metricstream

STATE OF IT AND CYBER RISK MANAGEMENT SURVEY REPORT 2021

Growing Enterprise Adoption of IT GRC Solutions: An Emerging Trend in the Post-Pandemic World

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The unprecedented events of 2020 have set in motion transformations on multiple fronts for organizations worldwide. As the COVID-19 pandemic engulfed the entire world, governments resorted to lockdown and travel restrictions, compelling companies to support remote working and accelerate the pace of digital transformation. However, as organizations looked to quickly adjust to the new normal, cyber adversaries were also on the lookout to exploit any vulnerabilities or loopholes.

Security teams and risk professionals were already inundated with ensuring the effectiveness of their cyber defense mechanism. The pandemic has only exacerbated their challenges as they now have to ensure cyber resilience for their organizations in a hostile open environment.

The dire situation warrants adopting a matured cyber risk management program by organizations, which will provide a holistic view of their cyber risk and compliance posture and cyberthreat exposures, bolster their risk identification and alleviation capabilities, and reduce response time to risk events. Automated IT GRC solutions can greatly help security professionals in their pursuit of achieving cyber certainty.

This is essentially the premise on which we publish the latest edition of our IT and Cyber Risk Management Survey Report. We reached out to organizations across industries and geographies to understand how their IT and cyber risk management programs have been impacted by the pandemic, their top priorities and challenges, areas of future investment, and more.

- **Low Level of Automation and Associated Challenges**

  Our survey highlighted the widespread dependency of organizations on basic office productivity software, knowledge management software, and point solutions for their IT and cyber risk and compliance management needs. These methods are largely manual in nature and time-consuming and greatly impede an organization's risk visibility and foresight capabilities, and therefore hamper quick and efficient decision-making.

  Subsequently, it was not surprising when survey participants identified a lack of visibility on cyber risks across the enterprise and a manual approach to managing cyber risks and compliance as the top challenges faced by their organization. Accordingly, respondents stated that creating real-time visibility on risk and compliance posture is their top priority for this year.

- **Impact of the Pandemic**

  The pandemic has proven to be a defining moment for organizations around the globe. The resulting push to go digital and support entirely remote working setup has not only amplified existing cyber threats but also created new ones. To navigate these untested waters, many organizations changed their plans and approaches to cyber risk and compliance management and reprioritized their activities, deployed new tools and systems to enhance their efficiency, and admitted that the current crisis has expanded the scope of IT and cyber risk and compliance programs. Only a few organizations said that they did not make any changes to their plans, approaches, and activities related to cyber risk and compliance management in the wake of the pandemic.

- **CISO – A Key Role in Today's Business Environment**

The survey highlighted a growing awareness among organizations to have a dedicated Chief Information Security Officer (CISO) for their security needs. Having a CISO is a business imperative in today's digital era as they possess the required expertise to have a peripheral view of cyber risks, take key decisions and mitigate security threats in an effective manner, ensure compliance with IT regulations and standards, and report back to the board on overall IT and cyber risk and compliance posture.

> *"In 2020, resilience has become table stake for cyber leaders. Cybersecurity is now operationally forced by the pandemic, legislatively required by governments, internally compelled by the executive management and the board, externally bulldozed by cyberattacks, technologically enabled by AI and automation, and finally, experientially desired by customers."*
>
> **- Andreas Diggelmann**,
> Chief Technology Officer,
> MetricStream

- **Areas of Future Investment**

As it appears, ensuring regulatory compliance sits on top of the minds of many organizations and they are seeking to implement specific solutions to achieve this goal. Other areas where organizations are likely to put their money into this year include tools and technologies for IT and security data aggregation and analytics, and centralized cyber risk and compliance solution.

Overall, a key takeaway from the survey is that organizations are gradually becoming cognizant of the benefits that an automated and integrated cyber risk and compliance solution can engender. As such, they are increasingly looking to implement IT GRC solutions that can ensure the efficiency and robustness of their cyber strategies, bolster cyber and operational resilience, and ultimately, create—not just protect—business value.

