Recent trends and best practices in operational risk management

Cyprus Economic Society
Dr. Ariane Chapelle
November 28, 2018
Topics

1. Definition and Scope of Operational Risk
2. Frameworks and Tools
3. Partners and Decision-Making
4. Governance and Culture
5. Maturity Criteria and Risk Management Trends
Operational Risk

.. is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. (Basel II, Solvency II)
Risk Events (in just one day)

TSB ROCKED BY FRAUD ATTACKS

JASPER JOLLY

Under fire high street bank TSB has been hit by more than 10,600 alerts of potential fraud since its computer systems went down at the end of April, MPs heard yesterday.

The bank’s chief executive Paul Pester faced stinging criticism from MPs and the banking ombudsman as he appeared before the Treasury Select Committee.

TSB has experienced more than 1,200 confirmed fraud episodes with more than 1,300 customers having money stolen. TSB has promised to compensate customers who are left out of pocket in any way.

Pester said the bank had been hit by an “unprecedented attack on US banking from organised crime”, with fraud attacks 70 times higher than normal. More than 12,900 TSB customers have switched current accounts to competitors.

Data firm was victim of media storm, boss says

Credit Suisse agrees to pay US $47m over Asia hiring practices

REBECCA SMITH

Credit Suisse will pay $47m (£35m) to the US Department of Justice over hiring practices in Asia, the bank confirmed yesterday.

The Swiss bank is paying the penalty to resolve a probe into hiring practices in Asia between 2007 and 2013, after it was announced in February that US authorities were investigating whether Credit Suisse had hired referrals from government agencies in Asia in return for business and regulatory green lights.

Credit Suisse said no criminal charges have been brought and the $47m has been “substantially provided” for in prior periods.

A GIANT blaze engulfed the top floors of the Mandarin Hotel in Knightsbridge yesterday. Plumes of smoke were seen billowing from the hotel’s rooftop. The London Fire Brigade said 15 fire engines and more than 100 firefighters were called to the scene. There were no reports of any injuries.

The fire is thought to have spread to multiple floors across a “vertical facade” containing plants.
Facebook comes under fire over data sharing deals with Chinese tech firms

It was revealed earlier in the week that Facebook reached at least 60 deals with Chinese device makers over the last decade, giving firms access to some users’ data for the purpose of building on “the Facebook experience” with features like address books and messaging.

Facebook denied allegations that any of these deals conflicted with its founder Mark Zuckerberg’s earlier testimony to US Congress, nor did they represent a new data breach.

A Facebook vice president said that all integrations with Chinese device makers were “controlled from the get go” with all features built and being approved by the company itself. He added that at no point was any data stored on company servers.

The US Senate commerce committee has written to Facebook asking for further clarification.

www.chapelleconsulting.com
## Top 10 risks in 2018

<table>
<thead>
<tr>
<th>Risk</th>
<th>2018 position</th>
<th>2017 position</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT disruption</td>
<td>1</td>
<td>1*</td>
<td>➡️</td>
</tr>
<tr>
<td>Data compromise</td>
<td>2</td>
<td>1*</td>
<td>➡️</td>
</tr>
<tr>
<td>Regulatory risk</td>
<td>3</td>
<td>2</td>
<td>➣</td>
</tr>
<tr>
<td>Theft and fraud</td>
<td>4</td>
<td>9</td>
<td>➤</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>5</td>
<td>3</td>
<td>➣</td>
</tr>
<tr>
<td>Mis-selling</td>
<td>6</td>
<td>5*</td>
<td>➣</td>
</tr>
<tr>
<td>Talent risk</td>
<td>7</td>
<td>new</td>
<td></td>
</tr>
<tr>
<td>Organisational change</td>
<td>8</td>
<td>6</td>
<td>➣</td>
</tr>
<tr>
<td>Unauthorised trading</td>
<td>9</td>
<td>5*</td>
<td>➣</td>
</tr>
<tr>
<td>Model risk</td>
<td>10</td>
<td>-</td>
<td>➤</td>
</tr>
</tbody>
</table>

Source: Risk.net, Feb 22, 2018
## ORM Strengths and Weaknesses: CRO survey 2017

Table 1: Frequently cited strengths and weaknesses in operational risk management

