transparently with digitally illiterate clients.

Notes from Other Discussions

Implementation Plan for the DFS Standards: Discussion

Debate: Integrate the DFS Standards into the Universal Standards, or create a standalone module?

- The moderator (Amelia Greenberg of SPTF) stated that all FSPs should implement the Universal Standards. In addition, those that offer digital products and services should also implement the DFS Standards. The current version of the DFS Standards leaves out many practices that FSPs should do because those practices are already covered in the Universal Standards. The question is, what is the best way to publish the DFS Standards? She asked the room whether they think the DFS Standards should be developed as a standalone module, or if they should be integrated within and throughout the Universal Standards manual. Participants responded as follows:

- There's lots of overlap between the DFS Standards and the USSEPM, so much so that it's probably best to integrate them.
- I do not think we should put the DFS standards in the same document as the Universal Standards.
- There are several things to consider. DFS needs to be a standalone document for fintechs. We could make the DFS standards an annex or an 8th dimension to the USSEPM so people can see they go together and just use it if its relevant to them. Or if we do integrate them into the manual, we should have some digital function inside social audit tool that makes it easy to identify and isolate the standards specific to DFS. The Excel-based evaluation tool should have the ability to filter by digital indicators.
- The level of maturity of the two documents is very different because the USSEPM is very mature, and field tested and the DFS Standards is new. Keep them separate until the DFS Standards are as vetted as the Universal Standards, and revised so that what remains in the Universal Standards are the broad standards ideas, not all of what it is currently in the draft document that feels more like implementation guidance but would be overly prescriptive to say everyone should be doing that. There should be references in the Standards to the implementation resources – the Standards are the WHAT to do and the implementation resources are the HOW to do it.
- [Several voices said this:] Integrate the DFS Standards into the main Universal Standards document because that's cleaner.
- It would be repetitive to include in a DFS Standards module the same practices that are already in the Universal Standards.
- The DFS Standards can fit into the existing seven dimensions of the Universal Standards. For example, managing algorithm bias is a governance issue. And there are already standards on data rights and privacy, data security, and product design.
- Let DFS become mandatory in time, like green. It took many years before green transitioned from optional to mandatory. That will give the DFS standards time to mature.
- When CFI released the Client Protection (CP) Standards, it released the CP Standards and also helped with implementation at the same time.
- The majority opinion in the room is that once the DFS Standards are finalized, they should be integrated into the Universal Standards manual with a way to identify easily which indicators relate specifically to DFS.

<u>Awareness raising about the DFS Standards:</u>

- Certain things are obligatory – like client protection and the environment, but DFS is still optional, and it should stay that way. Let them remain optional, especially if there's no money to support their implementation.

- There are options for implementing the DFS Standards – paper, Excel, or online versions of an assessment tool. Awareness raising activities should evaluate if DFS users have a preference or constraints that show us which way to go.
- We must give credit to the FSPs that helped pilot the DFS standards when the tool is finally built.
- We can't build DFS indicators into the online SPI social audit tool yet, because Cerise+SPTF need to fundraise for that work. So, we will start with an Excel-based evaluation tool.
- Fintechs are very young, very new – their products are raw – they need time to become more reliable sources of data.
- Talk to all stakeholders in inclusive finance about the DFS Standards. We all have a role to play in promoting them and/or supporting their implementation.
- The SEEP network is closed but the NGO organization community can reach out to fintechs directly.
- Reach out to people and get a champion of DFS Standards implementation within each organization. Explain what's in it for them.
- Nudges can be helpful. Remind clients about steps they are supposed to take. Could be SMS or audio recordings for illiterate clients.
- The regulators need to understand DFS as a product or a channel. In Nicaragua, fintechs are considered a channel and not like an MFI so they are not regulated at the moment. CONAMI wants the MFIs to be eligible for funding based on meeting all the social standards. We will need to train the MFIs and the clients on digital topics. The *Normas* (meaning, standards) will need to be refreshed taking these digital standards into account. We need to list out the MFIs' obligations and adjust the technology risk management *Norma* to include the ideas in these standards.
- Customer groups, like focus groups should be hosted to discuss these standards and obtain input for enhancing these standards and the customer protection tools. We should use testimony from the clients and complaints, and results from the DFS assessments, to continue to encourage FSPs to participate.
- At Genesis we have Evolution teams and Revolution Teams. Evolution Teams work on incremental change, improvement on what we already do. Revolution teams are for projects where's there's no map for where we are going but they are working on big changes and big ideas.
- Anyone who wants to is welcome to participate in awareness raising.

