protiviti®
Global Business Consulting

WIRC of ICAI: Internal Audit of FS Entities

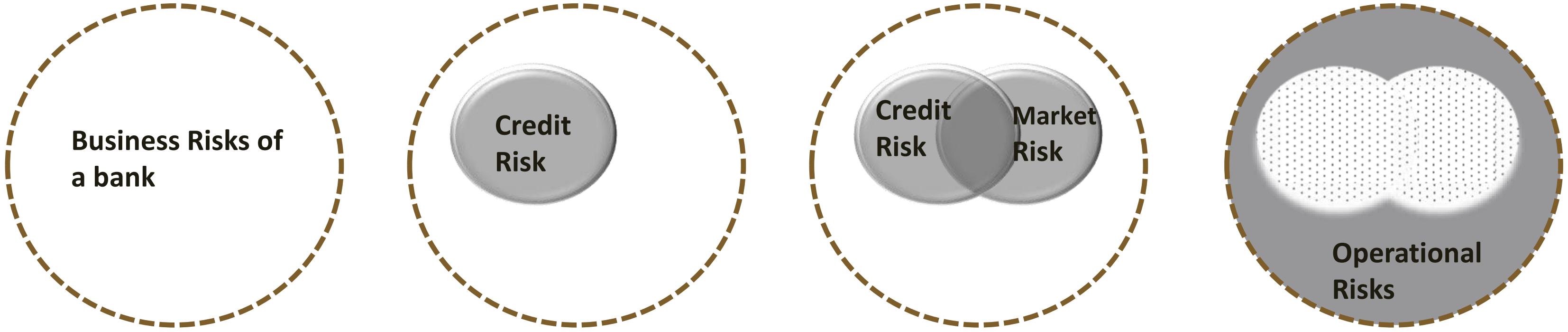
Operational Risk Management in Financial Services Entities

June 25, 2022

Ops Risk Events in FS

Scenario	Operational Risk Incidents	Cause
1.	Segregation of Duties	
	- **Client Confidential** - A dealer of the Investment Company was doing the job of settlement and maintaining trading books as well. As a result, he was able to do unauthorized trades and conceal losses by manipulating records. The Bank collapsed in 1995. (Loss - xxxx) - **Client Confidential** – In 2011, an equity trader managed to get access to back-office systems and run up unauthorized positions/ exposures and managed to keep them hidden which resulted in a xxxx loss for the Investment Company	- People – Fraud - Process- No SOD - System – Lack of IT security/SOD
2.	Mixing of Firm and Client Money	
	- **Client Confidential** – In 2010, the investment Company was found to be mixing its own money and client money with alarming regularity over a period of eight years. The company failed to segregate client cash in sterling money market deposits from its own funds for up to seven hours a day between December 1 2001 and December 29 2009. - **Client Confidential** –The regulatory body fined a client a record xxxx for infractions regarding client monies. Between 1st November 2002 and 8th July 2009, client failed to segregate the client money held by its futures and options business (F&O). Instead of being held overnight in a segregated money market account, F&O client money was held in an unsegregated account. This error remained undetected for nearly seven years.	- People – Internal Fraud - Process – Lack of control/ Monitoring
3.	Exceeding the Risk Limits	
	- **Client Confidential** – When analyzing risk management one can conclude that client's management countless times exceeded their own risk limits, ultimately exceeding their risk polices by margins of 70% as to commercial real estate and by 100% as to leverage loans. (Bankruptcy Report No.xxxxxx) - Besides exceeding their own risk limits they choose actively not to include their new business, real estate and leverage loans in their stress test simulations. (Bankruptcy Report No.xxxx) Consequently, client's management did not have a regular and systematic way of estimating the potential losses of these large and illiquid assets. They motivated this conduct by a false believe that these new business areas were small in comparison with their old ones and that the potential profits far exceeded the possible risks. This clearly demonstrates unnecessary high operational risk taking and could effectively been reduce by a more humble and professional mindset.	- People- Governance/ leadership failure to control limit breaches and maintain sanctity of stress testing - Process – Lack of inbuilt controls