DISTRIBUTION OF SURVEY PARTICIPANTS

The survey respondents comprised of key risk, compliance, cybersecurity, and audit executives across industries and included analysts, managers and senior managers, vice presidents, directors and heads of departments, CISOs, and others. Here is a look at the distribution of survey participants:

By Industry

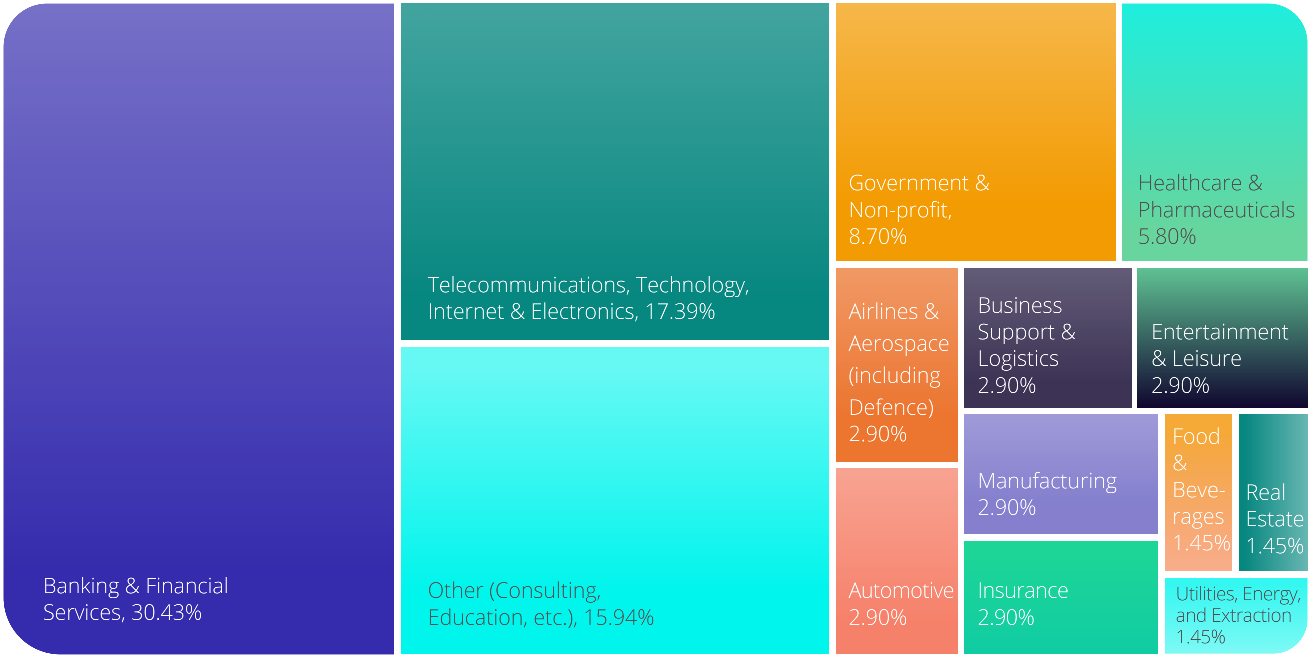


Figure 1: Industry

By Geography

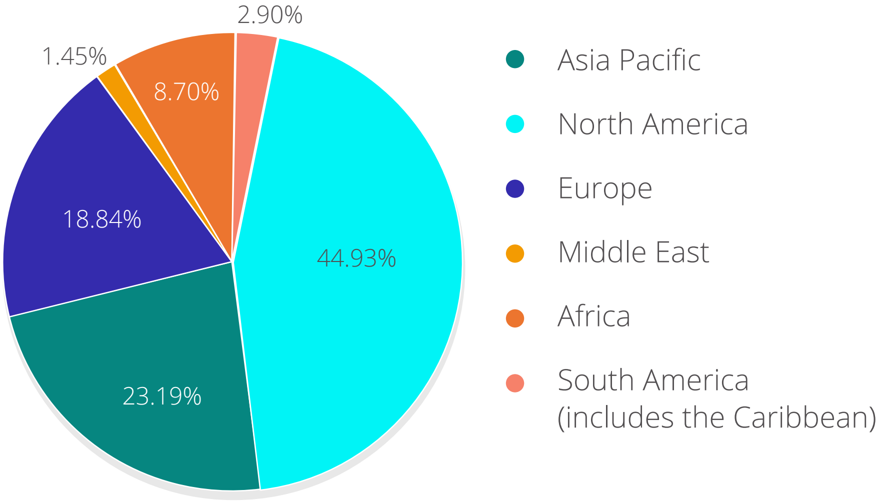


Figure 2: Geography

By Company Size

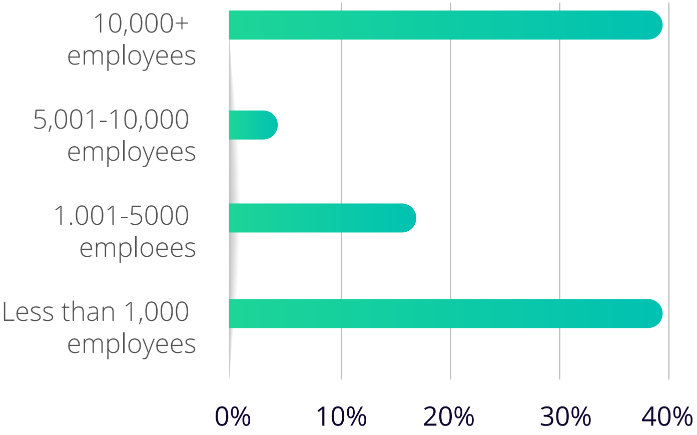


Figure 3: Company size

By Size of IT and Cyber Risk and Compliance Teams

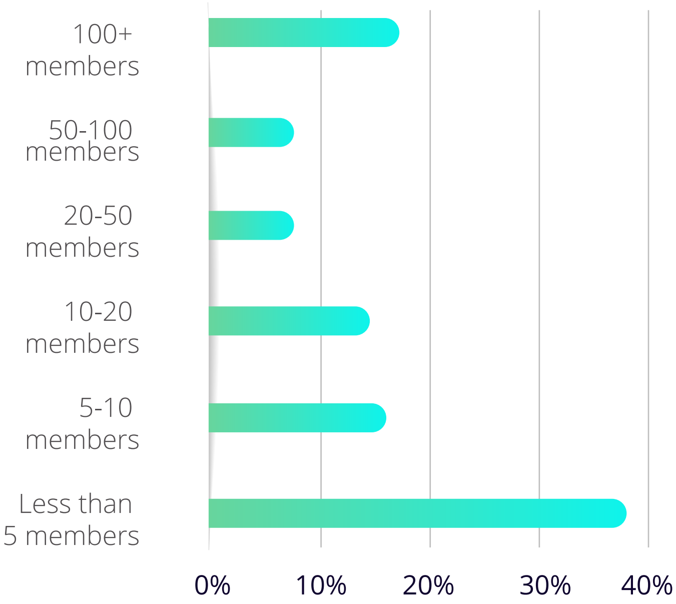


Figure 4: Size of IT and cyber risk and compliance teams

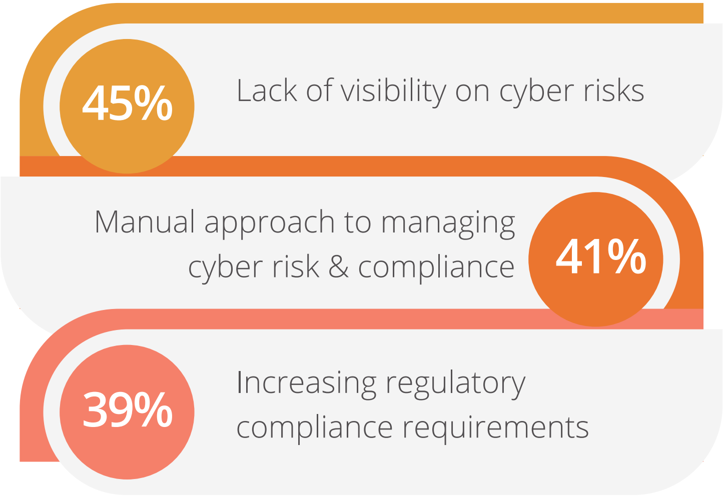
IT AND CYBER RISK MANAGEMENT SURVEY RESULTS AND ANALYSIS

KEY FINDINGS

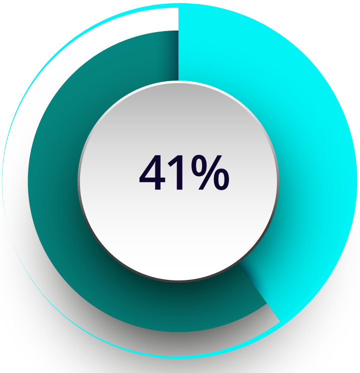
