European Risk Management Council

Risk Landscape Review

June 2019

- Focus on Operational Resilience
- Update on UK and APAC Risk Sentiment Indices

DEAR READER,

I am delighted to present Q2 2019 edition of the Risk Landscape Review which includes three articles.

The last quarterly Risk Council's meeting in London was dedicated to operational enterprise-wide resilience. To continue this important conversation, we include an article "Seize the Opportunity" by Andrew Husband, a financial services consulting partner at KPMG UK, who was one of our special guests and speakers at the meeting. In his article, Andrew Husband explains how the UK Financial Services supervisory authorities' determination to improve firms' operational resilience provides a valuable opportunity for firms to not only comply but to drive resilience and broad-based service excellence.

We also continue our publications of Risk Sentiment Index (RSI), an expert driven forward-looking index that reflects expectations of experts about the risk landscape of the financial sector in the next 12 months. In this edition, we publish two articles on RSI. Using results of our recent surveys that we conducted in London, Singapore and Hong Kong, we updated UK RSI and APAC RSI and publish the detailed results.

My huge thanks to all contributors.

Enjoy the reading.

Yours sincerely,

Dr Evgueni Ivantsov

Chairman of European Risk Management Council

Table of Contents

Seize the Opportunity

By Andrew Husband (a financial services consulting partner at KPMG UK LLP) [1]

Operational resilience has risen rapidly to the top of the agenda for financial services firms. But while last year's Operational Resilience discussion paper[2] published by the Bank of England, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA), collectively 'the supervisory authorities', has been a catalyst for this attention, many organisations now recognise that operational resilience and, more specifically, a focus on end-to-end business services, offers a very real opportunity to create enterprise value. This recognition is critical to securing board and executive sponsorship and therefore driving investment.

To see why, it's important to understand what differentiates operational resilience from its older sibling – operational risk – and how these disciplines can co-exist. Many have asked, isn't Operational Resilience just Operational Risk done properly? We think not.

The supervisory authorities' agenda

The discussion paper set out a joint vision for operational resilience across the financial services industry. Whilst they have intentionally avoided over-prescribing the ways in which firms design and build resilience in practice, having reviewed the paper and in discussions with clients, we believe the following areas are worthy of discussion and consideration at the most senior levels:

1. Board leadership

According to the paper, the supervisory authorities want firms to take a top-down, integrated view of operational resilience that is led and driven by the board and senior management. Executives will need to ensure they have sufficient expertise and information on operational resilience, with appropriately resourced enterprise-wide operational resilience procedures. The UK's Senior Managers Regime prescribes that the SMF24 is accountable for operational resilience. In practice this accountability is most often passed to the Chief Operating Officer (COO). Boards will expect the SMF24 to provide the reporting and insight required to ensure that investment decisions properly consider implications for the firm's resilience alongside cost and growth considerations.

[1] Andrew Husband is a financial services consulting partner at KPMG UK LLP and leads the firm's multi-disciplinary Operational Resilience practice. Andrew started his career in Operational and Technology consulting before spending eight years with a global Investment Bank where he led the CFO's strategic change team. He has extensive experience supporting banking clients in structuring and delivering their most complex regulatory and strategic change programmes. Andrew holds an MBA from INSEAD.

[2] https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

2. Operational resilience culture

The supervisory authorities expect firms to foster a culture that prizes resilience, and considers it a key priority in the design and build of new processes or services across everything a firm does. Firms will be expected to promote resilience as a core measure of the firm's health alongside the traditional suspects of revenue and growth, customer experience and cost management.

3. End-to-end business service approach

Disruption to end-to-end services causes consumer harm and market instability. The discussion paper hones in on resilience across end-to-end services and challenges the legacy practices aligned to vertical siloes – an organisation method not inherently resilient. Accountability must be considered and assigned for the resilience of horizontal services, which will require firms to identify their important business services and to continuously assess the resilience of the underlying technology, data, people, suppliers and property that support them. Critically, this will require firms to fully understand the role that third and fourth party suppliers play in the delivery of these services and the resilience implications they bring.

4. Specify tolerances

Firms should establish impact tolerances using specific outcomes or metrics from a consumer, business or financial stability perspective. For example, a firm might set a maximum acceptable outage time for a key business service. This quantifies the amount of disruption the firm believes could be tolerated during an incident and sets the point after which it believes disruption would begin to cause consumer harm, threaten the firm's ongoing viability or create material economic impact.

By setting impact tolerances, a firm's board and senior management can consider how to recover when a disruption does occur, rather than simply trying to minimise the probability of disruption.

5. Testing

Firms will need to establish rigorous end-to-end testing programmes that challenge their ability to remain within tolerance limits in severe but plausible scenarios. Tests will need to be designed to understand what impact a disruption to a key business service would have on customers of that service and also on other connected business services. Tests should also be used to understand the resilience and suitability of manual workarounds or substitute processes that seek to reduce or prevent harm to customers.

6. Recovery and response

Firms should assume that disruptive events will occur, so that their focus is on planning for what happens when such issues do arise. That will include potential responses to a disruptive event, such as the ability to rapidly identify the scale of the impact. It will also cover the firm's ability to recover from a disruptive event, through robust and well-tested recovery plans. These plans will set out how

firms can adapt or substitute their resources to enable the continuity or resumption of key business services within agreed tolerances.

7. Effective communication

Firms will need to communicate effectively. Internally, that includes upward reporting and effective decision-making. Externally, communication should manage the expectations and restore the confidence of those affected by disruption, including customers and other stakeholders. The role that timely and accurate communications can play in minimising service disruption can't be overstated, and must be properly recognised and planned for.

