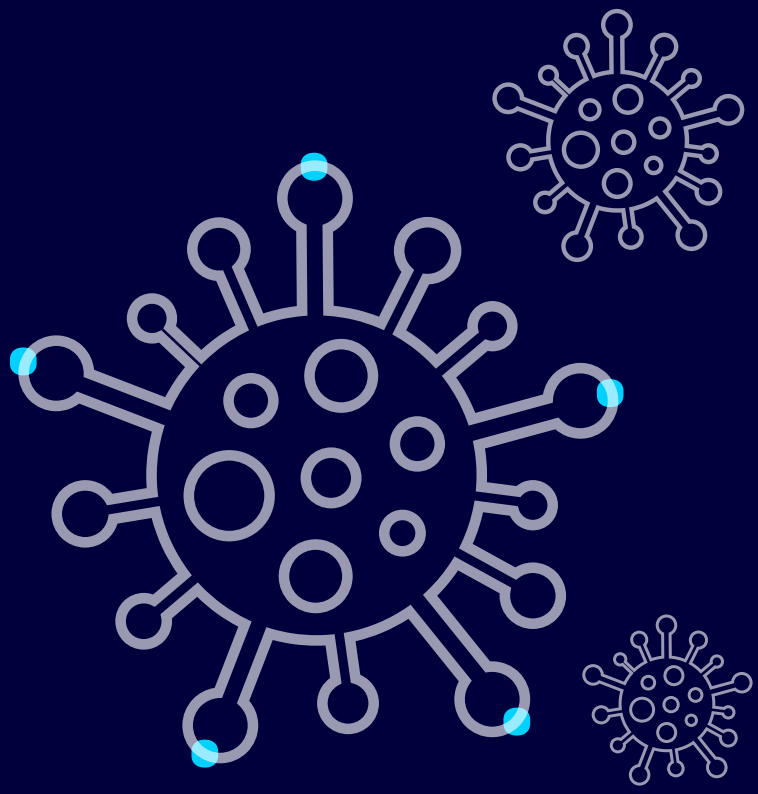
O.R.X

Covid Risk Review

The risks of the crisis

Summary report: June 2020



Material risks in focus

Topics covered:

- **Coronavirus (Covid-19)**
- **Business continuity**
- **Information security & cyber**
- **People**
- **Third party**
- **Fraud**
- **Conduct**

Free coronavirus-related resources from ORX

Since the outbreak of pandemic, ORX has been producing coronavirus-related resources to support our membership and the wider operational risk industry. This includes research, news round-ups, discussion summaries, videos and more.

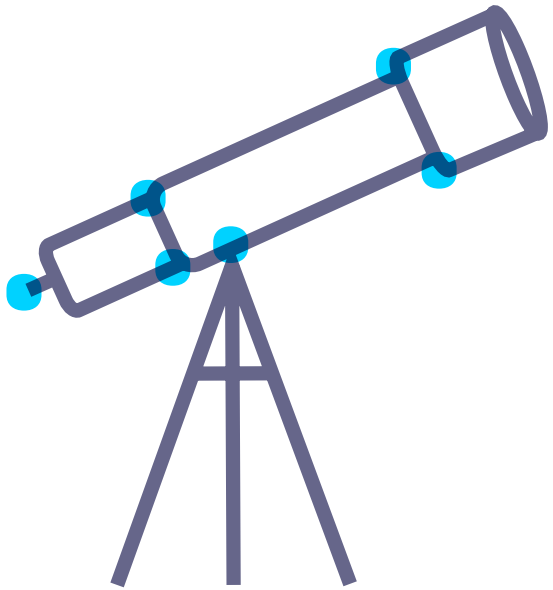
Explore the resources and see how ORX can support you during this crisis on our website:
managingrisktogether.orx.org/coronavirus

Executive summary

Since the outbreak of coronavirus in early 2020, ORX has hosted weekly meetings that enable our membership to discuss the impact of the coronavirus (Covid-19) pandemic and understand how the industry is responding. From these discussions, it soon became clear that the pandemic had caused a rapid change to – and ongoing evolution of – operational risk profiles.

To help the industry understand this further, we launched the Covid Risk Review to survey how individuals from across our global membership view the current operational risks facing the industry.

