FIRST+

Financial **I**nstitution **R**esilience & **ST**rengthening

Effective Risk Management:

Tools and Practices

Presenter name: Donna Nails

CapPlus
CapitalPlus Exchange

mastercard foundation

Young Africa Works

GHAMFIN
GHANA MICROFINANCE INSTITUTIONS NETWORK

What is risk management?

- Financial institutions are in the risk business.
- Risk department needs to **understand** the risk, **measure** the risk and **communicate** the level of risk.
- The senior management and board of directors decide if the risk should be minimized, controlled, or deleted.

Financial Institution's Risk Appetite

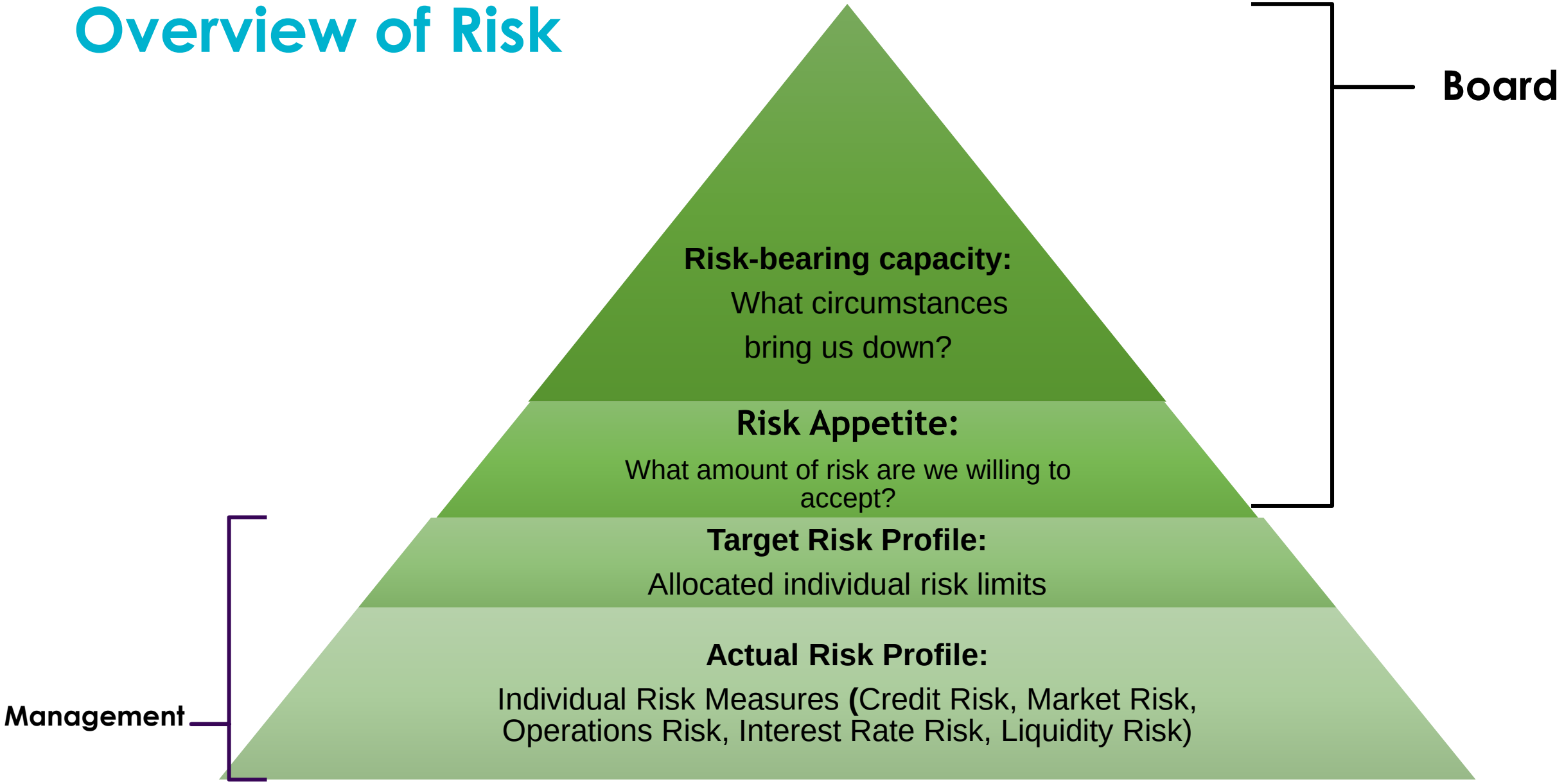
- Financial Institutions need to establish specific, measurable goals and benchmarks for all risks.

- The goals and benchmarks are the outgrowth of the financial institution's credit culture and risk profile.
    - Credit culture = credit values, beliefs, and behaviors.
    - Risk profile = various levels and types of risk on the balance sheet.