<u>Pilot testing:</u>

- Amelia (SPTF) shared that funding is in place for West Africa and Latin America/Caribbean to support assessments using the evaluation tool for the DFS Standards that will be released likely second quarter of 2023.
- There are roles for the non-FSP players as well, such as awareness raising, fundraising, piloting the indicators, and evaluation of the standards e.g., what did we learn and how did it help?.
- At Catholic Relief Services (CRS), we want to be brought into the learning about how to offer DFS responsibly ahead of time, so we can know the risks. We want

the DFS Standards pilot testing to cover all the regions where we work. There will be variations across the regions in terms of implementation.
- Make sure there's a variety of legal types of FSPs that test the DFS Standards. For example, MFIs, fintechs, mobile money providers, telcos.
- Questions we should ask during the pilot:
    - Which indicators of all the current ones are the most important?
    - Are there any indicators in the current list we can cut to make room for digital?
- GSMA has an evaluation tool. We should check on what's in it as we create ours. We can adopt their indicators, as relevant, rather than trying to write our own that cover the same concepts.
- Could the DFS assessment be run on a product basis instead of on a whole FSP? We'd like to try it out on a certain product offered by FINCA DRC, for example.
- Analyze results for different segments of clients. Also ask about the length of experience that the FSP has with digital, and take this into account when considering the results of the pilot.
- The Swiss Capacity Building Facility (SCBF) is a potential source for funding for the DFS pilots.
- GSMA has an evaluation tool - we should check what is in it as we create the assessment tool for the DFS standards.
- Can this be applied to a product instead of a whole MFI? It would be good if it could - for example, the Click product that FINCA DRC has.

Responsible Digital Ecosystem: Presentation by Eric Duflos (CGAP)
- Eric polled people in the room about their exposure to fraud. CGAP did research in the Ivory Coast on this. Their results were about the same as what we got from the informal poll of participants in this session, namely, that 80% of the people surveyed have received a fraud or spam or phishing message in the last year. But, in the Ivory Coast, 40% of the people had lost money from the fraud, while among conference participants, it was 8%, and the two people who raised their hands were African.
- CGAP's research on DFS has identified several main categories of risk:
    - Fraud
    - Misuse of data
    - Poor transparency, and
    - Poor redress of grievances.
- Fraud and misuse of data are on the rise.
- There are also two cross-cutting risks, which are networks and agents.
- Research also found that men and people in urban areas are more digitally capable, but that is mostly due to who owns the phones.

CGAP's Project to Help FSPs with Digital Transformation: Presentation by Gerhard Coetzee

- Over 2-3 years, CGAP did a demand analysis and impact analysis on MFI digitalization and worked with a first cohort of FSPs on digitalization.
    - 2020 – measured the success in the work of promoting digital
    - 2022 – deep dive on a few MFIs (6) on the principles
- In 2023, CGAP is launching work with a second cohort, with about 20 MFIs. This phase will offer a lighter amount of technical assistance, but the TA will be based on what worked with the first cohort. The purpose remains to support digitalization.
- After working with the first cohort, CGAP identified six **principles for successful digitalization**
    1) Start with the core business (e.g., the credit product). The project needs to generate value for the company because otherwise it won't cover the cost of the digitalization. You can digitalize processes without digitalizing the whole institution. For example, offer digital disbursements and renewal but not digital repayment capacity analysis.
    2) Minimum viable products – keep it simple in the initial phases.
    3) Measure return on investment (ROI). If the technology supports multiple parts of the business, then global measures of ROI are required.
    4) Change management – Start at the top and go down the line so there is buy-in among management and staff. You can start with the shareholders and the board, or the board and the international network level. Don't forget to do change management for the clients too.
    5) Measure customer behavior change to know the value created with these projects. The change needs to be measured from day 1. Measure change at the partner level too if there are partners. Talk to the clients to know if they perceive value from the digital product or the digitalization of processes.
    6) Incremental success is the common path to success in digitalization. Go step by step.
- The CGAP project can inform work on algorithm bias, though it has not yet evaluated fairness because it's too early for that and we need time to learn.
- We can prevent over-indebtedness with this type of project. For example, 4G has an early warning system for identifying over-indebtedness. If the money is disbursed too fast and too easily, then over-indebtedness will be the natural results of digitalizing the credit product.
- CGAP recommends that MFIs do not digitalize all the repeat loan applications automatically. For example, give a third or a quarter of the loans that are being renewed an in-person review, as a check, to prevent over-indebtedness.