Operational risk versus Operational resilience

Another key area that we have found stimulates discussion with clients is understanding the distinction between operational risk and operational resilience – which we believe lies in the origin of each.

Operational risk evolved as an integral part of a firm's approach to establishing capital adequacy under the Basel regime. The prevailing regulatory view was that if firms were financially stable, the system would be stable. If a firm had sufficient capital set aside to cover any operational risk events, then all would be well.

Operational risk management has undoubtedly evolved to embrace thematic risks and drive operational stability, but it has not been designed to address the core regulatory objectives behind today's focus on operational resilience. It has at its heart a necessary focus on the effectiveness of point controls within vertical organisational structures at the level of processes, applications, properties or third-party suppliers; the design and maintenance of these controls then ensures the ongoing stability of the firm.

With operational resilience, the focus is on putting in place a management system that will develop more resilient services both today and in the future as services – and disruptive forces – continue to evolve. Operational resilience understands the interconnected nature of our business reality, and the idea that a firm may now present material threats to a market's stability and cause great harm to consumers even when it is not in a position of financial stress.

The discussion paper makes it clear that the emphasis for operational resilience should be on the continuity of horizontal business services. It is the end-to-end business service that must be resilient; boards and senior management will need to make informed investment decisions on this basis.

While the current state of operational risk and operational resilience practices are distinct, we anticipate that these disciplines will grow closer. Viewing risk and resilience through the lens of the "Three Lines of Defence" model, it is easy to envisage a world in which a combined "Operational Risk and Resilience" capability is managed in the first line, with control and oversight exercised in the second.

We expect that key functions from across the Chief Risk Officer (CRO), Chief Operating Officer (COO) and Chief Information Security Officer (CISO) capabilities will move closer together under an umbrella of Operational Resilience. This will likely include the emerging COO Operational Resilience capabilities, the Operational Risk capabilities and the legacy resilience disciplines of Business Continuity Planning and IT disaster recovery as organisations look to streamline their capabilities and organise to efficiently deliver Enterprise-wide Operational Resilience alongside Enterprise-wide risk management.

Moving from compliance to enterprise value

Clearly establishing the distinction between operational risk and operational resilience, the initial rationale for their co-existence, and the incremental case for investment in operational resilience will be a key step in securing executive sponsorship and building the business case.

However, at the heart of regulatory thinking lie two key elements. Firms will need a deep understanding of what it takes to deliver their end-to-end services, and boards and senior managers will need deeper technical and operational knowledge of how these services are delivered.

Any investment in these elements has the potential to drive a business case that goes far beyond compliance. Forward-thinking firms will capitalise on their enhanced understanding of end-to-end service delivery and with increases in Board and executive expertise to drive broad-based service excellence.

So what ambition should firms set? Broadly, there are three options.

Compliance, albeit often a material challenge in and of itself, will mean meeting the minimum operational resilience requirements defined by the regulators. Over time, we expect most firms to move beyond compliance and adopt a real focus on driving ***substantive resilience***; investing in the management system that nurtures resilience across important business services as primary business objective, delivering compliance as a consequence. However, leading firms will look to go further, expressly targeting broad-based ***service excellence***.

Transformation, innovation, customer experience, profitability and most importantly, trust will all benefit from a service excellence driven approach.

Firms embracing service excellence will reshape their organisation and accountability models in alignment with the “horizontal” service management approach and will exploit that superior understanding of end-to-end service delivery models and the underlying assets, capabilities and suppliers that support them.

For this reason, the focus on operational resilience represents an opportunity as well as a challenge. Firms that think through how to pair end-to-end service management with a deep understanding of their technology and operations from board level down, will drive an increased return on investment over those who approach this agenda through regulatory compliance or stand-alone resilience lenses.

UK Risk Sentiment Index:

Finally, it's a downward trend, but for how long?

The European Risk Management Council has updated its UK Risk Sentiment Index (RSI). Fresh data was collected in June 2019. Chief Risk Officers and other senior risk executives provided their views on the future trends of seven types of risk. Using the survey results, the Council aggregated the data into a forward-looking index that reflects expectations about the risk landscape of the UK financial services sector in the next 12 months. Numerically, the RSI reflects the adjusted percentage of experts who consider that risk will increase in the next 12 months.

Aggregated RSI is down

Based on expert judgement of CROs and other risk executives, the aggregated RSI across seven risk types stands at 0.42 in June 2019. Compared to an RSI of 0.54 six months earlier and 0.56 in Q1 2019, the current level of RSI represents a substantial reduction (see figure 1). Overall, 60% of respondents believe that risks will increase in the next 12 months vs 73% respondents voted for an increase in March 2019 (see figure 2). Moreover, we observe a growing number of experts compared to that in the past quarter who believe that the industry has reached a "risk equilibrium" and the current level of risks will not change much in the next 12 months (one third of experts in Q2 2019 vs one fifth in Q1 2019 and Q4 2018).

