2019 Boulder
Digital Transformation of Microfinance Institutions Program
Course Syllabus

Course Information

Course:	**Risk, Fraud and Consumer Protection in DFS**
Faculty:	**Paul Makin**
Dates:	**Week 1 (July 22 – 26, 2019)**
Time:	**Afternoon (14:30 – 17:30)**
Language:	**English**

Course Description

The pace of change across financial services is broad, deep and accelerating. Customer needs are rapidly evolving while new entrants and digital technologies are bringing both increasing complexity and new value propositions to the market daily. It is imperative that MFIs do not underestimate the importance and challenges of privacy, security and protection in their drive to keep up.

The goal of this course is to develop an understanding of the key types of risks that MFIs face with the adoption of digital technologies. We will examine and discuss the key developments and issues in customer onboarding, privacy, and protection, as well as in cybersecurity, AML and fraud. With this foundational understanding, we will explore the risks and opportunities presented by new digital technologies from digital identity through APIs.

Objectives

By the end of the course, participants will understand key trends and issues around risk, fraud and consumer protection in DFS. Most importantly, they will have sharpened their ability to think in a holistic manner about digital risks, and be in a position to understand the specific risks their service is subject to, and how to ensure that those risks are being managed.

Prerequisites

An interest in how digital financial services are delivered, and in ensuring the risks inherent in these services for both the services themselves and their customers are properly managed.

Audience / Participants

The primary beneficiaries of this course will be MFIs that are considering or who have recently begun their journey in offering their services digitally; equally, it will also offer substantial benefit to those who have already established their digital presence, and are increasingly aware of the rise in cyber attacks and the consequent risk of fraud against both their customers and their own organisation.

The course would also benefit those with a broader interest in assessing the risk intrinsic to DFS services for both customers and the services themselves, and how that risk may be addressed.

Methodology

This course is taught in a collaborative manner using real life use cases. It is built around the following sub-module structure:

- A short 'lecture', introducing a subject, presenting the issues, and describing some responses and relevant learnings;
- A case study, relevant to the sub-module;
- Breakout discussion sessions;
- Each breakout group bringing the result of their discussion back to the group, by appointing a 'lead' to present their views (a different 'lead' each time);
- Presentation of the group's conclusions.

This will be repeated for each short section, with around 2 or 3 of these sub-modules completed each day of the course.

Suggested Reading List

Digital Financial Services and Risk Management:
https://www.ifc.org/wps/wcm/connect/06c7896a-47e1-40af-8213-af7f2672e68b/Digital+Financial+Services+and+Risk+Management+Handbook.pdf?MOD=AJPERES

Cybersecurity for Mobile Financial Services: A Growing Problem
https://www.cgap.org/blog/cybersecurity-mobile-financial-services-growing-problem

BOULDER
INSTITUTE OF MICROFINANCE

Outline

Day 1:	**Introduction** **Teaching:** • Introduction to Risk Management Frameworks • The Risk Wheel: Classes of Risk • The Generic Model of DFS service delivery **Applied Learning:** My Two Most Dramatic Stories **Breakout Discussion**
Day 2:	**Specific Risk Areas: Customers** **Teaching:** • Customer Onboarding (Including Identification and Verification) • Fraud • Money Laundering/terrorist financing **Case Study:** TBD **Breakout Discussion:** **Specific Risk Areas: Agents** **Teaching:** • Understanding agents • Training • Fraud – by, and against agents **Case Study:** TBD **Breakout Discussion:**

Day 3:	**Specific Risk Areas: Technology** **Teaching:** • Cybersecurity: why you should never touch your mobile phone again! • Technology-based real world attacks: USSD, SIM Swaps • Social Engineering: Job seekers, prize draws **Case Study:** TBD **Breakout Discussion:**
Day 4:	**Cross-referencing Cybersecurity and the Risk Wheel** **Teaching:** • Non-technical aspects of cybersecurity **Case Study:** TBD **Breakout Discussion:** **Applying a Risk Management Framework (Part 1)** • Setting the Context • Identify the Risks **Case Study:** TBD **Group Discussion:**
Day 5:	**Applying a Risk Management Framework (Part 2)** **Teaching:** • Analysis and Evaluation of Risk • Define Risk Strategies • Monitor and Review **Case Study:** TBD **Group Project:** Bringing it all back together