accenture

The sphere of control

Accenture 2019 Global Risk Management Study Insurance Report

Discover how insurance leaders are taking a holistic view of the risk landscape, prioritizing what they do know and preparing for what they don't.

Contents

INTRODUCTION

Get on the front foot

Insurance companies brace for the unknown consequences of new technology, aggressive competition and changing client expectations.

Welcome to Accenture's 2019 Global Risk Management Study report on insurance.

This year we explore how insurance companies are responding to emerging risks, particularly those relating to evolving regulation, cyber threats, insurance technology (InsurTech), changing customer expectations and LIBOR retirement.

This report presents the findings from our 2019 Global Risk Management Study, which uncovers how 683 surveyed risk executives across the entire financial services industry, including those working for insurance, banking and capital markets businesses, are adapting to the ever-increasing pace and volume of change outside the four walls of the organization.

What did we find in the survey? Let's quickly recap before delving deeper into the insurance findings.

For a start, risk managers across financial services acknowledge that complex, interconnected new risks are emerging at a more rapid pace than ever before. Over half (58 percent) say that disruptive technology risk has greater impact on their business today than it did two years ago.

A major cause of their concern relates to the growing adoption of new technologies across the organization. Of course, these technologies hold immense potential to unleash growth and drive efficiencies, but risk functions worry about the potential for unforeseen consequences, which they are currently not capable of identifying or assessing.

57%

of our study respondents expect to use marketing data to support their risk management activity in two years' time, but only 39 percent do so today.

Faced with an increasingly complex, but data-rich risk environment, risk functions should invest in smart technologies such as artificial intelligence (AI) and natural language processing (NLP) that have immense potential to improve effectiveness and efficiency. Indeed, survey respondents that have deployed machine learning feel much more confident that they have prepared their business for volatile future scenarios.

But while the benefits are significant, risk functions' use of the most sophisticated technologies is currently limited. Our study findings indicate that the risk function is aware of the need to embrace these new tools, but is simply slow in making effective use of these to date.

Technology aside, an effective risk function is one that is armed with the data it needs to anticipate, assess, and ultimately mitigate emerging threats.

But today, many are not. For example, 57 percent of our study respondents expect to use marketing data to support their risk management activity in two years' time, but only 39 percent do so today.

Getting access to relevant data is one thing, but maintaining the quality and knowing how to analyze it effectively to generate useful insights remains a significant challenge. The risk managers we surveyed as part of the 2019 Global Risk Management Study realize that they fall short here, so they are urgently seeking to improve both their data-collection and analysis skills: 63 percent are urgently improving their ability to collect enterprise-wide data, and 66 percent are honing their ability to analyze it.

How do our cohort of 227 surveyed insurance risk executives believe the risk environment has shifted? For a start, the growing frequency and sophistication of cyber threats has made insurance companies more susceptible to attack than ever before.

In parallel, the emergence of InsurTech creates huge opportunities, but also monumental risk if it disintermediates established carriers or leads to vulnerabilities when implemented.

And changing customer expectations, combined with fundamental shifts in consumer habits in certain markets (for example, vehicle ownership), is reducing the demand for specific types of insurance and increasing appetite for personalized products.

Furthermore, new regulations continue to be introduced and updated. In fact, the Accenture 2019 Global Risk Management Study data reveals that evolving regulation is currently causing insurance risk managers greatest concern (see Figure 1). This is primarily driven by the monumental effort and expense required to comply with the International Financial Reporting Standards (IFRS) 17 and data privacy laws. Indeed, some large insurers in jurisdictions where IFRS 17 applies are spending hundreds of millions to comply by 2021.

Regulations relating to customer best interest, conduct, capital standards and fraud also continue to evolve swiftly and require close attention.

This report explores which risks are currently most important to insurance companies. The survey data reveals a common theme: insurance risk managers fear the unknown.