In its 2020 Annual Cybersecurity Report, Trend Micro said that it detected over 16 million COVID-19 related threats. Of these, 88% of the threats came in the form of spam emails, 11% were in the form of URLs, while malware accounted for 0.2% of the threats. Cybersecurity Ventures estimates the cost of global cybercrime to grow by 15 percent per year over the next five years, reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015.

Data is the lifeblood of organizations in this era defined by rapid digitization and hyper-connectivity, and protecting it is pressing priority. Organizations today operate under the constant threat of cyberattacks and cannot assume that they have an impenetrable cyber defense infrastructure. As cybercriminals are becoming increasingly organized and sophisticated, the need to focus on building and sustaining cyber resilience capabilities is paramount. Adopting a proactive approach to cyber threat detection, response, and recovery is key to achieving cyber and business resilience. To delve deeper into the evolving cyber risk landscape and understand how organizations are approaching the critical business function of cyber risk management in the new normal, we conducted a survey of key IT and cybersecurity executives across multiple geographies and industries. Here is a look at the key findings:

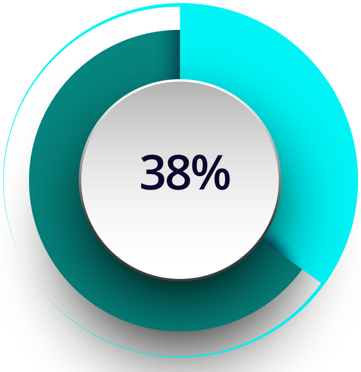
- Most survey respondents (45%) identified lack of visibility on cyber risks across the enterprise as the major challenge faced by their organization.



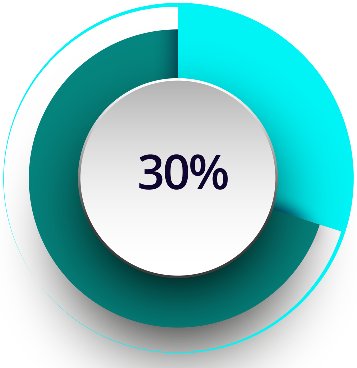
- Regulatory compliance is the first concern for many organizations, and therefore, a key area where future investments are likely to be directed (41%). Other areas of future investments include tools for IT and security data aggregation and analytics (38%), and a centralized cyber risk and compliance solution (30%).