Figure 1. RSI trend: Q4 2018 – Q2 2019

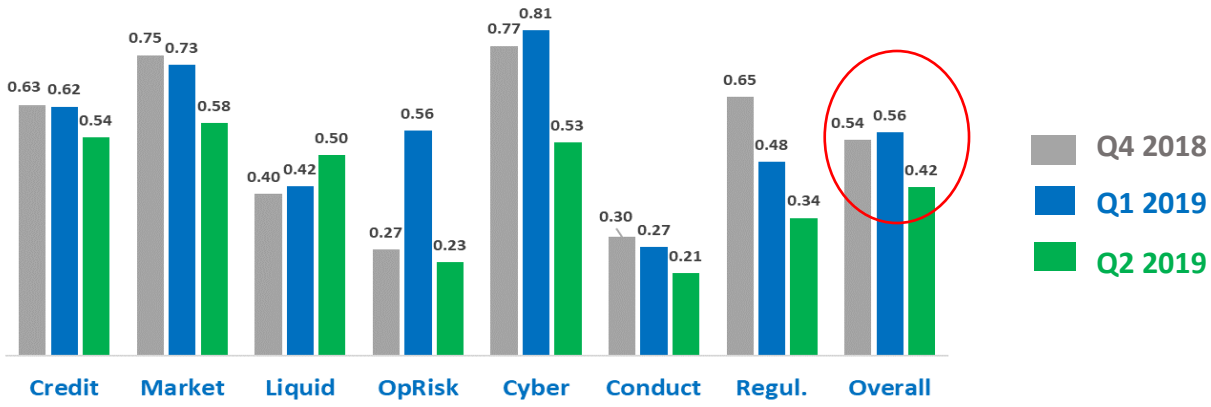
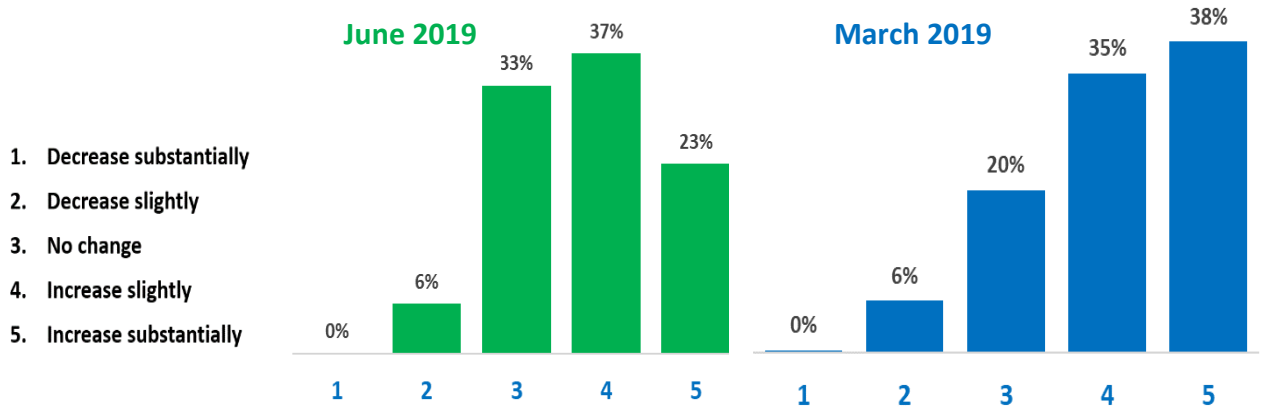


Figure 2. Aggregated results for all risks: June 2019 vs March 2019



Is the storm almost over?

One of the possible explanations of the changing RSI trend is Brexit. In Q4 2018 and Q1 2019, the UK was approaching the initial Brexit deadline (29 Match 2019). The chaotic last-minute negotiation with the EU-27, a deadlock in the UK Parliament over the Brexit, the government agony with numerous Cabinet resignations, a failure of UK political elite to reach any agreement on Brexit created a deep frustration and very negative expectations regarding UK's political and economic future. These expectations were reflected in experts' responses to survey questions and, eventually, led to very high RSIs recorded in Q4 2019 and Q1 2019 (0.54 and 0.56 respectively).

After the extensions of the initial Brexit deadline until 12 April and then until 31 October, the UK business society started developing visibly fatigue from the Brexit endless saga and became less concerned about the potential no-deal shock. The recent RSI survey in June 2019 suggests that 70% of experts believe that the industry either reached its risk plateau (no change in risk in the next 12 months) or almost reached it (a slight increase).

In spite of the changing RSI trend, a serious concern about the future UK risk landscape remains. A number of pessimists among the respondents is still relatively high – almost a quarter of our respondents expect a further substantial increase of risks in the next 12 months. Only 6% of experts are cautiously optimistic and anticipate a slight decrease of the risks in the near future. The main question that still stands is would we see a reverse of the RSI trend in case of further Brexit complication?

RSI per risk types

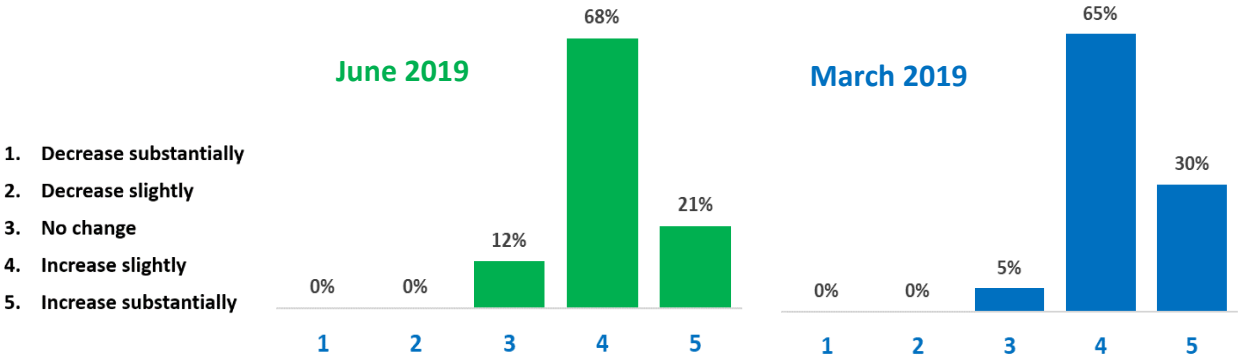
The changing trend is observed not only at the aggregated RSI level but also at the level of the rank order of individual risks. In the previous six months, cyber and IT risk was by far the major concern of the respondents which resulted in the highest RSI among all seven risk types. The recent survey suggests that experts have changed their view on cyber risk and don't think that cyber risk will grow more than other risks in the next 12 months. While RSI of cyber risk remains among the top three risks, experts shifted their focus to market and credit risks which now are ranked by them as number 1 and number 2 with RSIs of 0.58 and 0.54 respectively.