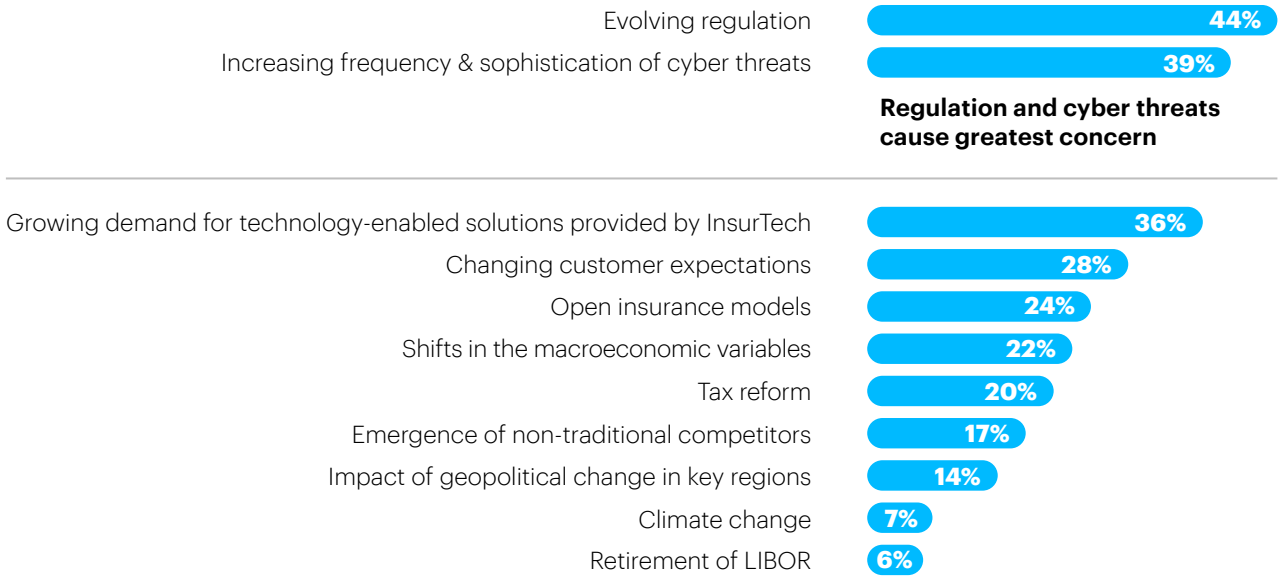
Take the increasing sophistication of cyber attacks, surveyed insurance companies' second-most important concern. They are aware of the risk and have adopted more quantitative and sophisticated approaches to identify them, but don't know where exactly they are most vulnerable.

The same applies to InsurTech. Respondents rank this as the third-greatest threat, but primarily because they are unsure whether their organization is keeping pace with sector-wide investment levels. They are also unsure what the unintended consequences of implementing these technologies might be.

With the external landscape changing so rapidly, insurance companies should urgently improve their ability to identify and assess new threats, and invest in the technology and skills required to mitigate them.

Figure 1. Areas of greatest concern to the insurance industry

Thinking specifically about the insurance industry, which of the following areas are currently causing your business the greatest amount of concern?



Source: Accenture 2019 Global Risk Management Study

SECTION 1

Cyber threats and new regulation—the perfect storm

Our 2019 Global Risk Management Study reveals the top two threats: evolving regulation and the increasing frequency and sophistication of cyber threats (See Figure 1).

Why have cyber threats increased in both frequency and severity? Firstly, insurance companies are now more vulnerable due to their reliance on new technology such as the internet of things (IoT). New alliances with InsurTech companies or other third parties also increase susceptibility. The tools that external bad actors use to facilitate cyber attacks have also become more sophisticated.

In parallel, General Data Protection Regulation (GDPR) in the EU and similar regulations around the world have introduced strict requirements for data protection, and significant penalties if these are not met. Therefore, the potential financial consequences, not to mention the threat of reputational damage resulting from a data breach, have never been more serious.