Defining Ops Risk



Business Risks of a bank

Credit Risk

Credit Risk

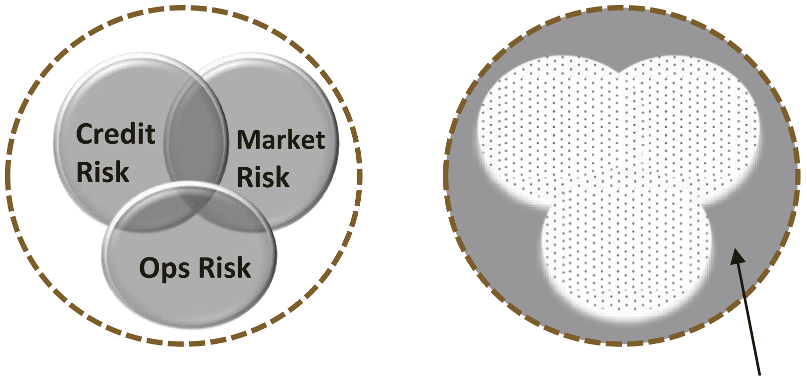
Market Risk

Operational Risks

Basel1 - 1988

Basel1 – 1995

Negative Definition : "All other risks that are not Credit or Market Risk are Operational Risk". Therefore, Residual Risk=Operational Risk



Credit Risk

Market Risk

Ops Risk

Basel II - 2004

Residual Risks
(e.g. Strategic or Reputational Risk)

Positive Definition : "Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk."

Exploring Ops Risk Definition

INTERNAL CAUSES

PEOPLE

- Internal Fraud
- Manual Error due to lack of skills
- Unauthorised access
- Errors due to maker checker not followed
- High workload due to lack of manpower
- Criminal Act-Burglary, Sexual Harassment etc.

PROCESS

- Lack of Policy & Procedure
- Lack of segregation of duty
- Improper project planning
- Incorrectly designed SOPs

SYSTEMS

- Use of unauthorised software
- IT security issues
- System downtimes
- Lack of access controls

EXTERNAL CAUSES

EXTERNAL EVENTS

- Natural calamities
- Riots & Arson
- Disruption in services such as power and water supply
- External fraud through rackets
- Government regulations and policy changes

LEGAL RISK

- Contract drafting errors
- Non collection relevant evidences
- Socio political effect on non enforcement of legal action

Ops Risk

ORM Lifecycle	Objective	Responsibility	Operational Risk Infrastructure	Frequency
Operational Risk Governance	To set ORM Strategy, Authority, Responsibility	To be approved by RMC	Operational Risk Policy & Procedure	Quarterly to Board and to CEO on a continuous basis
Risk Identification	To Identify the inherent risk in a process	ORM team in consultation with process owners	Risk Control Matrix (RCM)	• One time exercise • New process, product / system
Control Identification	To Identify the existing controls in processes	ORM team in consultation with process owners	Risk Control Matrix (RCM)	Introduction of new process, product or system
Risk Assessment	To classify risks as High, Medium & Low	ORM Team in consultation with respective departments	Risk Control Matrix (RCM)	Introduction of new process, product or system
Control Assessment	To assess control environment	ORM team with input from IA , CA, BA & RC	RCM and Control Assessment Dashboard	Quarterly
Risk Control & Mitigation	Update Policies & Procedures Develop/ Update KRIs	• Department/s with ORM • ORM team with Depts	Organisation Wide Policy & Procedure	Introduction of new process, product or system
Risk Monitoring & Reporting	To monitor & report KRIs, incidents, loss data & Actions	Monitoring- By Depts Consolidated reporting - ORM	KRIs, Incident & Loss Data Reporting, Action Plan Status	As per predefined frequency for departments & Quarterly in RMC

IA – Internal Audit, CA – Concurrent Audit, BA – Branch Audit, RC – Re-Credit

Current Scenario

Industry 4.0

Transformation

Digitalisation

Change is only constant

Automation

Big Data

Cloud Computing

Data Management

Internet

Smart Products

Data Analytics

Remote Workplace

Altered Business Models

What are Altered Business Models?