- Two different risk appetites:
    - Bosnia and Herzegovina:
        - Less than 1% Portfolio at Risk over 30 days and no charge offs
        - 3% loan portfolio growth annually
        - Acceptable profit level

    - Republic of Moldova:
        - 90% recovery rate (no Portfolio at Risk benchmark)
        - 15% loan portfolio growth annually
        - Very high profit level

Overview of Risk



Statement of Risk Appetite

- Board level document
- Quantifies and qualifies the desired level of risk (that an institution is willing to take)
- Expressed in terms of risk **limits**
- Normally refreshed at least annually
- Should not be a statement of what the financial institution aspires to.

Do not say "The company wants to be the largest financial institution in Ghana"

Say "The company does not accept risks that could result in a significant loss of its revenue base."

Statement of Risk Appetite

Examples of Benchmarks

Quantitative:

- **Earnings**: Do not deliver a below market average of earnings as compared to the company's peers.
- **Capital**: Capital ratio should not fall below 6%

Qualitative:

- **Manage growth effectively**: Monitor early warning indicators of non-sustainability
- **Business Activities:** Limit business activities to retail and commercial lending.
- **Zero Tolerance Risk:** No flagrant breaches, fines or headlines. No breach of delegated authority.

Risk Matrix

Overview

- **The tool** should be reviewed by management risk committee on a quarterly basis.
- Matrix is completed by ***compiling information*** such as liquidity reports and credit inspection reports will allow the committee to assess the risk.
- Matrix ***summarizes*** risk priorities and directs attention to high risk areas.
- Matrix is ***managed by the risk officer*** but is a result of communication with heads of departments.

***Quarterly review* is required because risks are unique to each financial institution and change over time.**

Matrix: Aggregate Risk Profile

Quantity of Risk	Quality of Risk Management: Weak	Quality of Risk Management: Acceptable	Quality of Risk Management: Strong
High	High	Moderate	Moderate
Mod	Moderate	Moderate	Low
Low	Moderate	Low	Low

Risk Direction:

- Increasing
- Stable
- Decreasing

Example: Risk Matrix

Activity	Aggregate Risk	Risk Direction	Comments
BUSINESS LENDING			
Credit underwriting	**High**	Increasing	- New lending team & leadership -Increase in volume and complexity of deals - Regulators had findings
Collateral valuation	**Moderate**	**Stable**	
Collection practices	**Moderate**	**Stable**	

Example Risk Matrix

Activity	Aggregate Risk	Risk Direction	Comments
LOAN ADMINISTRATION			
Loan review	Moderate	Stable	
Loan monitoring	Moderate	Increasing	-- New loan monitoring procedures being implemente --- Hot-button area of focus for regulator exams

Risk Matrix
Problems and Issues

- **Not reviewed often enough**…risk is not static, but changing continuously
- Not presented clearly and **not supported by information/data**
- **No actions** developed from findings
- **Responses are not honest**…no one wants to admit increased risk within their department
- **Not tailored** for the specific institution

Handout: Example of a Completed Risk Matrix

Operational Risk

- Credit Risk and Market Risk are 'assumed' risks with banking.
- Operational Risk is a general business risk with specific features in financial institutions.

Some Regulator's Complaints about Operational Risk:

- Needs to integrate qualitative considerations when completing a self-assessment
- Usually reactionary—do not sit back and think about the overall operation risk and impact on financial institution.

Operational Risk

7 Defined Risk Categories

1. **Internal Fraud**
   (theft of property, circumvention of regulations)
2. **External Fraud**
   (theft, robbery, hacking, phishing)
3. **Employment Practices and Workplace Safety**
   (breaches of employment laws)
4. **Clients, Products & Business Practice**
   (unintentional or negligent failure to meet an obligation)
5. **Damage to Physical Assets**
   (natural & human induced disaster)
6. **Business Disruption & Systems Failures**
   (disruption of business due to failure of IT, utility disruptions)
6. **Execution, Delivery & Process Management**
   (failed transaction processing such as accounting error)

Operational Risk

My Favorite Tool

Operational Risk Self Assessment:

- **Identify the operational risks in each department of the financial institution (Head Offices and Branches).**
- **Preliminary assessment questionnaire may help as well as internal audit findings of risk**
- **Regular updates (quarterly) and re-assessments based on Incidence Reports received from Branches and Departments and further input from the Internal Audit Reports**

Operational Risk Self Assessment

Five Areas:

- Administration
- Finance
- Human Resources
- IT/MIS
- Operations (including Branches)

Risk Areas are rated on the following:

- Inherent Risk
- Mitigation Factors

Then decide on response:

- Accept
- Manage/Control
- Share/Transfer
- Avoid/Insure

Each department develops list of risk areas. Then Risk Committee/Risk Person reviews.