The increasingly complex cyber environment has also changed the nature of other, more traditional risks. For example, fraudsters previously had to co-opt doctors or vehicle-repair companies to perpetrate insurance fraud. Now, they can deploy cyber techniques to mimic or steal credentials and use these synthetic identities to initiate fraudulent claims or withdrawals.

In short, there are multiple reasons why the threat has grown. But, rather than being concerned with specific, identified cyber threats, insurance risk managers are nervous about what they don't know.

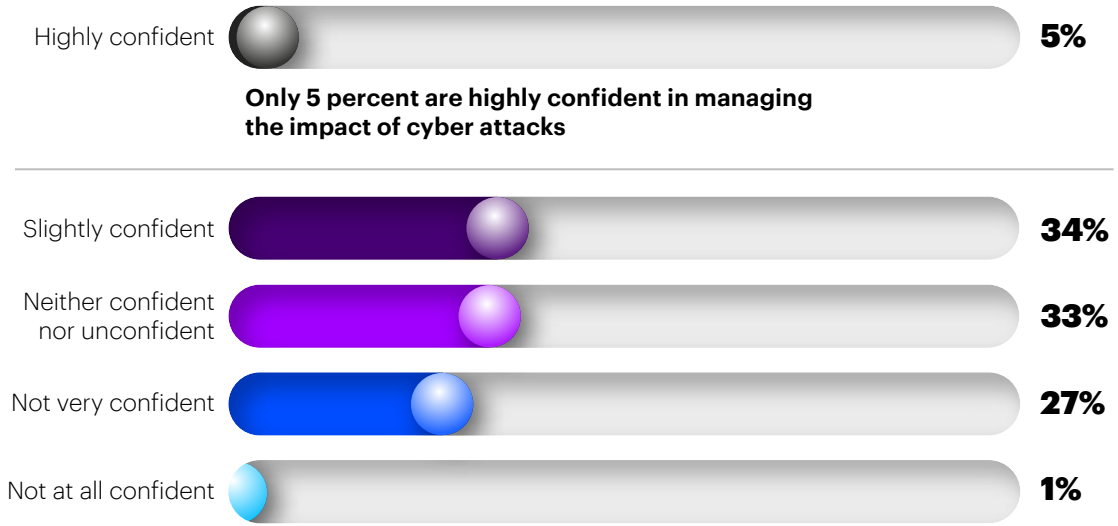
For example, they have typically been later than banks and capital markets businesses to adopt cloud. They know that their cyber risk profile has changed as a result, but cannot pinpoint where their new vulnerabilities lie. They know they are exposed, but don't know exactly where.

"Data privacy and cyber security have certainly become front of mind for insurance businesses recently. I think their concerns about evolving regulation continue to be broad-based, but they now think increasingly about the compounding impact of data privacy regulation on cyber security."

Chris Johnston
Managing Director, Accenture Financial Services
Finance & Risk

Figure 2. Level of confidence in managing the impact of cyber attacks

How confident are you that your risk function is set up to fully support your business in managing threats relating to the increasing frequency and sophistication of cyber threats?



Source: Accenture 2019 Global Risk Management Study

But while the threat level has risen, the study reveals that insurance risk managers are not prepared to handle the combination of complex cyber threats and harsher regulatory penalties for data breaches. Just 11 percent describe themselves as highly confident in managing threats related to evolving regulation and only 5 percent say the same about managing cyber threats (see Figure 2).

It's time for them to up their game. But how? There is no simple solution. As detailed in Accenture's 2018 State of Cyber Resilience for Insurance report, insurance companies should urgently make a number of improvements to achieve cyber mastery. These include investing in sophisticated cyber security technologies that allow an almost real-time response to threats, as well as stress-testing and simulating cyber attacks to assess resilience while training the entire workforce. This type of advanced simulation and controls testing goes well beyond the anti-phishing learning programs many insurers have deployed across their enterprises.