Business models continually evolve as companies react to changes large and small, and as they reposition to avoid emerging risks and seize opportunities. Over time, these accruing changes can transform everything about the business model – that is, how the business invests, how it earns and distributes its profits, and how it deploys its capital.

Banks are continuously looking for new ways to improve the client experience. Digitalization is not a choice for the banking industry; it is an unavoidable reality:

Digital Only

Bank facilities available exclusively via digital platforms like mobile, tablets, laptops, etc.

Platform Banking

A digital marketplace which offers banking services but is owned by another (potentially nonbank) entity

Unbundling Traditional Products

Re-bundling of Micro-products and services to provide better consumer propositions

Non-linear Model

Easier product componentization and value chain fragmentation

Altered Business Models

Why

Causes of Altered Business Models

Defects in Original Model

the original business model may be flawed, and changes may be made to it for the company to generate momentum.

Change in Value Proposition

Value proposition describes the collective benefits customers receive from using a product or service.

New Revenue Opportunities

The business model is modified and expanded to include the new revenue opportunities as they emerge

Change in Competitive Environment

When an old model puts a company in an unfavourable competitive position, it is changed.

Some of the emerging digital banking solutions in India:

811 kotak Kotak Mahindra Bank

payzello

Gimi

AXIS ASAP SAVINGS ACCOUNT IN 3 STEPS

yono SBI

Razorpay

Paytm

digibank

Altered Business Models

How

Digital disruptions are challenging the traditional role of banks

Banking is undergoing a significant change and all current business models are under scrutiny. Digitization is the most significant of several universal trends and disruptive new entrants may fundamentally change the competitive environment.

1. Payments

2. Deposits & lending

3. Investment management

4. Market provisioning

5. Ease of Capital raising

Decentralized currencies leverage Blockchain technology and mobile money solutions provide compelling alternatives to traditional value transferring systems by streamlining intermediation processes.

Alternative lending platforms leveraging peer-to-peer models are transforming credit evaluation and sourcing of capital, as well as, narrowing the spread between deposits and lending.

A number of disruptors, from automated wealth management services to social trading platforms, have emerged to provide low-cost, sophisticated alternatives to traditional wealth managers.

The development of smarter, faster machines in the field of algo trading, which are learning to process unstructured information will have unpredictable implications on market provisioning in terms of volume, volatility and spread.

In light of the growing interest in startups and digital democratization, alternative funding platforms have emerged, widening access to sources of capital and providing funding to a greater number of companies and projects.

Altered Business Models

Opportunities

Fintech innovations hold potential benefits for all users of financial services. The risks associated with fintech vary significantly across the different scenarios, the identified opportunities will depend less on particular scenarios and more on the technologies that will allow them to be realised. Some important opportunities to consider include:

01

Financial inclusion

Digital finance has improved access to financial services by under-served groups. Technology can reach remote locations.

02

Better and more tailored banking services

Fintech companies could help the banking industry improve their traditional offerings and increase the efficiency of incumbent businesses.

03

Lower transaction costs and faster banking services

Innovations from fintech players may speed up transfers and payments and cut their costs.

04

Improved and more efficient banking processes

Innovation may allow the conduct of operations in a safer environment thanks to the use of cryptographic or biometric technologies.

05

Positive impact on financial stability due to increased competition.