Information on how the survey results were collected and analysed can be found on page 8 of this report.



Key findings

Coronavirus has significantly changed operational risk profiles

When compared with the results of the ORX Operational Risk Horizon 2020 study (published in February 2020), it is clear that over a short period of time the overall operational risk profile of the industry has changed significantly:

- Business continuity was ranked the most significant risk and a significant driver, up from 11th place in the Horizon 2020 report. This highlights the nature of the current situation and strengthens the need for the existing regulatory focus on operational resiliency.
- Organisations' reliance on third parties for critical processes and services has been exposed, as the third parties' operational and financial resilience is brought into question.
- People cut across the risk profile as both a risk and a driver of risks, rising from 12th place in the Horizon 2020 report to being the 4th most significant current risk.
- The current climate is creating the potential for increased fraud, driven by a combination of factors including control environments adjusted for home working, the economic downturn and cybercriminals exploiting fears around the pandemic.
- Many of the top risks are interconnected, with changes driven by several key factors, including people, organisational and third party resilience, and macroeconomic factors.
- Regardless of the specific risk, the vast majority of responses reported an overall increase in risk exposure levels.

The risks or the consequences of the crisis?

It will be interesting to see whether the views expressed in this survey change as the pandemic plays out and the industry moves towards the new normal.

Does the picture presented reflect the risks of the crisis as opposed to the risks that may rise in importance as a consequence of it? Will we see a surge in conduct risk as a result of organisations having to deliver government-led products quickly or reduce staff supervision when managing customers? Will internal fraud increase due to control environment and process changes?

To monitor this, ORX will re-run this survey on a periodic basis over the remainder of 2020.

The ORX Operational Risk Horizon Study

Knowing which operational risks you need to be most aware of is one of the big challenges risk managers face. To help you with this, we survey our membership annually to see which operational risks they think will be top of the agenda for the coming year. We also ask them which risks they think will be the key emerging risks over the next three years.

Find out more and download the 2020 report:
managingrisktogether.orx.org/research/operational-risk-horizon-2020

