

CIBA

CERTIFICATE IN BANKING

Session 3- Risk management

✓ Learning objectives

In this session you will learn:

- To identify the main risks faced by the bank
- How banks can mitigate such risks
- What is money laundering
- What is the BASEL accord

DO THESE NEWSPAPER ARTICLES LOOK FAMILIAR?



NINE ARRESTED IN PMC BANK CASE

SEPT 30: EOW files FIR against 10 accused in PMC Bank loan fraud case. It has arrested 9 persons so far

ARRESTED ACCUSED

- Rakesh Wadhawan | EXECUTIVE CHAIRMAN, HDIL GROUP
- Sarang Wadhawan | RAKESH'S SON, AND VICE-CHAIRMAN AND MD, HDIL GROUP
- Joy Thomas | FORMER MD, PMC BANK
- Waryam Singh | FORMER DIRECTOR OF HDIL AND FORMER CHAIRMAN OF PMC BANK
- Surjit Singh Arora | DIRECTOR, PMC BANK
- Jayesh Sanghani | AUDITOR



- Ketan Lakdawala | AUDITOR
- Anita Kirdat | AUDITOR
- Ranjit Singh | DIRECTOR, PMC BANK

What Rs 94 cr online fraud says of bank security

MOHAMMETHAVER
MUMBAI, AUGUST 19

LAST WEEK, Pune-based Cosmos Bank lost Rs 94 crore in a coordinated digital fraud comprising thousands of online transactions made possible because of a malware attack on the bank's systems. A look at how the fraud was carried out, and what questions it raises of security systems:

The fraud began with a malware attack. Malware is malicious software that is normally sent as a link to the intended target, once clicked, it can install executable codes and scripts. It is normally avoided by using anti-malware and antivirus software, and firewalls. In this case, the malware compromised a digital system responsible for setting cash disbursement requests raised at ATMs. A person once swipes a card, a request is transferred to the core banking system (CBS) of the bank. If the account has enough money, the CBS will allow the transaction. In this case, the malware created a proxy server that bypassed the CBS and approved a series of 14,500 fraudulent transactions to withdraw Rs 80.5 crore — Rs 79 crore through 12,000 transactions in 28 countries, the rest in India. Another Rs 13.5 crore was transferred to a Hong Kong-based entity using a facility called Society for Worldwide Interbank Telecommunications (SWIFT).

The ATM transfers
These are suspected to have been done with 'clone-cards', although a senior source at National Payments Corporation of India (NPCI) said that this was certain in this stage. Clone-card and credit cards have been used in several cybercrimes. The fraudster collects the card details (these are sometimes even sold over the dark net, a network with restricted access) and uses a machine to copy these on dummy or blank plastic cards.

How SWIFT works
This is a network that enables financial institutions to send and receive information about transactions in a secure environment. Earlier this year, the SWIFT system at Citibank Bank, with its headquarters at Fort Belknap, Texas (Nada) was targeted, and nearly \$2 million in their loss was transferred to banks in Dubai, Turkey and China. The SWIFT system frequently releases security updates. Muskan Kose, director (product development) of Vinton, a cyber security firm, suggested that banks ensure that their systems are patched immediately after the update. "The developers at SWIFT need to understand the particular kind of exploits being used and neutralise them," he added. Fortinet NRC managing director and CEO A. Prakash said, "I think it is responsibility of individual banks to ensure that their protection measures are in place."

The timing
The attack on Cosmos took place around the same time that the RBI issued a warning of an "ATM cash out attack" where fraudsters could compromise a bank's payment processes using cloned cards at cash machines across the world to withdraw money. These attacks normally take place over the weekend, and Cosmos was attacked on Saturday.

Security concerns
It has said the RBI is in close grip of the problem and if these are followed, such incidents will not happen. "There is a case that far as security concerned, attention given to ensure a moral banker and cooperative banks have been identified. However, there are 10-15 cooperative banks as big as private banks and Cosmos Bank is one of them. Maybe RBI should pay special attention to large cooperative banks," he said. Cyber crime investigation expert Rishabh Bhatia said security measures across Indian banks are mediocre and gives the high level of coordination in international attacks. All banks need to upgrade their security mechanisms.

Customers' money
RBI guidelines say that if banks are at fault, they are liable to pay customers. "However, there is also the issue of inconvenience for account-holders. Account-holders at Cosmos Bank could not carry out internet and mobile banking which were suspended in the aftermath of the attack. Banks form a part of the 'critical infrastructure' and one would be sceptical about opening an account at a bank where security has been compromised," Bhatia said.