Operational Risk Register

Example: IT section

			1. Very low	1. Insignificant	Low 1 - 4
Operational Risk Register			2. Low	2. Moderate	Moderate 5 – 6
			3. Average	3. Major	High 7 - 8
Information Technology			4. High	4. Critical	Critical 9 -10
			5. Very high	5. Catastrophic	

Description of Risk	Function	Process	Likely-hood	Impact	Inherent Risk
Users of IT systems may fail to keep their user IDs and passwords confidential i.e. sharing of passwords is prevalent	Information Technology	IT Security	5	4	9
Inadequate staff numbers in IT department may affect the service delivery to departments	Information Technology	People Management	3	2	5
Bank may not have sufficient desktops, laptops, etc. to enable staff provide efficient services to their customers	Information Technology	Premises	2	2	4
IT Dept may fail to install up-to-date Anti-Virus and other protective software in all its computer based systems	Information Technology	IT Security	2	2	4
The IT system and/or Intranet connection could be hacked into or otherwise sabotaged or interfered with	Information Technology	IT Security	2	4	6
Staff may have operating rights and privileges that are not commensurate with their responsibilities - Customer Information can be changed on the system by Loan Officer (including clients name and ID Number)	Information Technology	IT Security	5	4	9

Operational Risk Register - Inherent Risk Rating

Inherent Risk Rating

Likelihood of the risk	Impact of the risk				
	Insignificant (1) *Impact is negligible. Normal, routine procedure will be sufficient to deal with the consequence.*	**Moderate (2)** *Would threaten the function/activity; May cause small delay or small disruption.*	**Major (3)** *would necessitate significant adjustment to the overall function, would threaten to achieve objectives of the dept.*	**Critical (4)** *would stop achievement of functional goals and objective.*	**Catastrophic (5)** *would cause cessation of key activities of the Affiliate.*
Very low (1), *occur only in exceptional circumstances*	2	3	4	5	6
Low (2) *could occur at some time*	3	4	5	6	7
Average (3) *might occur at some time*	4	5	6	7	8
High (4) *will probably occur in some circumstances*	5	6	7	8	9
Very High (5) *expected to occur in most circumstances*	6	7	8	9	10

Example: IT System Hacked

Bank ABC

Bank XYZ

Operational Risk Register

Mitigating Factor

	Score/Weight
Excellent *All necessary controls/mitigating actions are more than adequate and effectively used.*	**4**
Good *All control procedures are adequate and effectively used.*	**3**
Moderate *Controls/Procedures to implement are adequate, but are not all effectively used.*	**2**
Weak *Some mitigating actions/controls are adequate and effectively used; others are ineffective or inadequate.*	**1**
Unsatisfactory *Control/mitigating actions are inadequate or missing.*	**0**

Mitigating Factors:

- Strong policies
- Good controls
- Insurance
- Results of Internal Audit Review
- Results of Regulatory Review

Operational Risk Register

Residual Risk = Inherent Risk + Mitigating Factors

Inherent risk	Minus Mitigating/Control				
	Excellent (4)	*Good (3)*	*Moderate (2)*	*Weak (1)*	*Unsatisfactory (0)*
Critical (10)	6	7	8	9	10
Critical (9)	5	6	7	8	9
High (8)	4	5	6	7	8
High 7	3	4	5	6	7
Moderate 6	2	3	4	5	6
Moderate 5	1	2	3	4	5
Low 4		1	2	3	4
Low 3			1	2	3
Low 2				1	2

Example: IT System Hacked

Bank ABC

Likelihood		Impact		Inherent Risk		Mitigating Controls:		Residual Risk
2	+	4	=	6	−	4	=	2

Bank XYZ

Likelihood		Impact		Inherent Risk		Mitigating Controls:		Residual Risk
3	+	4	=	7	−	2	=	5

Legend of the Residual Risk (RR)	Score
Low No major concerns; the risk is not eliminated, but is properly mitigated by systems of internal control.	1,0-4,0
Moderate Control is not strong, but risk consequence is not high. Options are to improve quality or quantity of controls, or monitor risk consequence to ensure it does not increase over time.	5,0-6,0
High Risk is still high either because of the uneffective controls or the very heavy consequences of the inherent risk. Close attention of the management on this issue is required. Negligence by the Senior management may cause drastic effects in a short-medium run. Control has to be strenghtened, the procedures have to be revised and adjusted and their implementation has to be attentively followed-up.	7,0-8,0
Very high Risk remains very high, as effectiveness of control is not satisfactory. Management should immediately respond and put in place mitigating actions in order to prevent from the catastrophic effects the risk could cause. This risk also requires a close attention of the shareholders (Ex. necessity to inject additional equity).	9,0-10,0

Operational Risk Register

Proposed Strategy

- Accept
- Manage/Control
- Share/Transfer
- Accept/Insure

- Financial institution is small and only has one person working in the Human Resources unit.
- Management and the board decided to assume the risk of having one person in this department.
- But..decided to mitigate some of the risk by training two people in finance to handle payroll to.

Operational Risk Register

Dashboard Example

	30th September 2014				
Department	**Residual Risks**				
	Low	**Moderate**	**High**	**Critical**	**Total**
Administration	15	1	4	0	20
Finance	22	4	0	0	26
Human Resources	14	6	1	0	21
Information Technology	10	8	2	2	22
Operations (incl Branches)	33	9	6	0	48
Total	**94**	**28**	**13**	**2**	**137**

Critical Elements:

1) Passwords were shared
2) Rights were not reviewed.

One Issues: CFO thought that all risks were well managed/controlled

THANK YOU!!!