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk-neutral framework</td>
<td>Sub-optimal management information</td>
</tr>
<tr>
<td>Well-developed set of standard and mature tools</td>
<td>Minimal integration of advanced analytics</td>
</tr>
<tr>
<td>Good visibility of major risks</td>
<td>Ineffective and inefficient controls</td>
</tr>
<tr>
<td>Strong senior management mandate</td>
<td>Risk culture not sufficiently embedded</td>
</tr>
<tr>
<td></td>
<td>Lack of business and specialist skills</td>
</tr>
</tbody>
</table>

Framework and Tools
Risk is the effect of uncertainty on objectives
Risk Management Process

Exposure/Causes, due to:
• Strategy
• Environment

Risks
• Turning into incidents when materialized

Impacts
• Financial, Non financial

Controls

Incident management
## Risks Identification tool: Exposures and Vulnerabilities

<table>
<thead>
<tr>
<th>Exposures</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Key distribution channels</td>
<td>• Weakest links</td>
</tr>
<tr>
<td>• Main clients</td>
<td>• Fragile systems</td>
</tr>
<tr>
<td>• Main suppliers and third parties</td>
<td>• Revenue channels at risk</td>
</tr>
<tr>
<td>• Critical systems</td>
<td>• Systems or processes not integrated</td>
</tr>
<tr>
<td>• Regulatory exposure</td>
<td>• Parts of the business resistant to risk management</td>
</tr>
<tr>
<td>• Main drivers of revenues, drivers of value</td>
<td>• Small, unmonitored operations or people</td>
</tr>
<tr>
<td>• Brand value</td>
<td>• Unmaintained systems</td>
</tr>
<tr>
<td>• ...</td>
<td>• BCP due for testing or updates</td>
</tr>
</tbody>
</table>
Some key messages

1. Make your own personal list of key risks
2. An institution’s risk profile is personal, related to its exposures and vulnerabilities
3. Don’t neglect risks that haven’t materialised yet
4. Focus and prepare for large events… just in case
5. Watch the trends, but don’t forget blind spots
ORM tools and best practices in a nutshell

- **RCSA**: updated when needed (yearly or trigger event) and back-tested with loss experience and in line with risk appetite
- **KRI**s – **Key Risks Indicators**: leading, preventative
- **Scenario analysis**: to guide risk management actions and priorities
- **Risk reporting and root cause analysis**: effective, helping decision-making
Connectivity for management priorities: a network view of the top risks - 2017

#1 Cyber risk and data security
#3 Outsourcing
#5 Conduct risk
#6 Organisational change
#10 Physical attack
#9 Fraud

#2 Regulation
#8 AML, CTF and sanctions compliance
#7 IT failure

Partners and Decision-Making
Drivers of Operational Excellence: PPSE

<table>
<thead>
<tr>
<th>People</th>
<th>Process</th>
<th>Systems</th>
<th>External Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resourcing</td>
<td>Automated</td>
<td>Integration</td>
<td>External fraud and threats monitoring</td>
</tr>
<tr>
<td>Ability</td>
<td>Integrated</td>
<td>Capacity</td>
<td>Cyber crime protection</td>
</tr>
<tr>
<td>Engagement</td>
<td>Standardised</td>
<td>Performance</td>
<td>Legal &amp; Regulatory monitoring</td>
</tr>
<tr>
<td>Retention</td>
<td>Documented</td>
<td>Maintenance</td>
<td>Technological veil</td>
</tr>
</tbody>
</table>

Prioritising risk management for better decision-making

- **Likelihood**
  - Costs (of doing business)
  - Ignore
  - Monitor (Scenarios)
  - Fatal flaws