Top operational risks facing the industry

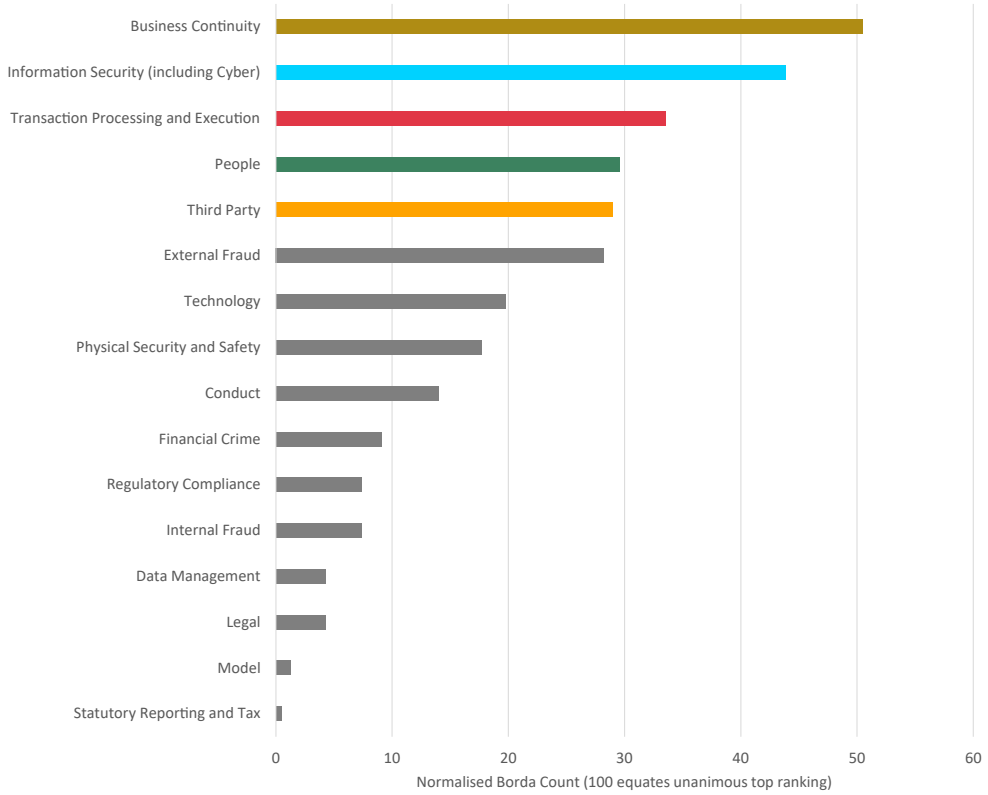
Overview

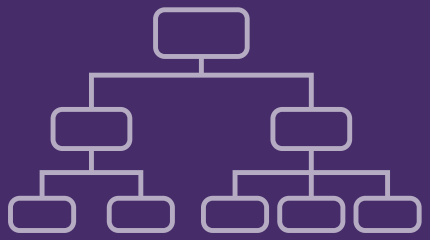
The view of the top 5 risks as ranked by industry risk professionals is presented in Figure 1. It is clear that overall risk profile has evolved considerably since our Horizon study was published at the beginning of the year.

Table 1. Comparison of rankings between the Covid Risk Review in May 2020 and the Operational Risk Horizon conducted at the end of 2019. Level 1 risks are taken from the ORX Reference Taxonomy.

	Covid Risk Review	Operational Risk Horizon 2020
1	Business Continuity	Information Security (inc. Cyber) ●
2	Information Security (inc. Cyber) ●	Conduct
3	Transaction Processing & Execution	Technology
4	People	Regulatory Compliance
5	Third Party	Financial Crime

Figure 1. The top current risks facing the industry by rank score.





The ORX Reference Taxonomy

In 2019, we published an updated level 1 taxomony for operational risk – the ORX Reference Taxonomy. This year, we're continuing our work on taxonomies by creating a cause and impact taxonomy. Download the ORX Reference Taxonomy and find out more on our website: **managingrisktogether.orx.org/operational-risk-taxonomy**

Top operational risks facing the industry

Highlights

- The top 5 risks differ substantially from the Horizon 2020 report, with only information security (including cyber) ranked in the top 5 in both surveys.
- Business continuity, rated as the top risk, had the largest proportion of respondents who felt the risk exposure had increased significantly.
- The vast majority of respondents felt that risk exposures had increased (whether marginally or significantly) since the beginning of the year. Respondents only felt risk exposure decreased when business continuity planning (BCP) was sufficient.
- The overriding risk impact concern is operational (including business disruption), with staff/internal impact also a key concern reflecting the nature of the current crisis.
- Typically, a wide range of drivers affecting these risks were reported, with most risks being interconnected in some way. For example, information security (including cyber) risk concerns were driven by insufficient BCP creating gaps in security controls. They were also driven by people failing to follow cybersecurity norms due to working in an unfamiliar environment and through inadequate third party controls increasing the likelihood of supply chain attacks.

Figure 2. Changes in exposure of the top 5 risks. See appendix on page 8 for full results on all reported risk types.