SECTION 2

InsurTech creates new category of risks

Insurance risk leaders surveyed as part of the 2019 Global Risk Management Study cite growing demand for technology-based solutions provided by InsurTech as their third-most significant concern.

10%

Fewer than 10 percent of surveyed risk managers are fully capable of assessing risks associated with adopting robotic process automation (RPA), AI, machine learning, and blockchain.

Again, we find that insurance risk leaders understand that this growth can create significant risks for their organizations, but that they don't quite understand how.

For example, they know that some InsurTech companies could erode revenue because they compete directly with traditional carriers in certain areas. But they do not know which parts of their businesses are vulnerable to disruption.

Large insurance carriers are striving to stay resilient to the competitive threat posed by InsurTech companies by adapting their customer experience and interactions, and refining products and services. But there are still significant risks.

Insurers that have taken the plunge and invested significantly in new technology worry about the effectiveness and potential business impacts of using sophisticated AI and machine learning technology to, for example, validate pricing or assess claims. Tellingly, fewer than 10 percent of surveyed risk managers are fully capable of assessing risks associated with adopting robotic process automation (RPA), AI, machine learning, and blockchain.

Intelligent automation (the combination of RPA and AI) is increasingly viewed as a key driver of operating profitability in the context of low interest rates and shifting consumer needs. Risk teams should therefore urgently improve their ability to assess risks associated with its deployment.

"There is a big element of the fear of the unknown. A number of companies express concern that others are running off and making use of these new technologies, while they are still struggling to find specific use cases to make them relevant, get scale and drive value."

Steve Culp
Senior Managing Director, Accenture Financial Services
Management Consulting and Finance & Risk

"Insurers are working with InsurTech companies to offer new solutions. This creates opportunities but also huge risks, especially if lots of customer data is transferred from the insurer to the InsurTech, which will likely have less sophisticated data protection measures."

Caroline Desroches
Managing Director, Accenture Financial Services Finance & Risk

Finally, insurers are also likely concerned about the potential unintended consequences of alliances with InsurTech and non-InsurTech companies as part of efforts to broaden their ecosystem.

The number of such alliances has grown significantly in recent years as insurers seek to create personalized insurance products and completely new non-insurance products for customers.

For example, a variety of carriers are incorporating financial wellness services into their Life & Annuity product offerings.

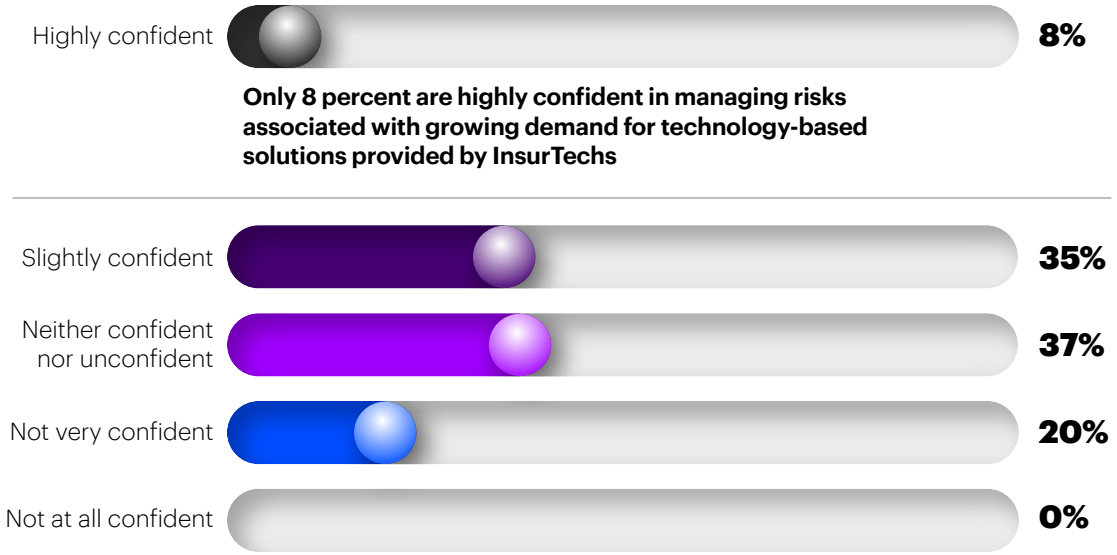
While allowing traditional insurance carriers to implement InsurTech and expand their product suite more quickly, these alliances can bring added risk, such as increased cyber vulnerability. This is especially the case when there is significant technical integration or large volumes of data are shared between the insurer and the alliance company.