Annex – Draft DFS Standards as of 27-Sep-2022

Cerise + SPTF
Standards for Responsible Digital Financial Services
(Draft as of 27 September 2022)

Target Audience
Financial service providers (FSPs) seeking to offer digital financial services (DFS) responsibly.

Goals
At minimum, FSPs will implement the management practices related to consumer protection described in this document. As a result, customers will not experience harm from using digital financial services. Additionally, FSPs that are committed to helping customers use DFS to improve their well-being will implement that management practices in this document related to the "doing good" elements of social performance management.

How to Begin
Evaluate your FSP's current performance against the Universal Standards for Social and Environmental Performance Management ("Universal Standards") *and* against the standards for responsible digital financial services ("DFS Standards"). The Universal Standards describe in general the management practices for an FSP to implement to protect customers and achieve social and environmental goals. The DFS Standards describe additional management practices that help mitigate risk and promote better outcomes for clients when the FSP delivers its products and/or services through digital channels.

Organization of this document
The document covers 13 different topics, organized into three main categories:

1. Risk management and consumer protection
    - Complaints mechanism
    - Cybersecurity
    - Data rights and privacy
    - Fair and respectful treatment of customers
    - Fraud mitigation
    - Prevention of over-indebtedness
    - Transparency
2. Promoting benefits for clients
    - Managing algorithm bias
    - Outcomes
    - Product design and delivery
    - Responsible pricing
3. Collaboration with third parties
    - Agent management
    - Partnerships

Risk Management and Consumer Protection

Complaints mechanism

1. Take responsibility to resolve a customer complaint even when it relates to an issue that the partner organization must correct.
2. At the outset of a partnership, establish who will be your point of contact within the partner organization, to help you resolve complaints by your own customers, but that are related to services provided by the partner.
3. Encourage your customers to come to you with complaints about partners.
4. Train customer service employees on how your partner's complaints mechanism works.
5. Train customer service employees on how to respond to customers who voice complaints related to services offered by a partner.
6. Train agents on how to respond to complaints.
7. Train/encourage agents to use your complaints mechanism.
8. Equip the complaints mechanism to register complaints by agents.
9. Analyze complaints data for the following information:
    i. to see if certain segments of customers are underrepresented among the customers who complain
    ii. to see if certain issues are underrepresented among the types of complaints
10. Research why some customers do not file complaints even when they have reason to complain, and address obstacles that prevent customers from complaining.
11. Proactively survey a sample of customers to ask if they have complaints.
12. Monitor social media to see if customers are complaining about your services, and respond as needed.
13. Do weekly trend analysis on the types of complaints you receive.

Cybersecurity

1. Define board and management responsibilities related to data security, including how the board will ensure risk management related to digital innovation and activities.
2. Include cybersecurity costs in the budget every year.
3. Implement a cybersecurity system that has at minimum these features: physical security, daily (at minimum) data back-up, ongoing automated checks that flag any suspicious activity, and an always-operational data security system that detects attempts to hack into your files.
4. At least once every quarter, have a professional (either internal or external) try to hack your own data.
5. When setting up a data security system, take the following actions:
    a. Increase awareness of management and the board.
    b. Get an external audit of your data security.
    c. Strengthen all gap areas.
    d. Train the technical team on risk management.
6. Identify what is core to business function versus what is less important, and implement the strongest security measures for the fundamental functions.