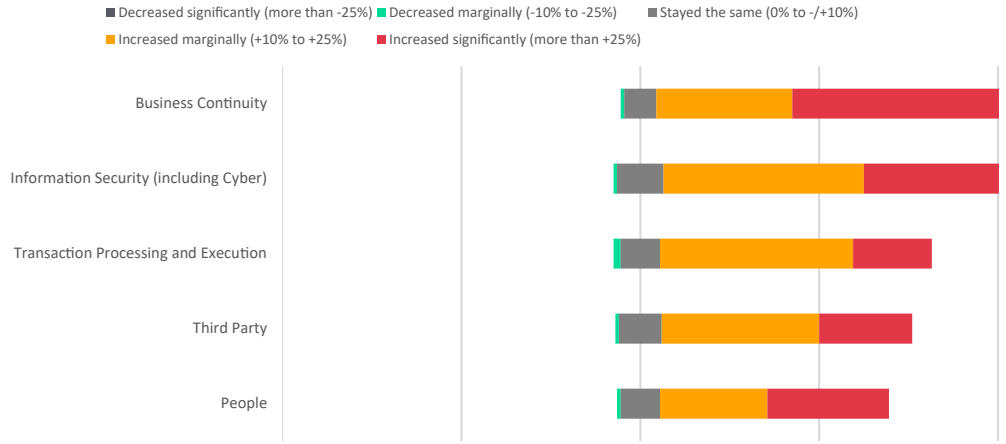


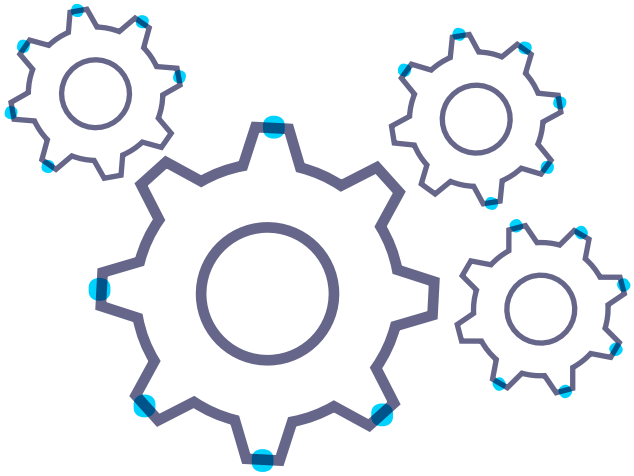
Figure 3. Main impact concern of the top 5 risks.

	Financial	Reputational	Staff/Internal	Regulatory	Operational (inc. business disruption)	Customer	Data privacy and loss
Business Continuity	8%	4%	7%	3%	71%	5%	3%
Information Security (inc. Cyber)	13%	13%	1%	0%	11%	5%	57%
Transaction Processing & Execution	35%	6%	5%	2%	40%	11%	1%
People	7%	3%	67%	0%	20%	4%	0%
Third party	11%	6%	0%	4%	75%	1%	3%

Risk factors impacting the changes in risk profile

Highlights

- The survey results showed several clear themes and that firms are facing similar challenges due to the current coronavirus pandemic.
- Risk factors, or drivers, were largely homogenous, indicating that the global industry overall views the situation in a similar way.
- The top risks and drivers reported were interconnected by a small number of key factors, such as new remote working arrangements, a rapid transition to online services, and potential impact from loss of key staff, among others.



People concerns an integral factor

The coronavirus pandemic has highlighted the significance of people as a driver of the current risk profile. People have been considered both from a material risk perspective and as a significant driver of other risk concerns (in particular for transaction processing and execution risks, fraud and, naturally, people risk).

People risk

- Physical and emotional wellbeing of staff is a key concern, with firms requiring additional health and safety measures both on their premises and in remote working locations.
- There is a concern that a failure to implement and comply with these measures could lead to regulatory sanctions or litigation from workers infected with coronavirus on company premises.
- Respondents noted concerns around key staff dependency and potential unavailability of staff due to sickness or additional pressures.
- There is a longer term concern regarding the management and development of staff who may not return to the office for a long period.

Transaction processing and execution risk

- Many respondents are seeing increased errors with the rapid move to remote working as employees may find it difficult to adapt or be as precise in their work. This may also be exacerbated by an overall reduction of internal controls and levels of supervision.
- Employees may also be distracted by additional responsibilities, such as childcare.

Internal and external fraud

- Modified controls and reduced oversight and monitoring which enable remote working mean firms are more exposed to internal fraud because employees have more opportunity to bypass controls, many of which are designed to operate in an office environment.
- Gaps in security, as well as distracted or stressed employees, are also increasing exposure to external fraud events. This includes cyber events often made possible as employees are less mindful of potential attacks.

Risk factors impacting the changes in risk profile

Business continuity and scenario planning inadequate

The coronavirus pandemic triggered the activation of business continuity plans and rapidly changed the way financial services firms operate. Insufficient BCP is therefore a significant driver of each of the top 5 risks, with the current situation being on a level never previously considered.

- Control environment changes and amended processes have increased exposure to a number of key risks and exposed the resilience of end-to-end processes.
- Compliance with regulatory demands, such as GDPR, is also impacted by the change in working environments. Organisations may not be adequately managing data storage and retention.
- While BCP has largely supported the rapid change in working environment, most frameworks do not account for prolonged remote working arrangements.
- Government responses vary from country to country, making it unclear when to escalate from country level crisis management to group level.
- Future business continuity and resilience planning will need to ensure a safe return to the office and account for a potential second wave of infections, although it is unclear when this might be. Focus will likely shift to planning for the long-term resilience of critical business services, considering these from an organisational, client/customer and macro-economic perspective.