Conduct risk remains at the bottom of the "worry list" with RSI of only 0.21. It doesn't mean that respondents expect the reduction of conduct risk. RSI does not reflect the absolute risk level but measures a "steepness of the slop" – an incremental change of risk expected in the next 12 months compared to its current level. Any RSI of more than 0 means an incremental growth. The current level of RSI for conduct risk is relatively low but a percentage of experts that anticipate a further increase of conduct risk is still higher than a percentage of respondents who think otherwise.

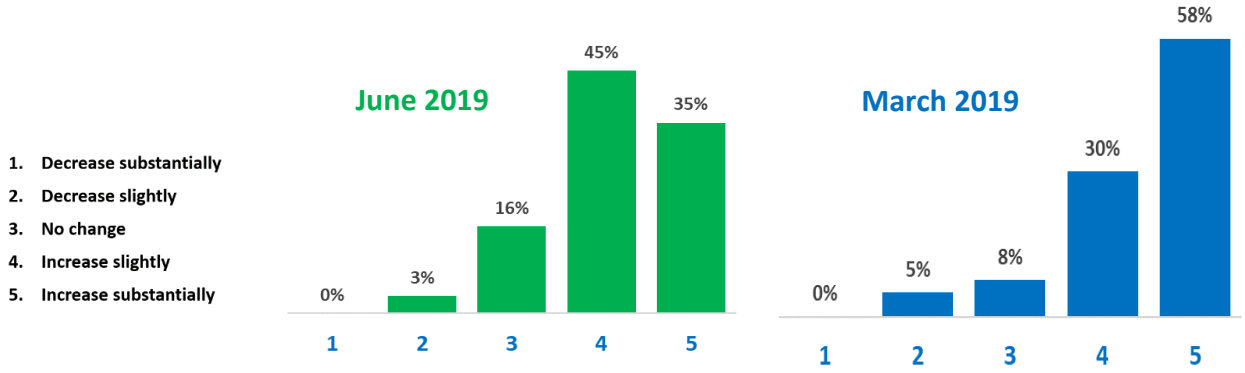
UK Risk Sentiment Index - Vote distribution (in % of total votes provided)

In your opinion, how will the following risks for UK financial industry change in the next 12 months?

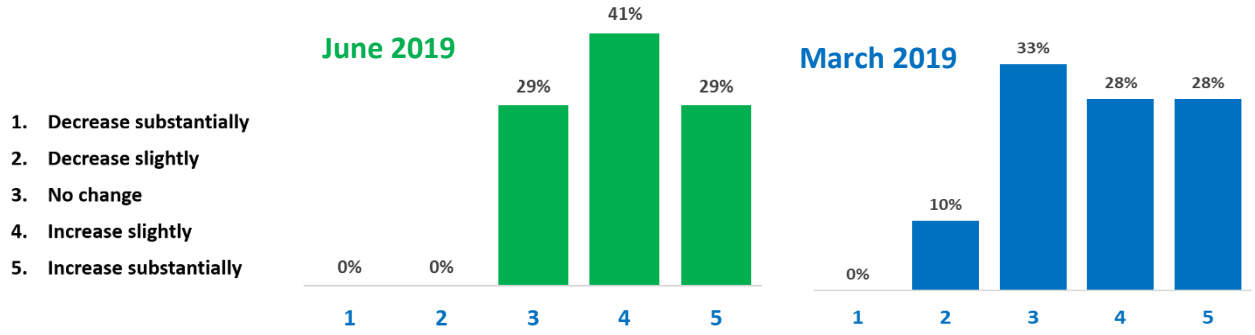
1. **Credit Risk** *(Risk that borrowers or counterparties will fail to meet its obligations in accordance with agreed terms)*



2. **Market Risk** *(Risk of losses in on and off-balance sheet positions arising from adverse movements in market prices)*

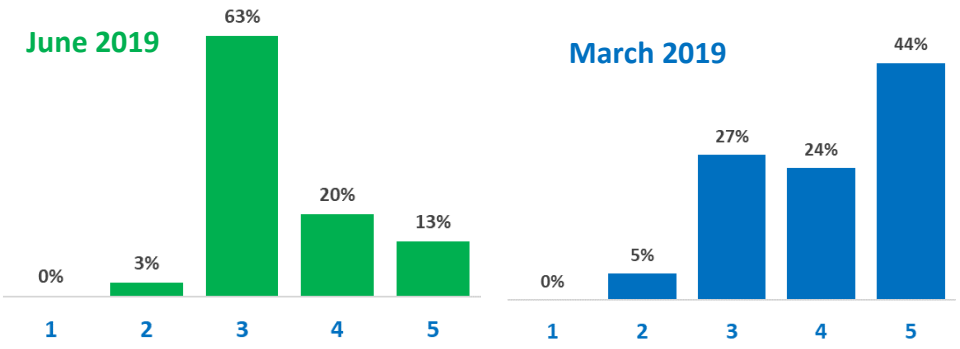


3. **Liquidity Risk** *(Risk for solvent institutions to lose their ability to make agreed upon payments in a timely fashion as well to raise funding in short notice)*