7. Take the following actions to achieve acceptable cyber-resilience:
    a. Develop threat scenarios for the kinds of incidents that relate to your organization's highest priority cyber risks.
    b. Have a response plan for cyberattacks.
    c. Build capacity to respond to those scenarios.
8. Any time you release a new digital product/service, assess data security for that product/service specifically, and implement new security measures as needed.
9. Monitor employees' use of computer systems and audit their activities.
10. Learn what cybersecurity measures any potential partner has in place, and work only with those with adequate cybersecurity systems.
11. If you work with a potential partner, assess cybersecurity risks that arise from the interconnection of your systems, and implement risk mitigation measures as needed.
12. Identify which person or team, either internal or external, is in charge of cybersecurity and, including who is in charge when the main person is out of the office.
13. Train customers on cybersecurity, on an ongoing basis.
14. Train employees on cybersecurity, on an ongoing basis., covering at minimum their own responsibilities, how to talk to customers about cybersecurity, and how to direct customers to the right person if customers raise an issue.
15. Train board members on cybersecurity, on an ongoing basis.
16. Report data on cybersecurity (e.g., hack attempts, measures taken, new risks identified) to the board at minimum quarterly.
17. Report data on security activities to management at minimum weekly.
18. Notify customers within 24 hours if you do get hacked.
19. If customers lose money because your systems got hacked, refund the customer.
20. Notify other FSPs in your market of any attempts hackers make on your data security, including sharing the specific methodology they used.
21. Participate in any initiatives in your country or region involving information sharing about cybersecurity threats.
22. If you do not have the resources to invest in cybersecurity, then do not offer digital financial services.

Data rights / privacy:

1. Inform customers of the benefits to them of agreeing to share their data, and explain to customers the consequences of opting out of data sharing.
2. Make it an opt-in option for customers to share their data.
3. Collect the minimum amount of data you need from customers.*
    * define the "minimum" data as the data you use to make a decision about whether to offer them a product or service, and at what price
4. Have a system for how to receive and process customer requests to correct inaccurate information you (the FSP) have about them, and inform customers of this system.
5. If you deny an application for a product, explain to the customer why you denied it.
6. The leadership of the FSP defines a strategy for how the FSP processes and uses data, and monitors the implementation of those practices.

Fair and respectful treatment of customers:

1. Inform your customers of the top risks they incur if they use the products or services offered via a partner.
2. Incorporate human touch at minimum at the following points in a customer's journey: a) Onboarding/receiving information about the product; b) Resolving a problem or complaint; c) Answering customer questions
3. Record calls made to the call center to monitor customer service, noting performance when responding to complaints both about the provider's services and complaints about third-party providers.
4. As part of the agent selection criteria, consider whether the personality, culture, and language(s) spoken will appeal to your target customers.
5. When you educate customers about a product, teach not only how the product works but also what behaviors are good/bad from the service providers, which can be employees, agents, other partners.

Fraud mitigation

1. Create a strategy to mitigate fraud risk and address fraud if/when it does occur:
    - Quantify how much instance of fraud, as a percent of overall portfolio, the FSP will tolerate.
    - Research which types of fraud are likely to occur at different stages of product use, and which segments of stakeholders perpetrate the fraud, and use this information to inform the fraud risk mitigation strategy.
    - Identify what investments in hardware, software, data analytics, and/or capacity building are necessary.
    - Define the systems you will put in place to mitigate fraud risk.
    - Define what your fraud response will be, including the specific responsibilities of various employees. The plan at minimum should state how the FSP will notify affected clients, inform the authorities, and stop the fraudulent activity, as well as defining what actions, if any, the FSP will take to assist customers who were victims of fraud, and what actions, if any, the FSP will take against the perpetrators of the fraud.
2. Implement fraud risk mitigation measures that at minimum include a system of checks and balances, automated data analytics that identify suspicious activity, using customer complaints data for insight into potential fraudulent activity, and audits. If the FSP works with third party partners, the system should also include mystery shopping.
3. Each time the FSP introduces a new product, analyze where fraud is most likely to occur and implement fraud mitigation measures as needed.
4. Report daily any possible fraudulent activity detected by data analytics to senior management.
5. Train customers using at minimum two different channels on how to protect themselves from fraud.

6. Train employees and agents on how to detect and avoid fraud.
7. If you identify fraudulent activity, notify customers within 24 hours.
8. If a customer is a victim of fraud despite adhering to good practices for fraud avoidance, the FSP restores to his/her account any lost funds.
9. Monitor your response times each time you respond to fraud.
10. Share publicly what fraud attempts your FSP has confronted, to help others avoid it.
11. The board of directors oversees the implementation of fraud mitigation measures and monitors instances of fraud.
12. The person in charge of monitoring fraud (e.g., the Risk Manager) reports directly to the Board and not the CEO.