A shift in the cyber threat environment

Changes in the external cyber threat environment mean respondents believe they are more exposed to information security (including cyber) risk.

- Attackers are exploiting the current situation to increasingly launch coronavirus-related phishing campaigns.
- The increased use of digital platforms, both by customers and employees, has increased opportunities for cyber exploitation. Customers with little experience of using digital services are particularly vulnerable

Attackers are taking advantage of relaxed control environments and isolated workforces with potentially lowered cyber and information security hygiene. This reflects discussions at ORX's roundtable for participants of our Cyber and Information Security Risk (CISR) programme.

Economic downturn likely to exacerbate risk exposures

Economic downturn and government measures to relieve economies, such as loan payment deferrals or business interruption loans, are likely to expose institutions to additional risks (including potential increases in future conduct risk). These measures will also increase the cost of debt servicing.

- A surge in customer onboarding for new loans may increase exposure to external fraud and processing errors, particularly given current arrangements and increased pressure on manually operated processes.
- With large parts of global economies at a standstill, bankruptcies of third-party vendors and outsourcing partners could also cause considerable business disruption.
- Furthermore, an economic downturn paired with current control environment channges is likely to drive the occurrence of internal fraud events.

Resilience of third parties a cause for concern

While financial services firms are facing new risks and challenges, their third-party suppliers are impacted by the same issues, with many not as well prepared. The industry's reliance on third parties' continuity has been highlighted by the rapid change in how firms operate and deliver services.

- Many third parties are smaller or less strictly regulated, so may not have sufficiently robust BCP. Financial services firms also lack oversight of their third parties.
- Many vendors operate in areas hardest hit by the coronavirus pandemic, so it is increasingly likely that they are unable to deliver due to lack of liquidity, personnel, or resources.
- The current climate has increased awareness of concentration risk but highlights a lack of data or information available to accurately estimate potential exposure.
- The current environment also exposes third-party vendors to increased cyber risks, and there may be an increase in supply chain attacks impacting financial services firms.

Views across the sectors and differing risk roles

Banks and insurers report largely consistent concerns

- Across the board, business continuity is considered the top current risk, although other risks within the top five diverge slightly.
- Third party risk ranks more highly for insurers with many responses focusing on resilience of third parties located in areas hit hard by the pandemic.
- Insurers considered physical security and safety a key risk, in particular focusing on employee safety and the need for social distancing upon return to the office.

Top risks across key roles

- Across different key roles, respondents largely reported the same risks within their top 5, with business continuity and information security (including cyber) the overriding concerns.
- Transaction processing and execution risk is also a significant concern due to the increased volumes of transactions being processed on new platforms. Responses also focused on the inability to adequately manage change
- Heads of Operational Risk and CROs were the only group not to rank external fraud in their top 5, giving instead a potentiall longer term view of their risk profile.

Table 2. Top 5 risks across the banking and insurance sectors. Level 1 risks taken from the ORX Reference Taxonomy.

	Banking	Insurance
1	Business Continuity	Business Continuity
2	Information Security (inc. Cyber)	Third party
3	Transaction Processing & Execution	People
4	People	Information Security (inc. Cyber)
5	External fraud	Physical Security & Safety

Table 3. Top risks across key roles. Level 1 risks taken from the ORX Reference Taxonomy.

	Heads of Op Risk (1st & 2nd line) and CROs	Op Risk Teams (1st & 2nd line)	Risk Specialists (1st & 2nd line)
1	Business Continuity	Business Continuity	Business Continuity
2	Information Security (inc. Cyber)	Information Security (inc. Cyber)	Information Security (inc. Cyber)
3	People	Transaction Processing & Execution	External fraud
4	Third party	External fraud	People
5	Transaction Processing & Execution	Third party	Transaction Processing & Execution