The Indian EXPRESS, 19th August 2018
www.indianexpress.com/1146912



WHAT IS RISK?

- Risk= Results Not = Expectations
- Risk is Probability of LOSS due to
 - Non-happening of an expected event
 - Happening of an Un-expected event

Why should we take risk? Can there be any activity without Risk?

WHAT ARE THE MAIN TYPES OF RISKS FACED BY BANKS?

- Market Risk
- Credit Risk
- Operational Risk

DRIVERS OF RISK

- Market Risk- External forces
- Credit Risk- Borrowers
- Operational risk- Internal processes

INTERNAL FACTORS- RISK DRIVERS



EXTERNAL FACTORS-RISK DRIVERS



MARKET RISK

- It is the risk of loss from adverse movements in the level or volatility of interest rates, Exchange Rates and market prices of assets/ Commodities.
- The Bank may experience losses due to factors that affect the overall performance of investments in the financial markets.

CREDIT RISK

It is the risk of loss from default by the Borrowers for repayment of principal as well as interest.

Operational Risk

It is the unexpected Loss arising on account of deficiencies in information systems or internal controls. Operational Risk is inherent in any financial activity.

WHAT IS RISK MANAGEMENT?

- ✓ Identify Risks
- ✓ Measure impact of Risk
- ✓ Establish Risk Hedging measures
- ✓ Overcome Risks before it comes over you
- ✓ Risk is inherent & co- extensive with activity



OPERATIONAL RISK EVENTS

- Internal fraud.
- External fraud.
- Employment practices and workplace safety.
- Damage to physical assets.
- Business disruption and system failures.
- Execution, delivery and process management.

MITIGATION OF OPERATIONAL RISK

- Define an operational risk policy at the Board level.
- Develop a system of effective internal controls with control activities defined at every business level.
- Have a well documented compliance policy
- Internal audit
- Employee training and motivation
- Stringent controls for new areas of activity including new products
- Disaster Recovery and Business continuity Plans
- Insurance and security measures
- Investment in Technology
- Outsourcing activities based on robust contracts and service level agreements

WHAT IS MONEY LAUNDERING?

- Money laundering refers to any procedure to change the identity of illegally obtained money so that they appear to have originated from a legitimate source.
- Stages of money laundering
 - Placement
 - Layering
 - Integration

AML GUIDELINES

- Prevention of Money Laundering Act passed in 2002 to prevent laundering. Came into effect from July 01, 2005
- It imposes obligation on banking companies, financial institutions and intermediaries to verify identity of clients, maintain records and furnish information in prescribed form to Financial Intelligence Unit (FIU-IND)
- RBI has provided detailed guidelines on the obligations of banks regarding KYC/AML/CFT
 - Every Bank is required to appoint a senior management officer as a Principal officer, who will report directly to senior management/ Board of Directors. He will be the liaison with the central Bank and other regulatory bodies for AML/CFT implementation. He will also be responsible for ensuring the guidelines within the Bank.
 - Every banking shall maintain a record of all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency
 - CTR and STR to be filed monthly with the FIU-IND

CREDIT RISK

Risk of loss from default by the borrowers for repayment of principal as well as interest.

Credit Risk may take other forms also:

- In the case of Guarantees or Letters of credit: Funds not forthcoming from the constituents upon crystallization of the liability
- In the case of Treasury Operations: Payment or series of payments due from the counter parties under the respective contracts not forthcoming or ceases
- In the case of Securities Trading businesses: Funds/ Securities settlement not getting effected due to insufficient funds or securities
- In the case of Cross-border exposure: Non availability and issues in free transfer of foreign currency funds or restrictions imposed by the sovereign.

WHAT CAUSES CREDIT RISK?

- Macroeconomic factors:
 - Slowdown in the economy
 - Government policies- monetary, fiscal, licensing
- Company specific:
 - Aggressive lending policy
 - Absence of proper credit management policy
 - Inefficient management,
 - Fraudulent practices

MITIGATION OF CREDIT RISK

- **Define a credit risk policy and strategy**
- **Adhere and review the 5C's of credit** –This is a system used by lenders to gauge the creditworthiness of potential borrowers.
 - **Character**—reflected by the applicant's credit history.
 - **Capacity**- measures the borrower's ability to repay a loan by comparing income against recurring debts and assessing the borrower's debt to income ratio
 - **Capital**- indicates the borrower's level of commitment / seriousness.
 - **Collateral**- This is the asset which is mortgaged for securing the loan.
 - **Conditions**- These are the terms and conditions of the loan.