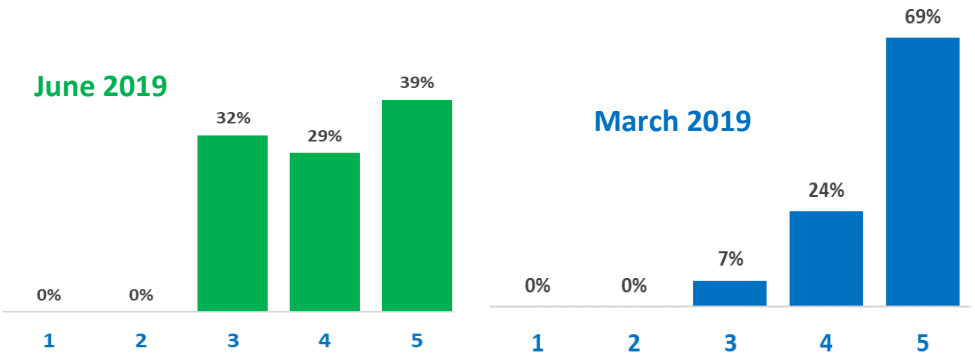
4. **Operational Risk excluding cyber and IT** *(Risk of human errors, control failures, failure of internal processes, model risk, risk of frauds, third party risk, physical safety risk)*

1. Decrease substantially
2. Decrease slightly
3. No change
4. Increase slightly
5. Increase substantially



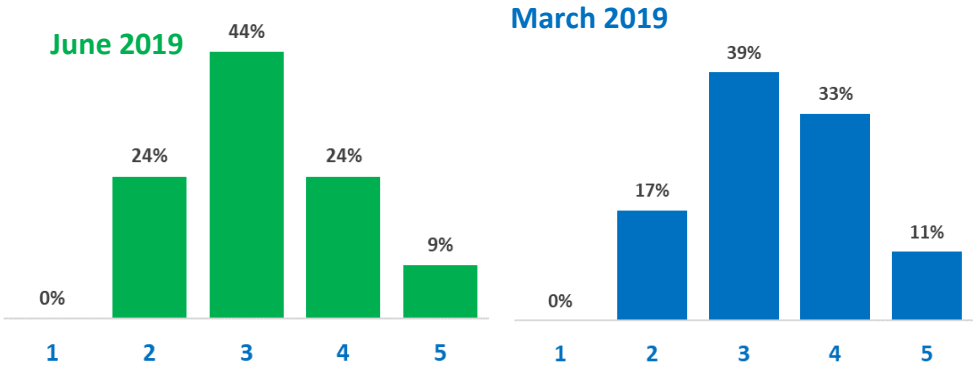
5. **Cyber Risk** *(Risk of events that can lead to data breaches, financial loss, reputational damage, and disruption of operations caused by a failure of IT systems and procedures)*

1. Decrease substantially
2. Decrease slightly
3. No change
4. Increase slightly
5. Increase substantially



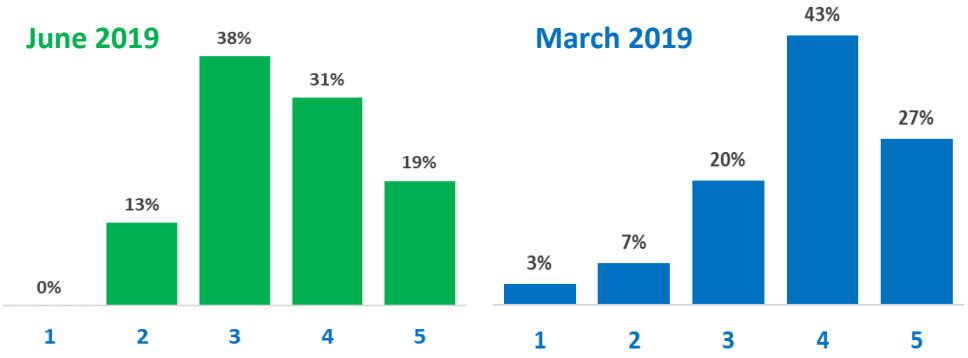
6. **Conduct Risk** *(Risk of actions that lead to customer detriment or has an adverse effect on market stability and effective competition as well as a failure to comply with a regulatory defined code of conduct)*

1. Decrease substantially
2. Decrease slightly
3. No change
4. Increase slightly
5. Increase substantially



7. Regulatory Risk *(Risk that a change in laws and regulations or unintended consequences of that change will materially impact a security, business, or market)*

1. **Decrease substantially**
2. **Decrease slightly**
3. **No change**
4. **Increase slightly**
5. **Increase substantially**



APAC Risk Sentiment Index:

The story remains the same

The European Risk Management Council has updated its APAC Risk Sentiment Index (RSI). Fresh data was collected at APAC Risk Council's think tank meetings in Singapore and Hong Kong in May 2019. Chief Risk Officers and other senior risk executives from APAC region provided their expert opinions on the future trends of seven types of risk. Using the survey results, the Council aggregated the data into a forward-looking index that reflects expectations about the risk landscape of APAC financial services sector in the next 12 months. Numerically, the RSI reflects the adjusted percentage of experts who consider that risk will increase in the next 12 months.

