RiskSpotlight

Operational Risks associated with COVID-19 pandemic - Updated on 24Mar2020

Authored by Manoj Kulwal, Co-Founder & CRO at RiskSpotlight

Link to the article on LinkedIn - https://www.linkedin.com/pulse/operational-risks-associated-covid-19-pandemic-updated-manoj-kulwal

This article highlights the specific operational risks financial services firms need to manage in relation to the COVID-19 pandemic. Due to the evolving nature of this topic, the article will be regularly updated and the date stamp in the title will reflect the last update. So please do visit the article frequently if you are interested in updates on this topic.

Health & Safety + Employment Practices

HS1. Illness or death of employees due to COVID-19 infection in the work environment: firms will have a high level of influence on managing this risk and hence should be able to implement adequate level of controls to manage this risk

HS2. Illness or death of employees due to COVID-19 infection outside the work environment: firms will not have the same level of influence on mitigating this risk as Risk 1 and hence the level of controls it can implement will be limited but firms will need to consider and implement specific controls to manage this risk

HS3. Illness or death of external stakeholders (e.g. customers, vendor staff) due to COVID-19 infection in the work environment (e.g. customers coming to branch get infected OR vendor staff working in the firm's business office get infected)

HS4. Employees suffering from mental illness issues due to multiple issues such as working from home for long periods, being fearful of their and their family's health, being fearful of their employment status with the firm in the near future and being fearful of running out of food supplies

HS5. Harassment or discrimination of certain employees due to their association with certain COVID-19 related factors (e.g. harassment or discrimination of employees based in China or Italy, unfairly excluding certain employees from key business meetings and decisions)

Business Process Execution Failures - Customer Processes

PC1. Disruption to customer related business processes due to inadequate resource availability (e.g. delays in handling customer enquiries due to 50% reduction in availability of call centre staff)

PC2. Disruption to customer related business processes due to third parties being unable to fulfil their obligations (e.g. delays in processing loans due to third parties

not being able to complete the necessary KYC checks). This should also include the risk of potential bankruptcy of key third parties.

PC3. Disruption to customer related business processes due to excess levels of demand for certain services (e.g. disruption to a trading system due to very high volumes of buy or sell orders placed by customers in a short time window, large number of customers requesting increase in overdraft limits)

PC4. Delays in implementing processes/products/services to implement the government policies and measures in response to COVID-19 (e.g. handling customer requests for implementing mortgage holidays)

PC5. Poor quality deliverables delivered from processes/products/services implemented in response to government policies and measures in response to COVID-19 (e.g. inconsistent advice given to customers requesting mortgage holidays)

Business Process Execution Failures - Internal Processes

PE1. Disruption to internal business processes due to inadequate resource availability (e.g. delays in processing monthly payroll due to 50% reduction in availability of payroll processing team)

PE2. Disruption to internal business processes due to third parties being unable to fulfil their obligations (e.g. delays in processing monthly payroll where the payroll process is outsourced to a third party). This should also include the risk of potential bankruptcy of key third parties.

PE3. Disruption to internal business processes due to excess levels of demand for certain services (e.g. hundreds of employees requesting access to certain software to enable them to work from home, large number of employees asking questions on whether next payroll will be processed on time to enable them to make their personal mortgage/loan payments)

Technology Failures & Damages

TF1. Failure of IT equipment utilised by employees to work from home due to excessive usage/inappropriate usage/accidents

TF2. Unplanned outages of key IT systems due to delays in performing planned maintenance because of resource constraints

TF3. Unplanned outages of key IT systems due to breakdown of critical infrastructure such as internet and electricity

RiskSpotlight

External Theft & Fraud + Cyber Risks

EC1. Employees targeted with phishing attacks by cyber criminals who are utilising the pandemic to launch phishing attacks

EC2. Customers targeted with phishing attacks by cyber criminals who are utilising the pandemic to launch phishing attacks

EC3. Theft of information by cyber criminals from employee computers utilised to work from home if the level of security on these computers is lower than the level of security implemented in the workplace

EC4. Theft of information from key IT systems by cyber criminals due to lack of adequate monitoring/patching resulting from resource constraints

EC5. Criminals utilising financial services for money laundering to take advantage of the resources constraints faced by financial services firms with the hope that the level of scrutiny on financial transactions will be lower than usual

Improper Business Practices (Conduct Risks)

IB1. Changes to terms and conditions of products and services that may be considered unfair by customers and regulators (e.g. increase in fees to cover the cost of extra staff deployed to offer a service)

IB2. Termination of customer relationships that may be considered unfair by customers and regulators (e.g. cancelling mortgages of customers unable to pay their mortgage due to COVID-19 related circumstances)

IB3. Harassment or discrimination of certain customers due to their perceived association with certain COVID-19 related factors (e.g. harassment or discrimination of customers with Chinese origin)

Internal Theft & Fraud

IF1. Fraud, theft or embezzlement by employees facing financial hardship due to COVID-19 related circumstances

IF2. Financial statement fraud by senior executives who may want to hide financial impacts of the crisis from key stakeholders because of the resulting impact on their personal compensation and incentives

Damage to Physical Assets

DA1. Damage to physical assets due to lack of adequate maintenance resulting from inadequate resource availability (e.g. unclean offices due to lack of cleaning

staff, breakdown of vehicles used to transport cash to ATM machines + branches due to lack of maintenance)

I have added an identifier for each of the above risks so you can utilise these to discuss specific risks with other operational risk practitioners in the comments section.

What additional COVID-19 related operational risks are you managing in your firm that are not covered in the above list? Based on your feedback I will update the above list to ensure all operational risk practitioners globally have access to the updated set of COVID-19 related operational risks.

Which of the above risks are most difficult to manage in your firm at the moment? COVID-19 will require firms to collaborate on global level in terms of understanding the risks and their impacts + identify effective risk responses. Please utilise the comments section below to share your thoughts and ideas on this topic. Based on the level of responses to this article - my team is also ready to organise online sessions to discuss these topics and share the recording of these sessions with the global operational risk management community.

If you want to monitor daily updates of news articles related to the above risks then please register for a 2 months free trial of RiskSpotlight Portal from here - https://www.riskspotlight.com/portaltrial/