Specific solutions to ensure regulatory compliance

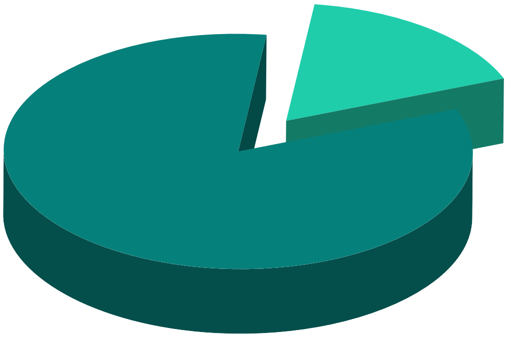


Tools for IT and security data aggregation and analytics



Centralized cyber risk and compliance solutions

- A majority of organizations still depend on basic office productivity software, knowledge management software, and point solutions for their cyber risk management requirements. The implementation of an integrated IT GRC solution is at low level across industries.



- Most respondents (45%) said that they changed their plans and approaches to cyber risk and compliance management and reprioritized their activities to contend with the pandemic-driven new operational landscape, while 33% of the participants said they deployed new tools and systems to enhance their efficiency.

45% Changed our plans, approaches to IT and cyber risk and compliance, reprioritized our activities

42% Increased scope of IT and Cyber Risk and Compliance Programs

33% Deployed new tools & systems to improve efficiency

20% No change in plans, approaches, and activities

4% Increased our team capacity

MAJOR PAIN POINTS FOR CYBERSECURITY PROFESSIONALS

Top IT and cyber risk and compliance challenges

The COVID-19 pandemic has undoubtedly impacted every organization irrespective of the industry. As work moved home—beyond the reach of the office firewall and enterprise security mechanism, the entire workforce became more susceptible to cyberattacks. As such, security teams are struggling to effectively manage the expanded attack surface and their organization's evolving cyber risk profile.

In this new normal, survey respondents identified lack of visibility on cyber risks across the enterprise, lack of automation in managing cyber risks and compliance, and limited security awareness as the top three IT and cyber risk and compliance challenges for their organizations (Fig.5).

The current remote working conditions and augmented digital interconnectedness of people, systems, processes, and organizations are likely to stay even after the crisis is over. The new paradigm has necessitated adopting a more matured cybersecurity framework—an integrated IT and cyber risk and compliance management solution which provides a holistic view of the risks, prioritizes risks and response strategies, and ensures involvement of the frontline in the cyber risk management strategy.

How a Global Retailer Manages Cybersecurity Risks through an Integrated Approach

Faced with amplified security risks associated with thousands of customers and third-party vendors, a global retailer tapped MetricStream to build an effective cybersecurity program that would meet their business objectives and customer demands. The company adopted MetricStream's integrated GRC solution with capabilities for IT risk management, IT compliance management, and third-party management. With the implementation, the retailer has benefitted from improved visibility into IT and cyber risks, effective monitoring of third-party risks, efficient management of all compliance requirements related to Payment Card Industry Data Security Standard (PCI-DSS) and the Sarbanes Oxley Act (SOX), and has successfully reinforced its GRC journey.

Question: What are your organization’s top IT and cyber risk and compliance challenges?