Further reduction of aggregated RSI

Based on expert judgement of CROs and other risk executives, the aggregated APAC RSI across seven risk types reduced from 0.51 in Q1 2019 to 0.42 in Q2 2019. Therefore, the downward trend that we already identified three months ago accelerated further in Q2 (see figure 1). Overall, the level of optimism among respondents has grown substantially. Now more than a third of respondents don't expect an increase of risks in the next 12 months versus less than one quarter in Q1. A percentage of "pessimists" who expect a substantial increase of risks in the next 12 months also has gone down from 26% to 20% between the Q1 and Q2 surveys (see figure 2).

Figure 1. RSI trend: Q4 2018 – Q2 2019

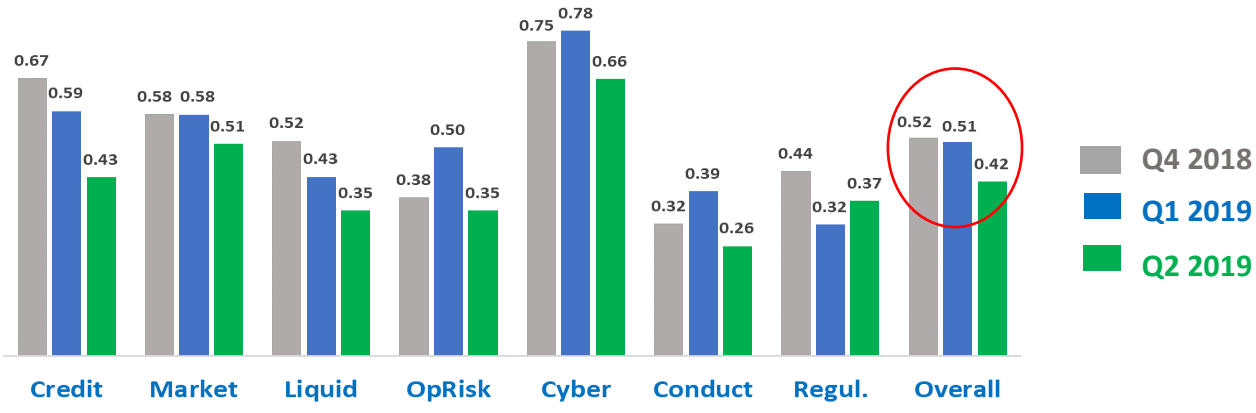
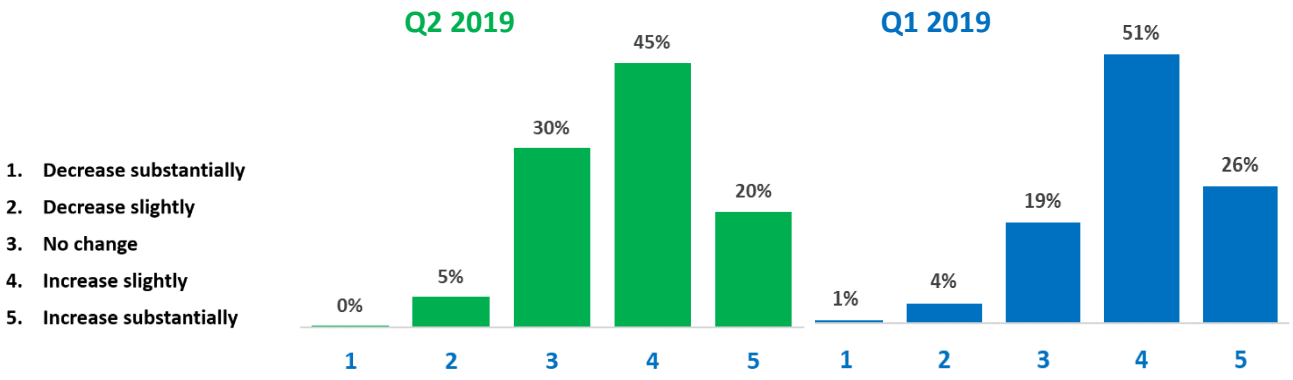


Figure 2. Aggregated results for all risks: Q2 2019 vs Q1 2019



RSI per risk types

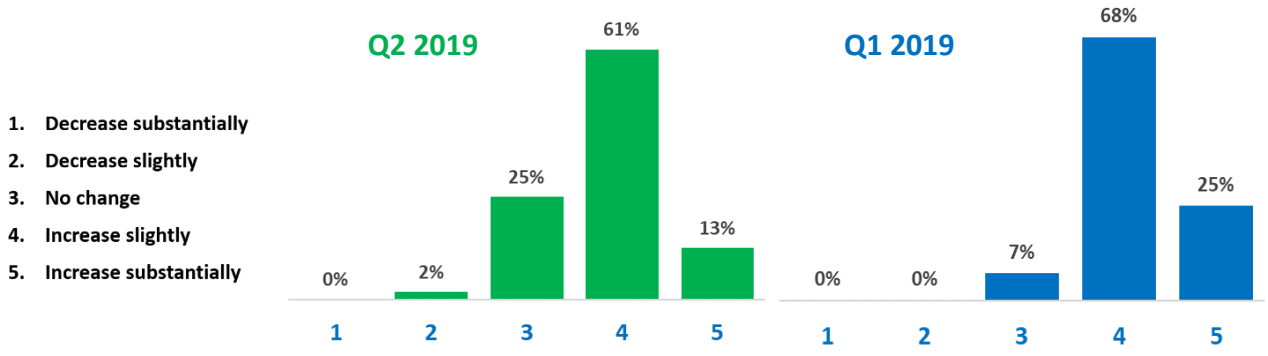
The substantial reduction of the aggregated RSI in Q2 was achieved due to a reduction across all risk types except one. The only risk type which RSI increased in Q2 was regulatory risk. The largest drops in individual RSIs have been observed for credit, operational, conduct and cyber risks. The reduction of these RSIs doesn't mean that experts anticipate a reduction of these risks in absolute terms in the future. As RSI measures a "steepness of the risk landscape slop", the quarter-by-quarter reduction of RSI observed for these risks mean that experts anticipate that an incremental increase of these risks in the next 12 months will be less than they expected in the previous quarter.