Today, risk teams are not equipped to manage risks associated with growing demand for technology-based solutions. Just 8 percent of study respondents describe themselves as highly confident in managing these threats (see Figure 3).

They should, therefore, rapidly improve their ability to identify and manage threats associated with InsurTech and other emerging technology solutions that can improve customer experiences and overall business growth, especially if they are forming new alliances. Understanding these technologies and the risks they bring is key to doing this effectively.

Figure 3. Level of confidence in managing risks associated with technology-based solutions

How confident are you that your risk function is set up to fully support your business in managing threats relating to the growing demand for technology-enabled solutions provided by InsurTechs?



Source: Accenture 2019 Global Risk Management Study

SECTION 3

Keep sight of changing customer sentiment

2019 Global Risk Management Study insurance respondents rank changing customer expectations as their fourth-most important threat. Customer preferences are shifting in multiple ways, and this is creating numerous risks.

For a start, whenever they interact with their insurer, consumers now expect the quick, intuitive and seamless experience that they have grown used to with online retailers. Failure to provide this can result in customer renewal attrition.

Changing customer expectations outside the insurance industry also create new risks for insurers. For example, a marked shift in customer preferences away from car ownership to using ride-sharing services and manufacturers including insurance through the car purchase are already starting to create implications for the auto insurance market.

"If you don't have a set of offerings or an interaction model that is frictionless, simple, and essentially Amazon-like, then you are in trouble, especially in those moments of truth when insurers deal with claims."

Jim Bramblet
Managing Director, Accenture Financial Services
North America Insurance

Risk teams should also 'be live' to customer demands for new types of insurance. In particular, business demand for cyber security coverage has grown significantly in recent years in response to rising threat levels. The paucity of data means that risk teams have to carefully evaluate how these products are priced and managed.

Only 10 percent of surveyed insurance risk managers describe themselves as highly confident in managing threats that stem from changing customer expectations. Therefore, they should urgently improve their ability to identify trends in customer expectations and adjust their products and channels to market accordingly.

Having the appropriate data is key to identifying changes in customer sentiment. But today, use of this data is mixed. For example, 54 percent of surveyed insurance companies use consumer data to support risk management activity, and just 36 percent use social media data. Acknowledging the importance of this data, more insurance risk teams plan to use it regularly in two years' time: 74 percent expect to use customer data and 54 percent intend to use social media data by 2021.

10%

Only 10 percent describe themselves as highly confident in managing threats that stem from changing customer expectations.

SECTION 4

Proactively manage LIBOR retirement risk

The 2021 retirement of LIBOR and transition to other interbank offered rates (IBORs) may not pose an immediate threat that is of the same magnitude as other risks discussed in this report, but it can't be ignored.

Whether it is the risk of basis exposure, the sheer effort required to update LIBOR provisions in contracts, or managing conduct risk, LIBOR transition is a major undertaking that demands proactive risk management.