- **Impact**

---

www.chapelleconsulting.com
## Risk and Opportunity – Typology of decisions

<table>
<thead>
<tr>
<th>Type</th>
<th>Characteristics</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silly risky decisions</td>
<td>Large downside, no upside, small cost of control</td>
<td>Not buckling a car seat belt, not locking a work station</td>
</tr>
<tr>
<td>Violating decisions</td>
<td>Attractiveness of large personal upside (profit) or fear of a large personal downside (sanction, lay-off) conducing to break a rule</td>
<td>Rogue trading, compliance breaches, conduct violations, misstatements of accounts</td>
</tr>
<tr>
<td>Chilly decisions</td>
<td>Fear-driven, excessive protection destroying the likelihood and value of the initial upside</td>
<td>Redundant controls on non critical processes, more financial, human and technical resources dedicated to the controls than to the operations, more controls layers than execution layers, “quality assurance of quality assurance” (sic)</td>
</tr>
<tr>
<td>Balanced decisions</td>
<td>Striking an accepted trade-off between risks and expected rewards, balancing the prospects of upside with the eventuality of downside.</td>
<td>All thought-trough investments decisions, commercial initiatives, entrepreneurial projects, where risk is accepted if fairly compensated by expected returns.</td>
</tr>
</tbody>
</table>

Governance and Culture
Three lines of defense model

First line: business operations / risks owners
- Front line of risk management
- Real line of risk management
- Risk is managed where it is generated

Second line: risk management
- Methodology unit and coordination
- Oversight and harmonisation of practice
- Advice and support
- Challenge if need be

Third line: internal audit
- Independent review and assurance
How to embed a risk culture?

- **Tone Done at the top**
  - “People do what you **do**, not what you **say**” -> lead by example

- **Tune in the middle**
  - “Tell people what to **do**, not only what the objectives are -> focus on **key behaviours**

- **Part of the processes**
  - OpRisk is about PPSE
  - People – Process - Systems
  - External Events
  -> focus on fundamentals
Risk Buy in - The role of the Risk Function

Building an *Invisible Framework*, for risk management it is:

- Adjusting to the business
- Accounting for existing practices and leverage them
- Avoiding jargon outside of the risk management specialists
- Solving problems
- Enabling business to grow safely
- Providing technical support
- Making friends

Maturity Criteria & Risk Management Trends
Framework Maturity Criteria

1. Incident Data Base is comprehensive.
2. Risk reporting is fed from and back to business lines with benchmarks and comparisons across similar entities.
3. Risk assessments are consistent and comparable across business lines.
4. Action plans and mitigating actions are based on risk assessment, not just in response to incidents. They are linked to risk appetite.
5. Results of scenarios identification and assessments are used to improve management decisions.
6. KRIIs are preventative, relevant and actively used.
7. Executive directors understand the concept of risk appetite to agree on limits of exposure and necessary controls.
8. Risk management culture is valued throughout the organisation.

Evolutions of Risk Management

Resilience focus
- Better incident management
- Crisis management pre-planning

Control assessment and testing
- Observability of controls
- Optimisation of processes

Behavioural economics
- Culture and Conduct through behaviour drivers
- Desirable versus unacceptable behaviours

Positive risk management
- Recognise the rewards when taking risk
- Recognise the value of risk management
- Positioning risk management as an enabler of performance
To know more
From December 2018

Operational Risk Management: Best Practices in the Financial Services Industry

ARIANE CHAPELLE

Operational Risk Management: Best Practices in the Financial Services Industry provides a comprehensive overview of the most up to date methods and practices in operational risk management applied in financial services firms.

Coverage includes:

- Risk Identification: tools, scenario analysis, risk register and taxonomy, risk connectivity, and risk networks
- Risk Assessment: risk appetite, risk and control self-assessment, scenario analysis, regulatory capital and modelling
- Risk Mitigation: operational risk governance, controls, transfers and prevention by design, root cause analysis and action plans, conduct, and culture
- Risk Monitoring: incident data collection, key indicators, risk reporting, and the value of risk management
- Advanced tools and techniques developed by the most mature firms in operational risk management.

Order your copy from wiley.com
Since 2017

Reflections on Operational Risk Management

28 articles around 6 themes

1. Essentials of Operational Risk and Risk Management Framework
2. Risk appetite and Risk decisions
3. Key Risk Indicators and reporting
4. Culture and Conduct
5. Scenario Analysis and tail risks
6. Operational risk capital & measurement
Thank you for your attention

Any question or comments:
ariane@chapelleconsulting.com

Need for more resources:
www.chapelleconsulting.com