As in previous six months, cyber and IT risk remains at the top of the "worries league table" although the RSI of cyber risk experienced a substantial reduction this quarter from 0.78 to 0.66. Market risk now moved to the second spot of the table overtaking credit risk. RSI of credit risk has a large drop in Q2 2019 as respondents are less worry about a future risk hike – a percentage of experts who believe that credit risk will not increase has grown from 7% in Q1 2019 to 27% in Q2 2019! According to experts' opinion, conduct risk is an area where risk will increase least. In fact, 62% of respondents expect either no change or a reduction of conduct risk.

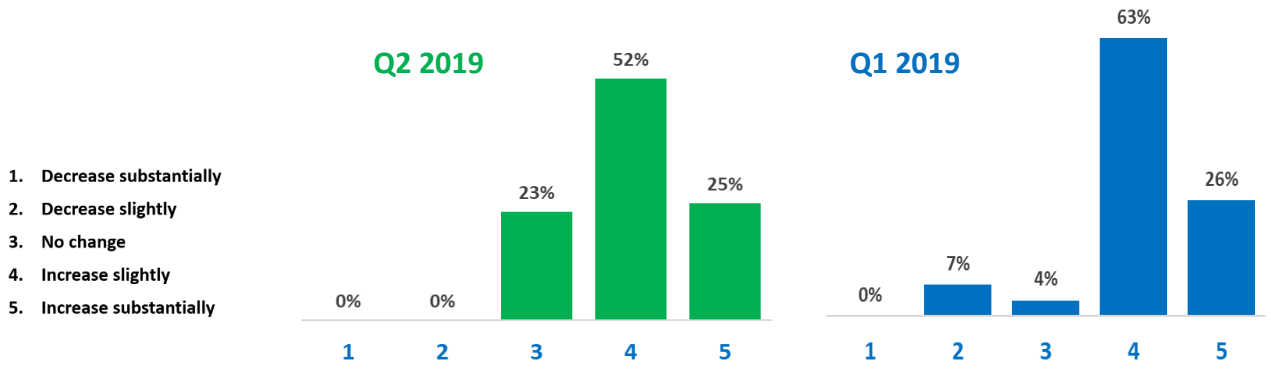
APAC Risk Sentiment Index - Vote distribution (in % of total votes provided)

In your opinion, how will the following risks for APAC financial industry change in the next 12 months?

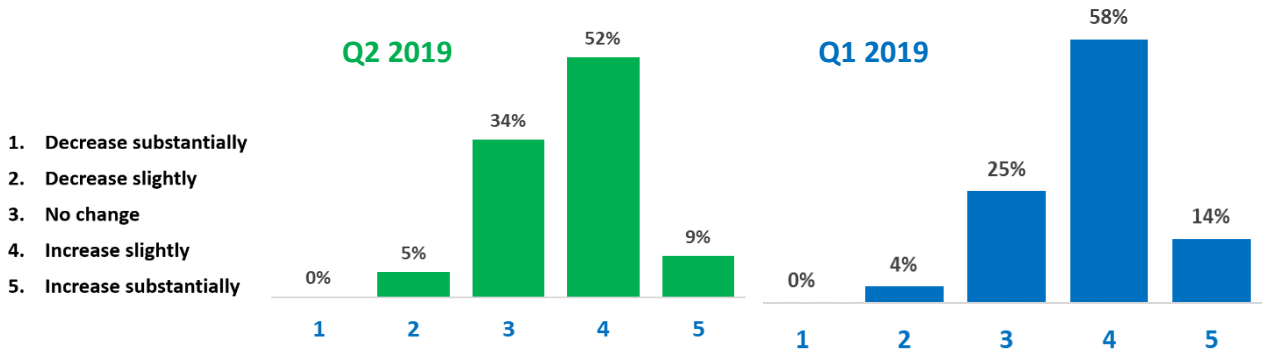
Credit Risk *(Risk that borrowers or counterparties will fail to meet its obligations in accordance with agreed terms)*