Non-risk business leaders acknowledge this and have called on risk teams to assist. Almost three-quarters of financial services businesses surveyed in Accenture's 2019 LIBOR Survey say risk management is of greater importance in supporting LIBOR transition.[1]

But our Global Risk Management Study reveals that this call has, to date, gone unanswered. Tellingly, just 6 percent of surveyed insurance risk managers cite LIBOR retirement as a top-three concern. They have not even recognized it as a major threat, let alone started to act.

Now it is time for risk leaders to step up. Instead of simply recalibrating risk models, they should work collaboratively with other business functions to unearth the impact on the entire business.

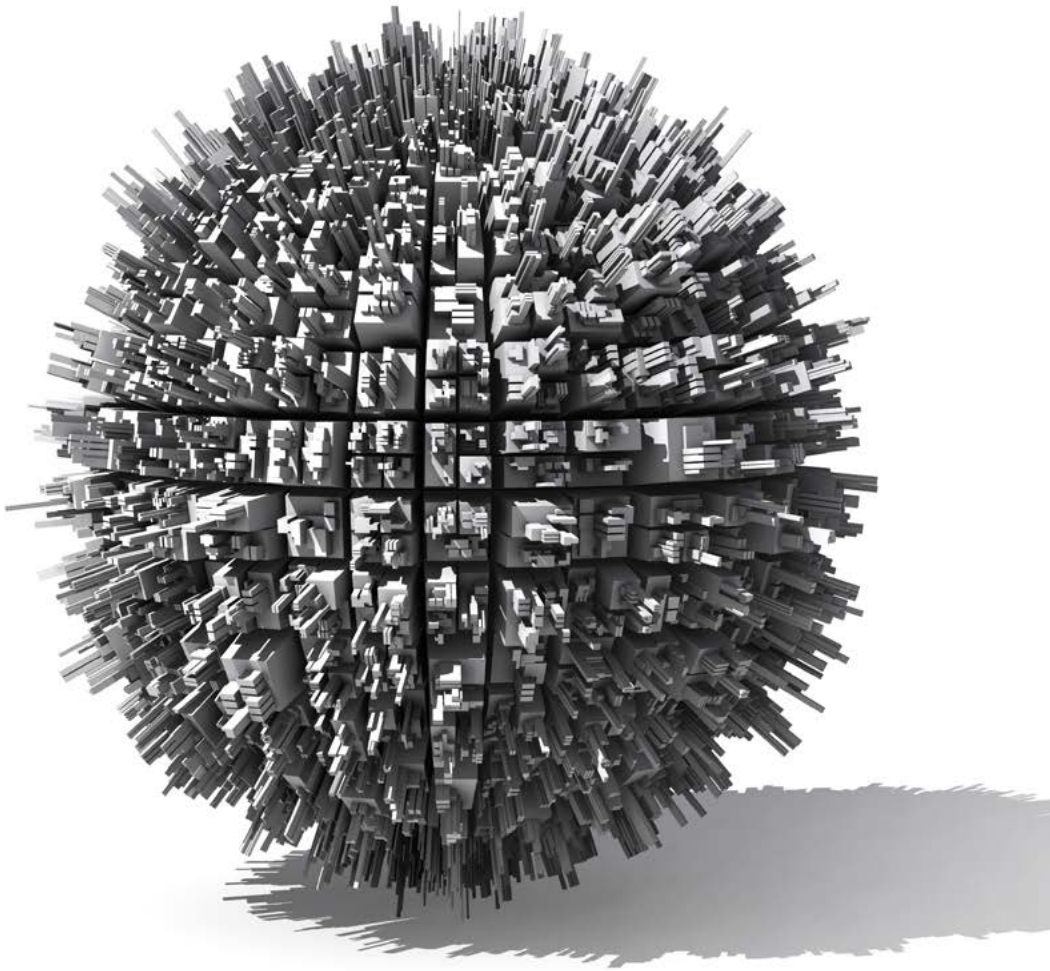
1 "Accenture 2019 LIBOR Survey," September 2019

Uncover the hidden risks of LIBOR transition

What exactly should risk teams do to help prepare? The first step is to identify and then quantify exposure to specific LIBOR risks. LIBOR exposure lurks in hidden corners of businesses' operations, so risk managers should be thorough in their approach.