The entry of new players competing with incumbent banks could eventually fragment the banking services market and reduce the systemic risk

06

Regtech

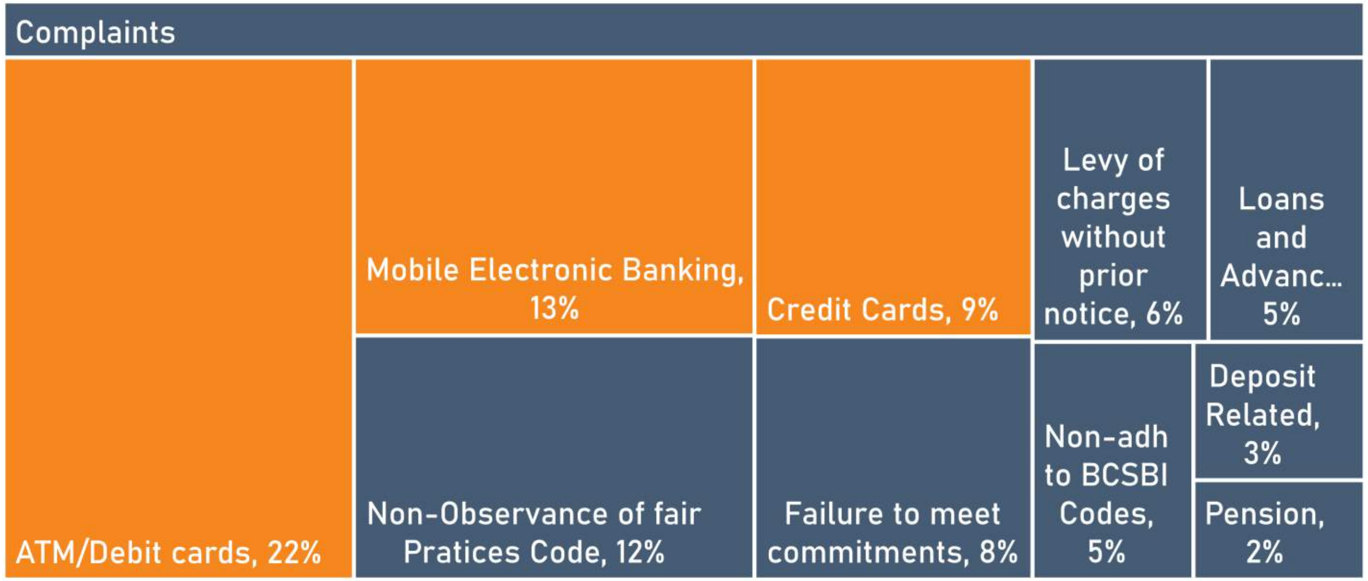
Fintech could be used to improve compliance processes at financial institutions. Ex-automate regulatory reporting and compliance requirements

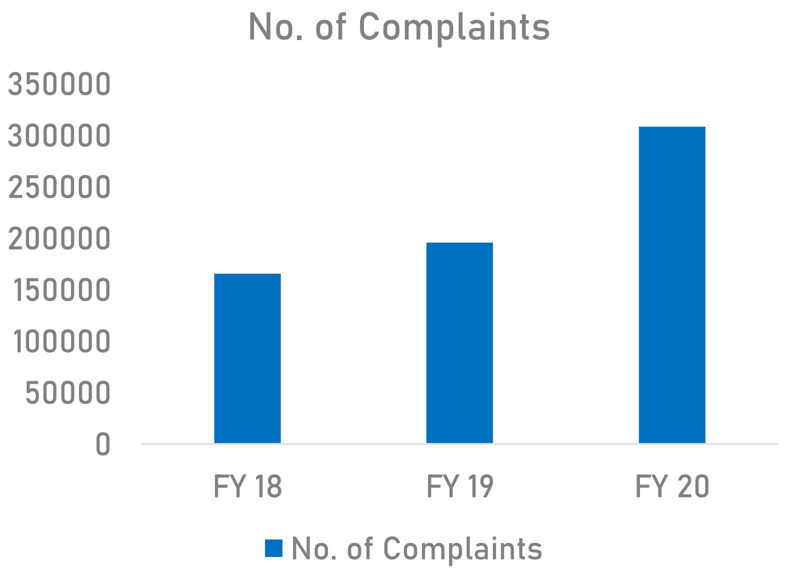
ORM: Current Scenario

Indicators of Operational Risk Levels continue to rise

Banks/Fintech have made good progress in ORM, managing operational risk remains intrinsically difficult, for a number of reasons.