MITIGATION OF CREDIT RISK (contd.)

- **Portfolio monitoring**
 - Ensuring compliance with the terms and conditions of the loan.
 - Physically inspecting the factory, godown and the financial statements
 - Monitoring performance to check the continued viability of operations.
 - Verifying end use of credit.

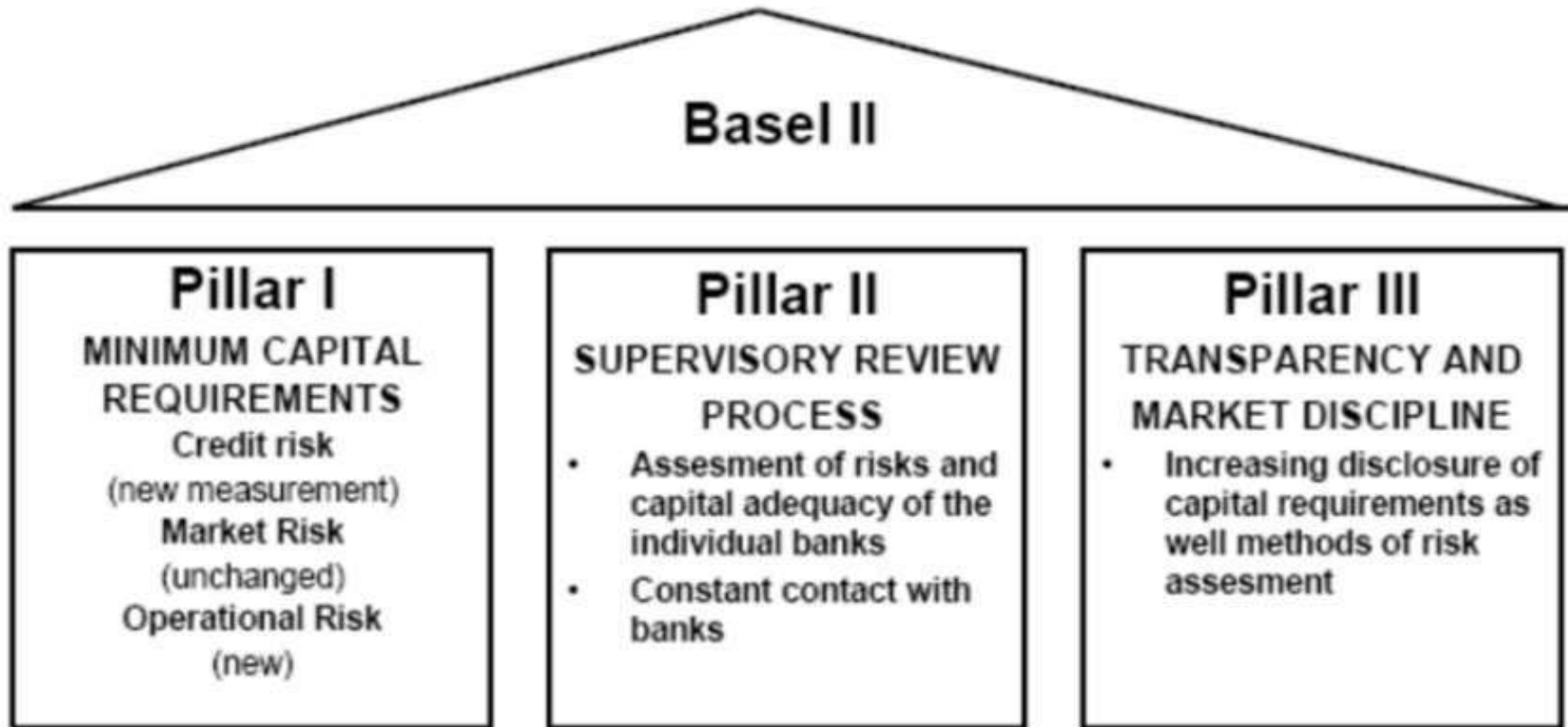
BASEL-AN INTRODUCTION

- Basel Committee on Banking Supervision (BCBS) was formed in 1974 by central bankers from the G10 countries to develop global regulatory standards for banks and to strengthen micro and macroprudential supervision.
- It is one of the committees of the Bank for International Settlements (BIS), based in Basel, Switzerland.
- Presently 45 members.
- Committee's proposals do not have any legal force but are the accepted international standards of best practices in banking supervision.
- IMF and World Bank use the Basel's standards as a benchmark in conducting their assessment of the banking system of a country.