Prevention of Over-indebtedness:

1. Analyze instances of aggressive sales (tracked via client complaints) and poor portfolio quality by the channel through which the FSP recruited the client (e.g., Facebook) and/or through which the FSP delivers services.
2. Offer a cooling off period, during which the customer can choose to return a loan without penalties. The exception would be for micro/nano loans.
    - NB: Some interviewees agreed with this idea and others did not.
3. Use electronic data (e.g., transactions with suppliers, retail transactions, mobile transactions if the MNOs will share it) to estimate a customer's monthly expenditures/income, and therefore appropriate loan size.
4. Educate customers about risks of taking out loans from unscrupulous actors.
5. The FSP should interact with credit customers regularly to remind them of their obligations.
    - "Best portfolio performance is in places where the credit officer has the best training and they're interacting with customers to remind them of their obligations." – a DFS expert
6. Pro-actively seek feedback periodically from customers who are getting automated loan increases, to check on positive or negative effects from taking out loans.
    - "Be very careful with any strongly automated underwriting. At the end of the day, I don't think a fully digital banking system for customers who have a certain level of financial literacy is a responsible thing to do. Personal touch has to remain in place. It means you understand what's happening in the other person's life. Even if you're standardizing and segmenting, you have to understand what's happening. There's a chance of putting them in a worse situation by giving them automated loan increases." – a DFS expert

Transparency

1. In addition to document and sharing key facts in an agreement, develop clear messaging, in local languages, to use to disclose key facts again in a quick and accessible manner.
2. Define a strategy for how and when to share messages with key information. This strategy should include a different system for how many messages you send to first time users versus to those who have used the same product multiple times.
3. Design digital interfaces to be simple and visual enough to be used even by those who are not digitally literate.

4. Give customers an option to speak to a live person.
5. Do a spot check on a sample of customers to test whether customers understand key elements of the terms and conditions. If not, improve disclosure processes.
6. Every time the customer conducts a digital transaction, the customer should receive a digital receipt and the credit officer (or equivalent) should receive on his/her device a confirmation message for that same transaction.
7. If the provider is working with a third-party partner to provide payments, each time the customer makes a digital payment, both the third-party partner and the FSP must provide the customer with a receipt.
8. Collect information about the digital channels to which your customers have access, so you know through which channels you can share information. / SIMILAR TO / Ask customers how they get information. Then deliver information through those channels. Segment the answers by customer type.

Promoting Benefits for Clients

Managing algorithm bias

1. The provider defines specifically what "fair" algorithmic function means.
2. The provider shares the definition of fair with its board of directors.
3. The board of directors hold management accountable for fair algorithmic function.
4. If outsourcing algorithm development:
   - Inform your development partner of target customers and discuss a strategy to avoid algorithmic discrimination.
   - In the service agreement, do the following:
     i. Define parameters for algorithm
     ii. Define what specific tests the partner will run to check that that the algorithm is "fair" according to your definition
     iii. Require the partner to check annually the algorithm's fairness, according to the definition determined by the provider, and make corrections, as needed.
5. If developing the algorithm in-house, credit officers and management take part in the development of algorithm design.
6. If you have information technology (IT) specialists developing your algorithm, train them on your mission and vision and target customers so they understand the context in which the algorithm will be deployed.
   - Before you launch the use of algorithm, test whether your *data* are biased.
   - Before you launch the use of an algorithm, use synthetic or real data to test the following:
     i. Whether the algorithm is "fair," according to your definition of fairness
     ii. Whether the algorithm is treating equally men compared with women
     iii. Whether the algorithm is treating equally any other customer segments that are relevant to your social goals (e.g., rural vs. urban)
7. Before you launch the use of an algorithm, take the following steps to solicit feedback from stakeholders:
     i. Identify the stakeholders involved in the use of this algorithm