1. Compared with financial risk such as credit or market risk, operational risk is more complex, involving dozens of diverse risk types.
2. Operational risk management requires oversight and transparency of almost all organizational processes and business activities.
3. The distinguishing definitions of the roles of the operational-risk function and other oversight groups—especially compliance, financial crime, cyberrisk, and IT risk are not defined completely.





Over 3 lakh complaints were made against banks to the RBI's banking ombudsman in FY20, over 50% more than in FY19.

About 45% of complaints in FY20 were related to digital services such as ATM/debit/credit cards and mobile/electronic transactions.

Source: RBI Annual Report On Ombudsman Schemes

Key Challenges in ORM

Operational Risk Professionals will likely face these key challenges:

1 Inefficient risk identification

- The current KRIs, KCIs, and KPIs used for ORM reporting in most banks are inefficient and do not provide a holistic data view, leading to incorrect risk identification. These KRIs are assessed in silos and a correlation among them is not quantified. Further, there is inconsistent risk measurement across business lines.

2 Large data processing

- For ORM, the number of transactions that need to be monitored is growing at an exponential rate. This directly puts pressure on the current banking infrastructure and the existing processing logic is unable to handle the steep increase.

3 Absence of Risk Datamart

- The biggest challenge in ORM is the lack of centralized and synchronized data. This can be further attributed to challenges around risk data aggregation. Most banks have incomplete coverage of data sources across business lines and hence, are unable to extract the full potential of huge data warehouses

4 Embedding new technology

- Firms with fragmented operational risk infrastructures found it difficult to respond quickly and with agility during the pandemic crisis, and it showed on the shortcomings of financial institutions' current systems and processes.

Evolving Risk Landscape- (1/3)

The digital transformation in banking, presents many challenges, with several operational risks related to downtime and timeout services due to system failures.

1 **Online Hacking-** Online hacking and malware attacks became prominent in the past some time. SWIFT systems are used by almost all the banks to exchange vital financial information more securely. However, the recent cyberattack on one of the SWIFT infrastructure indicated the level sophistication of the hackers. The banks and financial institutions have vulnerabilities in their processes, and the hackers take advantage of these vulnerabilities to launch malware attacks.

2 **Application Security Risk-** Fintech applications are used by many banks to access the real-time financial information of their customers. But, if a software application does not have full-proof security modules and efficient codes, then it automatically becomes prone to cyber crimes. The attackers leverage the weak security of the apps to steal the customer data.

Five IT failures in 2021

Date	Outage	Business line	Country
Mar-21	Mizuho Bank data glitch, which closed about 80% of the bank's cash machines and lasted over 24 hours, originated from a failed data migration.	Retail banking	Japan
May-21	Santander customers in Scotland experienced difficulty carrying out online and in-store card payment and were unable to use cash machines and online banking.	Retail banking	UK
Sep-21	BBVA México system failure left more than 20 million users without access to cash machines and mobile app.	Retail banking	Mexico
Oct-21	The Hong Kong Monetary Authority experienced business disruption after its Faster Payment System crashed and real-time fund transfers and registration of account proxy were unavailable for approximately five hours.	Retail banking	Hong Kong
Nov-21	DBS Bank Singapore customers experienced a three-day outage, unable to access the bank's digital services.	Retail banking	Singapore

Evolving Risk Landscape- (2/3)

3 **Money Laundering Risk-** Money laundering has become one of the prominent issues of today's world. Fintech-driven banks often use cryptocurrency that are not formally regulated by any set of standards and global regulations. Hence, the frequent use of non-regulated currencies results in illegal money laundering and even in terrorist funding, as identifying the beneficiary in any fintech-enabled transactions is not possible due to fintech's pseudonymous nature.