BASEL ACCORDS

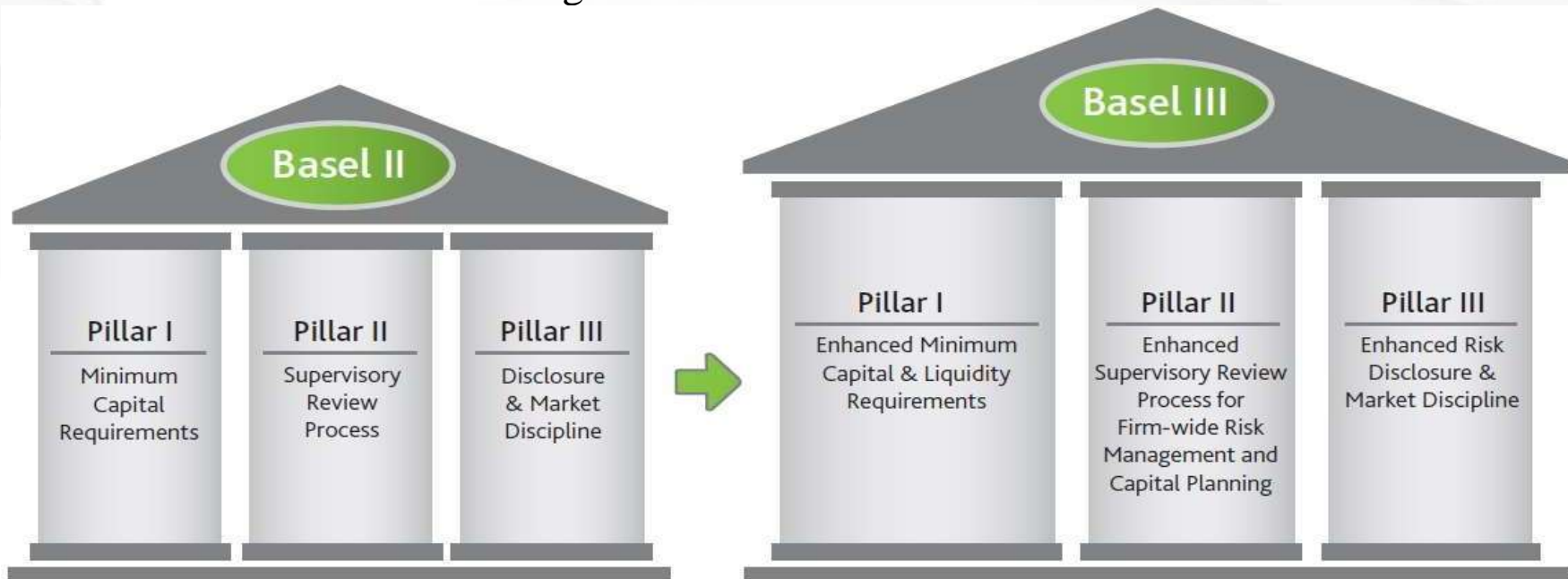
- **Basel 1** – introduced in 1988 and focused on the capital adequacy of financial institutions.
- Under Basel I, banks that operate internationally must maintain capital equal to at least 8% of their risk-weighted assets. This ensures banks hold a certain amount of capital to meet obligations.
- **Basel II** -introduced in June 2004

3 PILLARS OF BASEL II



BASEL II TO BASEL III

- Basel III was introduced in Nov 2010 after reviewing the reasons for the collapse Lehman Brothers and other big financial institutions in 2008.



Capital requirement under Basel II and III

Introduction to Basel III

- Major features of Basel III are
 - Recommends to keep better liquidity (norms expected by 2015 end)
 - Counter cyclical buffer – to be used when stressed / bad times (hence 0%) and keep when healthy (3%)
 - Systematically Important Financial Institution (SIFI) expected to go beyond Basel III recommendation
 - Snapshot of Basel II vs Basel III comparison

Requirements	Under Basel II	Under Basel III
Capital Conservation Buffers to RWAs	None	2.50%
Minimum Ratio of Total Capital To RWAs	8%	10.50%
Minimum Ratio of Common Equity to RWAs	2%	4.50%
Tier I capital to RWAs	4%	6.00%
Leverage Ratio	None	3.00%
Leverage Ratio for 8 SIFIs in US	None	8.00%
Countercyclical Buffer	None	0% to 2.50%
Minimum Liquidity Coverage Ratio	None	TBD (2015)
Net Stable Funding Ratio (NSFR)	None	TBD

Thank You