   ii. For stakeholders who are not clients, speak with representatives from each of the stakeholder groups to identify any concerns they have about the use of the algorithm
   iii. For stakeholders who are clients, interview representatives from each segment of customer that the FSP identifies as important (e.g., women/men)
   iv. Document what you've learned in a way that makes it clear which stakeholder group had which concerns.
   v. Qualify risks in terms of which would be high or low priority to mitigate, and then decide which you will address and which you will not
   vi. Take action to mitigate the risks you are going to address
8. Analyze your algorithm function for fairness on an ongoing basis, according the frequencies below:
   i. If the algorithm is learning continuously, check function at minimum monthly.
   ii. If an algorithm function is fixed, check function at minimum annually.
9. If you find that bias exists, determine if it is coherent with your social goals and strategy.
10. Prepare reports, at minimum quarterly, on algorithm function. Analyze at minimum this:
    - Who is being approved, by customer segment, and compare who is actually being served with the market that you want to serve
    - Whether the algorithm is accurate (e.g., check whether the algorithm's decisions on loan sizes for target customers are the same that traditional repayment capacity analysis would make)
11. Share reports on algorithm function with senior management, credit department, the risk management team, and the board of directors; discuss results and identify any corrective action needed.
12. Use information from customer complaints to inform your review of algorithm function.
13. In cases of a systemic shock (e.g., a pandemic), discontinue the algorithm and review it.
14. At least some members of the team that define algorithmic "fairness," and determine what analyses to conduct to test fairness, represent the population whose data are being scored by the algorithm.
15. Do not use algorithms if you do not have the capacity to analyze whether they are fair.

Outcomes

1. Collect data on which customers are using digital products and which are not, by customer segment
2. Verify accuracy of customer data via automated, digital checks.
3. Have annual discussion at the management level to review data and identify potential concerns related to digital products (e.g., low liquidity among agents).
4. Continue to track each customer's journey.
   - Tip: Use technology (e.g., call centers, SMS, IVR)
   - Tip: You can combine into one survey questions related to outcomes and questions related to digital literacy and digital demand of customers.
5. Track data on mobile phone usage, by gender. There is still a much lower use by women.

6. When building the strategic plan for DFS, identify simultaneously what is the business case for the FSP and what is the value that the customer will gain.
7. Identify which outcomes you need qualitative data to monitor and which you don't.
    - Example: If your goal is to promote savings, you can see quantitatively whether customers are using a savings product. But you would do quantitative calls to understand why certain customers are dormant.
8. Use outcomes data to inform product design.

Product design and delivery

1. Start product development with the discussion of what is not working well for customers and how to solve it.
    a. Should be bottom-up, not top-down. Example: Select partners that have found ways to use technology to address the pain points your customers experience.
    b. Don't start with technology and then develop a product around it.
2. Use the data you have to identify problems (e.g., no liquidity among agents)
3. Build the digital literacy of your customers enough for them to use the digital products and services you offer safely and effectively. Some tips:
    a. Figure out who customers trust and deliver training for customers through them
    b. View training as ongoing, not one-time
    c. Embed the tools that are used to build digital financial capability into the product delivery process. Providers should see this as part of their service provision.
    d. Use a lot of step-by-step guides and a lot of visuals.
    e. Leverage peer learning.
        i. "The beauty is once one customer learns, then they teach the others. Usually after they learn, it's a straightforward process." – a DFS expert
        ii. "The FSP needs to identify who the customers trust. We tried having partner orgs who knew the tech best offer awareness raising and digital literacy training. Then we switched to a model where there were early adopters, they trained them, and then the early adopters trained customers." – a DFS expert
4. Design digital products around technology that target customers already know how to use OR build capacity of target customers to use a technology before implementing it.
5. Research levels of digital literacy, by customer segment, during market and pilot research
6. Design digital pilot testing to be done quickly (about 3 months), with a focus on pilot testing solution ideas but not a fully developed project.
    a. This requires a break from traditional thinking, which involves spending a lot of time building and testing a single solution.
    b. Drop things quickly that do not work.
    c. Consider conceptually testing a piece of the solution, then if it preliminary signs are that it could work, develop it more and pilot further.
        i. "Piloting needs to change – the FSP needs to be like a startup – trying a bunch of things and constantly upgrading internal technology." – a DFS expert
7. Integrate strengthening digital literacy as a part of product design and delivery, in multiple stages:

   a. At the point of onboarding, when a customer first uses financial services.
   b. Refresher digital literacy training
   c. [optional] In between, there could be business development services where users build capacities on different aspects of digital literacy.
      i. Note: Technology allows for innovative and effective ways to deliver trainings to customers, including over videos or via IVR
8. When training customers on new products, make it clear not only how to use the product but also how this product brings value to the customer.
9. Provide confirmation to a customer immediately after she makes a transaction. If customers are paying from a mobile wallet, they get two confirmations (from the MNO and the FSP) that the transaction happened.
10. Offer technology in an opt-in way, not mandated.
11. Design digital interfaces as simply as possible, so that even those unfamiliar with numbers can use them.
12. Design your products for the hardest to reach customer, who is likely a poor woman. If the product design works for the hardest to reach person, it will work for anyone.
13. Design products to address the four main barriers:
   a. Affordability (This is not just price, but infrastructure – does she have a phone? Can she buy minutes?)
   b. Availability (Note: women tend to need to be in their homes most of the day)
   c. Ability (Consider social norms too, meaning, understand not only whether she is able to use a phone, but also whether she thinks technology is for her.)
   d. Appetite (Does the product meet her needs? Does she trust it?)
14. Design products iteratively with customers. Select a small group of customers for this.
15. Use data to inform product design, from all stages of the customer journey, meaning even before they become customers. Examples:
   a. Analyze data from potential customers that started applying for a product and then quit, to see where in the process people exit. (Example: on an app, if your onboarding is two pages long and they start but don't finish, you can check at which question on page 1 or page 2 they stopped filling in the form.)
   b. Track dormancy and reach out to dormant customers to understand why they have stopped using your products.
16. Make KYC questions and requirements as simple and easy for customers as possible. Think through the purpose of every question you ask to be sure it is necessary.
17. Engage employees and/or agents in product design:
   a. Raise awareness – what are the benefits of this product?
   b. Train employees on all products
   c. Pilot test new products with employees first
      i. "If my staff have to go out and convince the customers, it becomes easier if they are going out and talking about something they know and that they have tested." – a DFS expert
   d. Define incentives. Are employees incentivized to sell in the right way?
18. Assign a unique identifier to each customer.
   a. Note: A phone number is not always a unique identifier, as people share phones.

19. Adapt design and marketing strategies for products to customer segments (e.g., rural women, rural young adults)

Responsible Pricing:

1. Board and management create a pricing strategy and review it with at minimum [X] frequency.
2. Communicate the annual percentage rate (APR) and all fees.
3. Have a simple fee structure.
4. Disclose the fee structure at the time the customer is choosing to use a product, not only at the moment when the customer is being charged a fee.
5. Do not have a minimum balance requirement for a savings account.
6. Put systems in place to protect customers from overdraft fees.
7. When a customer defaults, do not charge compounding interest or late fees.
8. Structure interest rate and repayment schedules for loans so that the customer never ends up paying more in interest than s/he received in loan capital.
9. Do not pass on innovation costs, inefficiency costs, or poor loan portfolio costs, to customers.
10. Reduce prices for customers who have a demonstrated record of on-time payment.
11. Monitor credit scoring algorithms to make sure they get more effective over time, leading to better ability by the FSP to price appropriately given actual customer risk and repayment probability.

Collaboration with Third Parties

Agent management

1. Define criteria to determine how many agents the FSP needs and in what locations, and apply those criteria when deciding which new agents to add to the network.
2. Have an agent code of conduct.
3. Sign a contract with each agent that includes at minimum the following information:
    a. what information that the agent must display in her place of business;
    b. the code of conduct the agent must follow when interacting with customers;
    c. the responsibilities of the agent in terms of recording and reporting transactions data;
    d. the responsibilities of the agent in terms of participating in training;
    e. agent base salary and incentive structure;
    f. the consequences for violating the terms of the contract / under what conditions the FSP would sever the relationship with the agent.
4. Before launching an agent network, create a strategy for managing agent liquidity in each market, at minimum for urban versus rural markets.
5. Raise awareness among customers that they may encounter insufficient liquidity among agents and the implications of that on how they plan or manage their financial lives.
6. Evaluate and mitigate the risk of harm that agents incur because of their work.
7. Train agents up front on the following topics, at minimum:
    a. the provider's policies, processes, products and services