4 **New Encryption Technology-**With disruptive technologies, the overall performance of the finance sector drastically improved. Blockchain, one of the disruptive technologies, gave birth to some serious security concerns. Firstly, blockchain can be hacked by attackers like any other platform very efficiently. Secondly, blockchain transactions are based on trust between two or more parties. Many people use bitcoin in exchanges and trust that the exchange firms will look after that, but it does not happen quite often.

Top Five publicly reported fraud losses 2021

S.N.	Firm	Loss Amount (US$)	Business line	Description
1	Envy Group	1.23 billion	Asset management	Defrauded of $1.23 billion by former director, involving fake nickel deals and forged contracts.
2	Westpac	255 million	Commercial banking	Exposed to A$341 million loss through Forum Finance leasing invoice fraud.
3	Sberbank	108.2 million	Commercial banking	Defrauded of 8 billion rubles through commercial loans to supermarket chain.
4	Sumitomo Mitsui	73.9 million	Commercial banking	Exposed to A$98.9 million loss through Forum Finance leasing invoice fraud.
5	Mercuria	36 million	Commercial banking	Defrauded of $36 million after purchasing warrants for copper replaced with painted paving stones.

Source: ORX News

Evolving Risk Landscape- (3/3)

5 **Digital Identity Risks-** With the introduction of digital tools in the banking and finance industry, the use of mobile-based services that used one-time passwords and security codes increased drastically. These security codes and passwords could be easily accessed due to the faulty fintech system provided by some of the fintech service providers. Hence, financial institutions need to revisit their online security architecture to address these risk factors before planning for fintech implementation.

6 **Cloud-based Security Risks-** Cloud-based solutions are one of the significant aspects of the fintech industry in terms of data security. But, even though the cloud-based services offer secure data storage, lack of adequate security measures can result in the corruption of your sensitive financial information. There are instances when the company partners with an inefficient cloud-based solution provider and then deals with significant data losses. Therefore, stay updated and be wise while selecting your cloud-based service partner.

Five publicly reported Data breaches in India

Date	Firm	Description
Apr-21	Upstox	Indian trading platform Upstox acknowledged a breach of know-your-customer (KYC) data.
Jan-21	Juspay	Details of close to 35 million customer accounts, including masked card data and card fingerprints, were taken from a server using an unrecycled access key.
Jan-19	SBI	SBI data breach leaks account details of millions of customers.
Mar-21	Mobikwik	Mobile phone number, bank account details, email, and even credit card numbers of 9.9 crore Mobikwik users was leaked online.
Apr-21	Moneycontrol	Moneycontrol Data leaks personal data of more than seven lakh users. The data was available on the dark web, for sale at US$350.

Next Gen ORM – (1/4)

1. Develop New Frameworks

New frameworks are needed to properly evaluate the resiliency of business processes, challenge business management as appropriate. These frameworks should support the following types of actions:

1. Mapping the processes, along with associated risks and controls, including overall complexity, number of handoffs involved, and automation versus reliance on manual activities.
2. Identify and understand the points where processes rely on technology.
3. Monitor risks and controls. Create mechanisms to monitor the risk levels and control effectiveness, in real time wherever possible.
4. Link resource planning to the understanding of processes and associated needs. How are we prepared for the increased volumes and are able to manage the downtimes.
5. Training. Reinforce needed behaviour using communications, training, performance management, and incentives.
6. Enable feedback. Establish feedback mechanisms for flagging potential issues, undertaking root-cause analysis, and updating or revising processes as needed to address the causes.
7. Establish change management. Establish systematic, ongoing change management to ensure the right talent is in place, test processes and capacity, and provide guidance, particularly for technology.