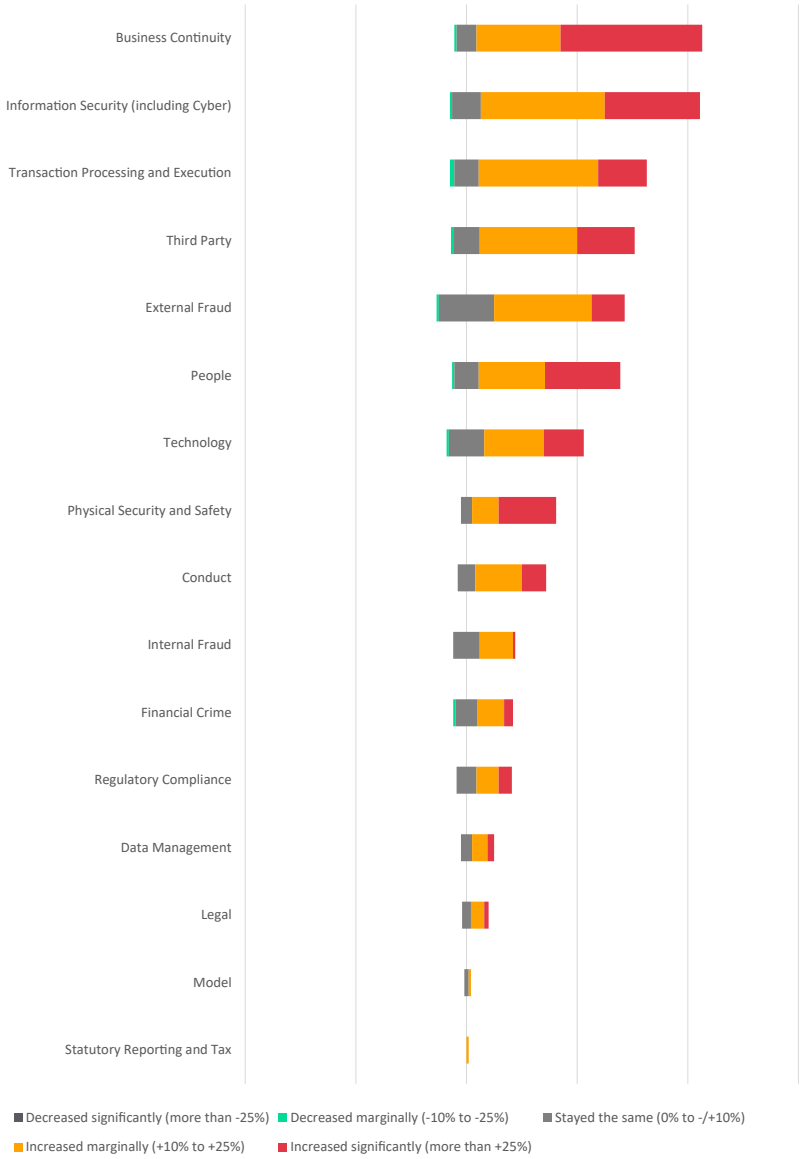
Survey methodology

Participants in the Covid Risk Review were asked to choose and rank their top 5 current risks using the ORX Reference Taxonomy. For each selected risk, participants were then asked to assess whether the risk's overall exposure had increased or decreased since January 2020 (before the outbreak of coronavirus) and to select its top impact concern.

To determine the top 5 risks, we used the Borda count method to apply weightings to risks based on their position in the top five and calculate their overall ranking. The term "rank score" is used in this report to refer to the score calculated in the Borda count method.

Appendix

Figure 4. Changes in exposure of all reported risks.



O.R.X

Managing risk together

ORX believes many heads are better than one. We're here to bring the best minds of the international operational risk community together.

By pooling our resources, sharing ideas, information and experiences, we can learn how best to manage, understand and measure operational risk and become less vulnerable to losses.

We work closely with over 90 member firms to develop a deeper understanding of the discipline and practical tools. We set the agenda, maintain industry standards, and garner fresh insights.

ORX is owned and controlled on an equal basis by its members.

For more information about ORX, visit our website at **www.orx.org**

Contact

Steve Bishop
Head of Risk Information and Insurance, ORX
steve.bishop@orx.org

Lauren Kelleher
Research Analyst, ORX
lauren.kelleher@orx.org


www.orx.org


@ORX_Association


@ORX_association