   b. the risks involved in the mobile money business, notably how to avoid fraud, and the mitigation strategies
   c. good customer service
8. Provider refresher trainings on key topic to agents, on an ongoing basis.
9. When introducing a new product, train agents on that product.
10. Assess the effectiveness of agent training.
11. Build agent buy-in to the mission and vision of the organization through continuous engagement
12. Monitor each agent's adherence to the terms of her contract. Use both in-person and remote channels for monitoring.
13. Measure the level of activity for agents on a regular basis, at minimum in the following areas:
    a. what types of transactions the agent completed
    b. what types of transactions were request but the agent could not complete, and why
    c. frequency of transactions
    d. amount of transactions
    e. which platform/app the agent uses to conduct each transaction
14. Use data to monitor early warning sights of agent distress, rather than waiting for actual default or other bad behavior by agents.
15. Analyze customer complaints data for insights on agent behavior.
16. Implement a system of performance evaluation of agents. This system will include at minimum the following elements:
    a. Defining the performance indicators to be used for evaluation
    b. Defining the agent monitoring system
    c. Sharing with agents what the evaluation criteria are and how the FSP will monitor agent performance
    d. After an evaluation, share the results with the agent
17. Invest in experiential learning. Have your staff who are going to be responsible for agent management go into the field and observe how agents work.
18. Provide a channel that agents can use to ask questions/receive support on demand.
19. Conduct annual satisfaction survey with agents.
20. If the FSP operates in a country where the regulator or another stakeholder hosts a database of fraudulent agents, the FSP reports agents that it has blacklisted to that database and uses that database to conduct due diligence before signing a new agent.
21. When a new digital product launches:
    a. Select agents for the pilot test that are among the most active in the network
    b. Establish targets, incentives
    c. Launch an awareness raising program
    d. Provide more than one round of training for agents on the new product
    e. Track data on how many agents are aware of or using the new product.
22. Consult agents about ideas for product design improvement.
23. Pay agents a base salary.
24. Have a business plan that allows for agents to make money.
25. Make it possible for customers to use agents with their same gender.
26. Notify clients when agent locations change or close.

27. Inform customers of the principal ways in which agents can defraud customers (e.g., unauthorized fees) and what channel the customer can use to report any concerns.
28. Define a theory of change for agents. What does the FSP provide (e.g., trainings, incentives, oversight) and how do the agents perform as a result?

Partnerships

1. Research the 3-5 most common problems that customers tend to have with any partner organization you are considering, and ask the partner what steps it is taking to address these problems.
2. During contract discussions, ask about the potential partner's client protection practices:
    - Ask how the partner receives and resolves complaints.
    - Ask if the partners has a code of conduct policy and how the partner trains its staff on customer care.
    - Ask how the partner protects customers from fraud.
    - Ask how the partner keeps client data secure.
    - Ask what terms and conditions the partners imposes on its customers.
3. If potential partners do not yet serve the segment of customers you serve, discuss their strategies for serving them, and make the case why doing so would benefit them:
    - Ask potential partners if they already have plans to serve your customer segment and, if yes, what those plans are.
    - Prepare a case for why it's a win-win for the partner to adapt their offer to your customers
4. Have a service-level agreement (SLA) with each partner that includes at minimum the following: a) Complaints handling – who is responsible for what, and how do they resolve complaints; b) A plan to manage client data privacy given the data that will be shared between partners; c) Pricing; d) Data reporting – how does the partner report its data? How does the FSP have access?; e) If the partner uses algorithms, agree on a definition of what a "fair" algorithm function would be; f) If you are partnering to offer some online service to customers, specific who is responsible for what if that online system gets hacked; g) Exit clauses – under what conditions do you cancel the agreement;
5. If you partner with an MNO, if possible, select one that achieved GSMA certification.
6. Establish a direct line of communication and point of contact for your organization within the partner organization.
7. Define the indicators of success for the partnership. Agree on them with the partner and put them into the contract.
8. Meet annually with the partner to review what is and is not working and set expectation for the coming year:
    - Review and amend as needed the projections for revenue and numbers of customers related to the product/service that is offered via the partnership

- Analyze performance according to the indicators of success for the partnership

9. If customers lose money because of a failure in a partner's system, it is nonetheless the FSP's responsibility to restore funds to the customers' accounts. The FSP can pursue a refund from its partner organization separately.