Next Gen ORM – (2/4)

2. Use Advanced Analytics

Advanced analytics has applications in all areas of operational risk. It is creating significant improvements in detecting operational risks, revealing risks more quickly, and reducing false positives. Some applications are described below:

Anti-money laundering
Replacing rules-driven alerts with machine-learning models can reduce false positives and focus resources on cases that actually require investigation.

Conduct
Analytics engines can identify suspicious sales patterns, connecting the dots across sales, product usage, incentives, and customer complaints

Cyberrisk
Machine learning can analyze sources of signals, identify emerging threats, replace existing rules-based triggers, and reduce false-positive alerts.

Fraud
Machine learning, including unsupervised techniques, can identify fraudulent transactions and reduce false positives;

Process quality and regulatory risks
Automated call surveillance using natural-language processing can monitor adherence to disclosure requirements.

Third-party risk
Models can be developed that quantify the reliance on key third parties to drive better business-continuity planning

Next Gen ORM – (3/4)

3. Develop Specialized talent

A range of emerging risks, all of which fall under the operational-risk umbrella, present new challenges for banks. To manage these risks—in areas such as technology, data, and financial crime—banks need specialized knowledge

Cyber risk

1

Expertise needed:

- Pathways to vulnerability
- The bank's most valuable assets
- Sources of exposure for a given organization

Talent profiles:

- Cybersecurity background
- Senior status to engage the business and technology organizations

Fraud

2

Expertise needed:

- Fraud patterns (for instance, dark web)
- Technology and cybersecurity
- Interdependencies across fraud, IT, and business-product decisions

Talent profiles:

- Former senior technology managers
- Cybersecurity professionals, ideally with an analytics background

Conduct

3

Expertise needed:

- Ways employees can game the system in each business unit (for instance, retail, wealth)
- Specific patterns, such as how traders could harm client interests for their own gain

Talent profiles:

- Former branch managers and supervisors
- Former traders and back-office managers
- First-line risk managers with experience in investigating conduct issues

With specialized talent in place, banks/FIs will then need to integrate the people and work of the operational-risk function as never before. To meet the challenge, organizations have to prepare leaders, business staff, and specialist teams to think and work in new ways. The overall objective is to create an operational-risk function that embraces agile development, data exploration, and interdisciplinary teamwork.

Next Gen ORM – (4/4)

4. Human Factor Risk

These risks are linked with culture, personal motives, and incentives than with the operational processes and infrastructure. They are difficult to quantify, prioritize in large organizations.

First step is to identify functions / group which presents highest human-factor risks, including misconduct, mistakes with heavy regulatory or business consequences, and internal fraud.

The next step is to design monitoring, oversight, role modeling, and tone setting for each of such functions. In addition; training, consequence management, a modified incentive structure, and contingency planning for critical employees are tools for managing human factor risk.

Automating your operations processes is the most *efficient* and most *reliable* way to reduce operational risk. That's because, no matter what the external risk or circumstances present, your operations teams are prepared to take the right steps every time – automatically.

Evaluate the processes along two dimensions:

1. Automation Maturity–
When your team handles a given operational situation, how many steps of the process are coordinated in an ad hoc, manual way, using – for example – email or phone calls? Processes ranking higher in this dimension will be more prone to error and more resource-intensive.

2. Business Criticality–
Essentially, how "life or death" is this process to the continuity of your business? Will you lose customers? Reputation? Money? Processes ranking higher in this dimension will be the ones that require the most timely and well-coordinated responses.

Based on this evaluation create a ranked prioritization list of the tasks to be automated.

Automating fintech operations is not handing the job over to robots. Rather, when you automate the coordination and management of your most risk-intensive processes, you remove several, hefty burdens from your operations teams:

- They no longer have to "figure it out"
- They no longer need to organize their response
- They no longer have to waste time on coordination
- They no longer need approval

Face the Future with Confidence