Second, risk managers should establish a robust framework to assess and manage the risks associated with the transition. This should cover how the transition impacts a range of risks, including operational and portfolio risk. Importantly, risk teams should assess how these risks materialize both internally and externally. A poorly timed and ill-executed transition strategy—both internally and across the entire financial services industry—could potentially leave insurers with significant operational risk.

Conduct risk cannot be forgotten, and risk managers should devise measures to protect clients and markets from possible abuse and mis-selling. This could involve enhanced training controls or market education programs. In parallel, risk teams should review new and amended products to make sure they do not adversely impact clients.



LIBOR retirement is fast approaching. Risk managers are encouraged to act quickly or be left behind as the rest of the business prepares for the transition.

SECTION 5

How insurers can manage today's major threats

Managing the new threats facing insurers is no simple task. There are no easy wins or quick fixes. Rather, risk leaders should implement a number of measures to boost resilience. Some of these involve simply implementing the basics that have been neglected.

There is a certain amount of catching up to do with the likes of banks and capital market businesses. We recommend that insurers take the following steps:

1. Define emerging threats

The sheer pace of change in the risk landscape has left insurance companies fretting about unexpected and unknown threats. It is impossible to identify all risks, but risk leaders can limit their exposure by being proactive.

Specifically, they should map out how the increased use of new technology and data, as well as alliance with third-party InsurTech companies, increases cyber security exposure. They should also seek to identify how changing customer expectations impact demand for certain types of insurance.

These threats can only be tackled once they are identified. Of course, some threats materialize quickly and unexpectedly, so risk managers have to strike the right balance between prediction and preparation.

2. Fight fire with fire

Smart analytical tools can help to identify and mitigate a range of threats. They can detect data anomalies that indicate fraud and trawl networks to identify malware, for instance. But they are currently under-used: Only 9 percent of insurance respondents deploy machine learning as part of their risk management, for example.

3. Prioritize data hygiene

Smart analytical technologies such as AI and machine learning can help risk functions detect threats. But they won't work if the data that feeds them is not clean or standardized.

It is not possible to completely standardize data across the entire organization. But risk managers should still implement the necessary structures and governance controls to keep data as clean as possible. AI tools can also be deployed to cleanse data.

In addition to improving data quality, strict governance and access controls make it harder for internal and external bad actors to exfiltrate critical or personal data.

4. Right-size new product compliance to speed innovation

In response to customers' increasing demand for technology-based solutions, many insurers have ramped up their own innovation efforts and initiated alliances and business relationships.

At some stage, the risk function should be called upon to approve new products and business partners, and it is here that tensions can surface. The product team is keen to release its new product to the market, but the risk team might have hundreds of compliance checks that have to be completed first.

Agility is key. Risk teams should only process the checks that are absolutely essential at the early stages of product development or the formation of an alliance. An overbearing approach, incorporating unnecessary checks, can stifle innovation and delay new product releases, while denying the alliance the oxygen to thrive.

This is not just about undertaking checks at the right time, but also about automating manual work. For example, risk teams spend a lot of time checking the risk profile of new products and making sure risky solutions are not employed with risk-averse clients. Today, much of that work can be executed effectively using RPA.

CONCLUSION

Define your sphere of control

Unknown, interconnected risks are multiplying at a faster rate than ever before. It is impossible to try and control all aspects of the complex business environment in which insurers operate, and the faster that risk leaders acknowledge this fact, the better.

Firstly, risk functions should prioritize what matters most. Taking a holistic view of the risk environment, they should have clear criteria to gauge the value of their assets and assess which are most critical to protect.

Secondly, leaders should prepare their function by allocating resources smartly, embracing the latest tools and technologies, and upskilling their people so they can wield them reliably.