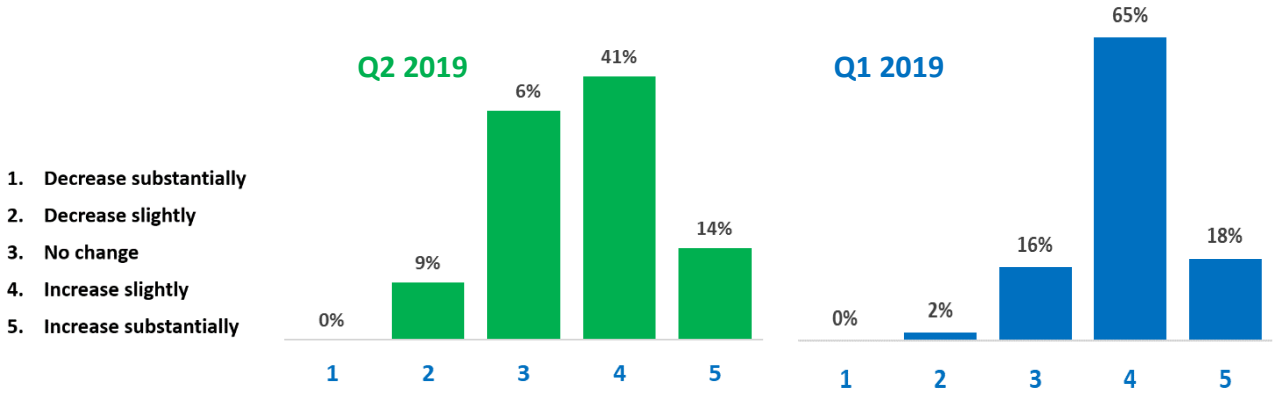
1. **Market Risk** *(Risk of losses in on and off-balance sheet positions arising from adverse movements in market prices)*



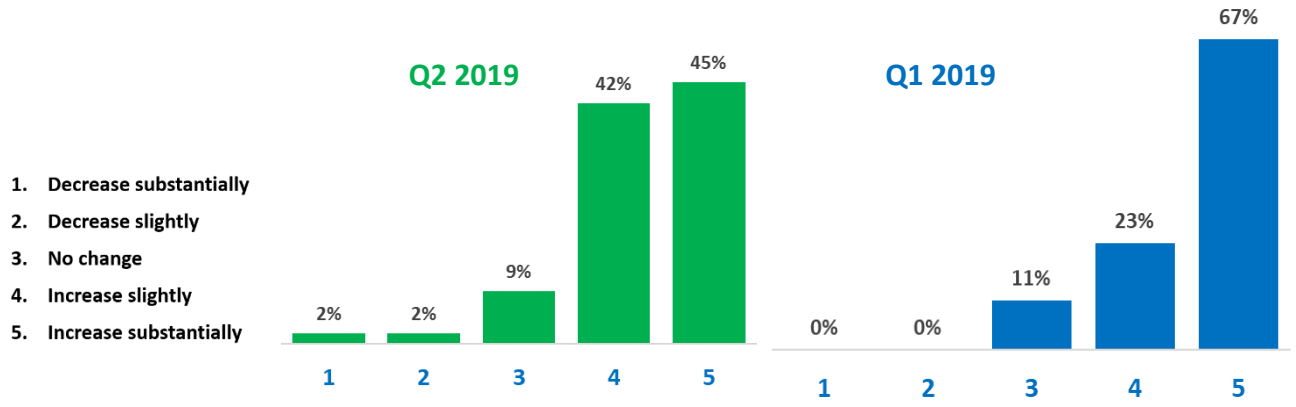
2. **Liquidity Risk** *(Risk for solvent institutions to lose their ability to make agreed upon payments in a timely fashion as well to raise funding in short notice)*



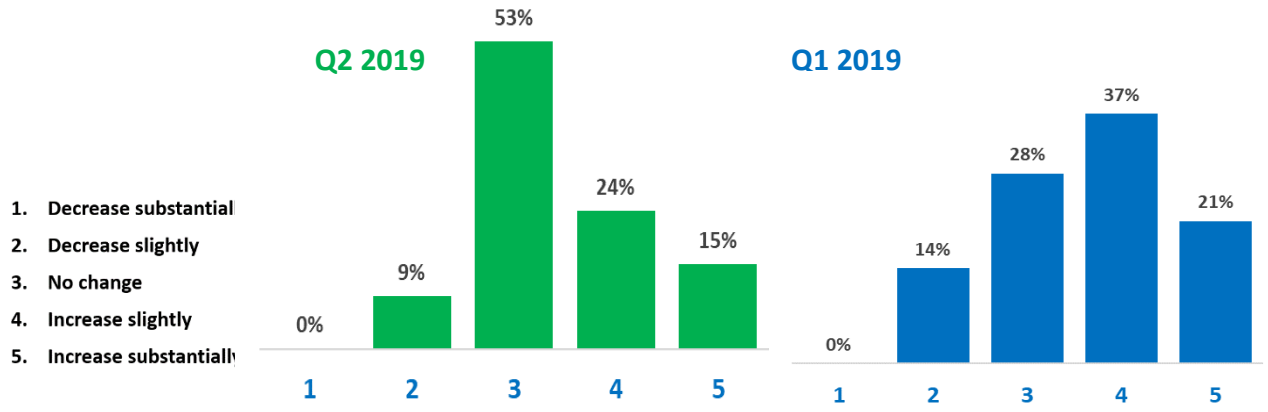
3. **Operational Risk excluding cyber and IT** *(Risk of human errors, control failures, failure of internal processes, model risk, risk of frauds, third party risk, physical safety risk)*



4. **Cyber Risk** *(Risk of events that can lead to data breaches, financial loss, reputational damage, and disruption of operations caused by a failure of IT systems and procedures)*



5. **Conduct Risk** *(Risk of actions that lead to customer detriment or has an adverse effect on market stability and effective competition as well as a failure to comply with a regulatory defined code of conduct)*



6. **Regulatory Risk** *(Risk that a change in laws and regulations or unintended consequences of that change will materially impact a security, business, or market)*