Finally, risk leaders should build a more proactive function, diligently scanning the horizon for the next threats, as risks evolve and approach in unfamiliar forms. Rather than plan for specific eventualities, they should continue to prepare for disruption—looking outwards in every direction.

Those who can draw a clear line between the factors they control and the factors they cannot are taking an important step towards focus and prioritization. Equally, the risk management function should focus its efforts and energy on preparation and planning, rather than on prediction—so irrespective of the cause of the issue, the insurer is ready to respond effectively to mitigate the impact.

This is how to manage your sphere of control.

Acknowledgments

About the authors

Steve Culp
Steve Culp is a Senior Managing Director—Accenture Financial Services, Management Consulting and the Finance & Risk practice. Based in Chicago, Steve has more than 25 years of experience working with clients across multiple geographies to define strategy and execute change programs across risk management and the broader finance function. His current focus is to work with client leadership to help them advance their business performance through innovative strategies, processes and change. Steve holds a Bachelor of Science in Finance and Economics from Northern Illinois University and earned an Executive Master of Business Administration degree at Kellogg in 1999.

Aliette Leleux
Aliette Leleux is a Managing Director—Accenture Financial Services, Finance & Risk. With over 20 years of deep industry and consultancy experience, Aliette leads the Finance & Risk practice in Asia Pacific. Her current focus is working with global financial institutions and their C-suite executives and leadership to help them navigate large enterprise and IT change and transformation projects to drive sustainable business value. A consummate developer of talent, Aliette also holds a Master in Corporate Finance from Paris-Dauphine University.

Chris Johnston
Chris Johnston is a Managing Director—Accenture Financial Services, Finance & Risk. Based in Chicago, Chris leads the practice in North America and brings nearly 30 years of deep experience driving complex transformation programs involving core finance, enterprise risk, organization and culture, data integration, cyber resiliency, compliance, and procurement. His fresh thinking and approach to streamlining operating models allow him to support CFOs, CROs, CPOs, CIOs and their agendas. Chris holds a Bachelor of Science in Engineering from the University of Illinois.

Contributors: Julia Heinzer, Niccolo Bergamini and Masaharu Akasaka

About the research

The Accenture 2019 Global Risk Management Study is the sixth edition of our study first published in 2009. It is based on a telephone survey (computer-assisted telephone interviewing, CATI) of 683 senior risk management executives conducted by Longitude Research Ltd on behalf of Accenture between March 2019 and April 2019.

Survey participants were sourced from around the world and work in three sectors within financial services: banking (255 participants), capital markets (201 participants), and insurance (227 participants).

To complement the survey data, Accenture applied natural language processing to a database of earnings calls and conference transcripts from 2010 to 2018 in order to verify financial services firms' most pressing risks. This analysis covered 225 firms in banking, capital markets, and insurance. It identifies the risk types being addressed, the intensity of the discussion, and how this changes over time.

For each of the 10 risk types probed, a set of keywords were developed to generate a risk frequency. This frequency was then divided by the total number of words available for each company across all earnings calls and conference transcripts to arrive at the proportion of transcripts devoted to a risk overall and over time. This measure was then log-transformed to smooth out extreme values and rescaled to allow relative comparisons across risk types and industries.

Finally, a normalization process was applied to generate an index of values between 0 and 100 for each company-risk type, where 100 indicates the highest intensity of discussion around a risk and 0 indicates no discussion. The normalized measures are relative in nature and allow comparison of the intensity of discussions across topics as well as over time. When presenting the results, financial, operational, and regulatory risks were grouped into a 'traditional risks' category.

Contact

Accenture Finance and Risk
www.accenture.com/financeandrisk

Finance and Risk Blog
financeandriskblog.accenture.com

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 492,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**

Join the Conversation

www.linkedin.com/showcase/16183502

@AccentureFSRisk

12460807