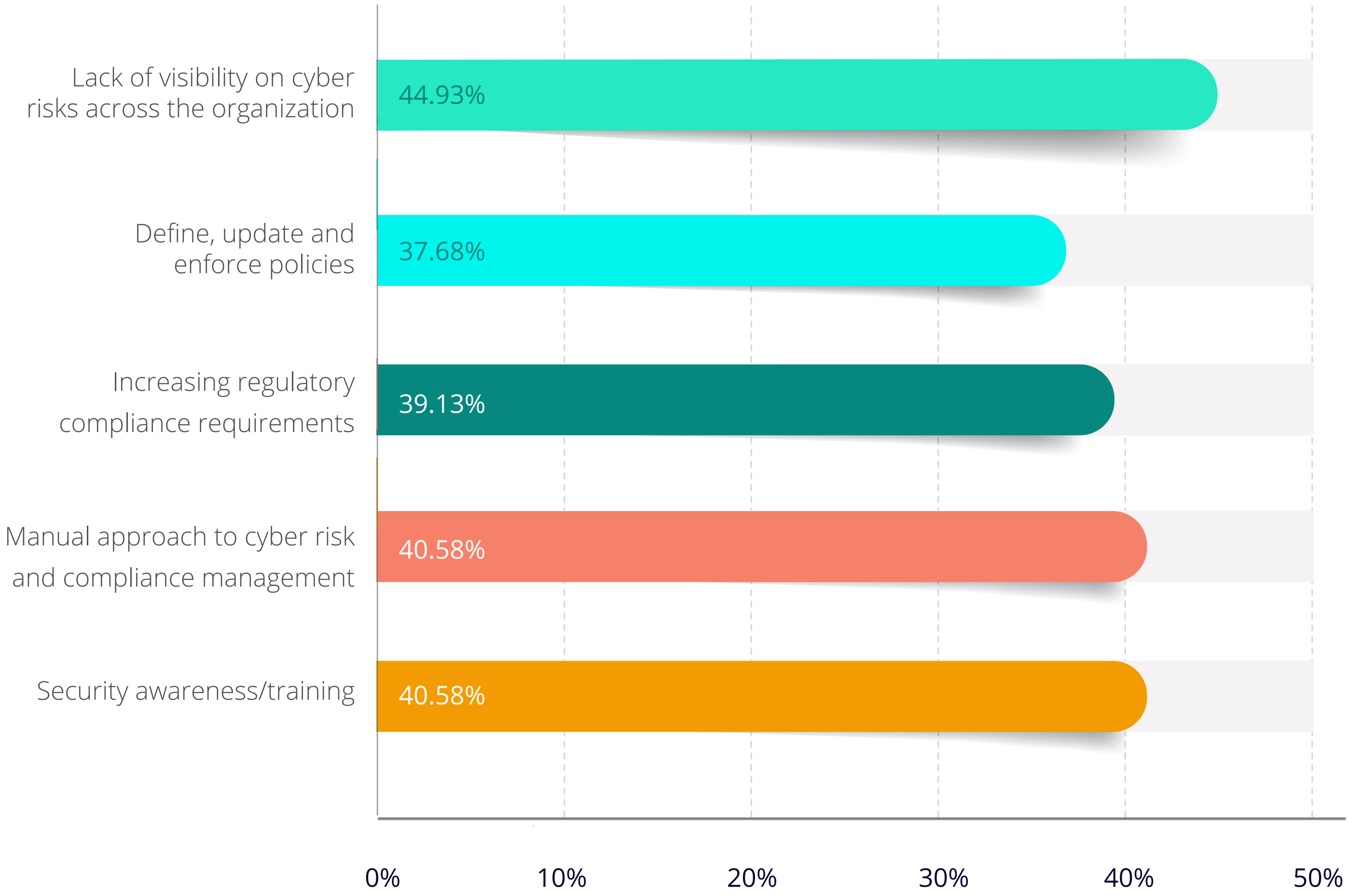


Figure 5: Top IT and cyber risk and compliance challenges

The surge in cyberattacks have prompted regulatory bodies to become more active and vigilant, resulting in a flurry of new regulations, regulatory updates, and guidelines -- the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and the Homeland Security Act in the United States, the General Data Protection Regulation (GDPR) and the European Banking Authority (EBA) Guidelines on ICT and security risk management in Europe, and many others.

Tracking these growing number of regulations and updates and ensuring compliance could be a formidable task for organizations of any size (39%). A technology-based solution that automates various associated activities, including tracking regulatory content, sending alerts to concerned business units, and mapping regulations and updates to existing policies, can greatly simplify IT compliance and regulations management in organizations.

Furthermore, in the current work-from-home setup, or rather work-from-anywhere, it is crucial to train the workforce on cybersecurity to protect against cyberattacks. In fact, human error is considered as the leading cause of cybersecurity breaches. Boosting employee awareness on latest cybersecurity trends and technologies, along with clarity on their roles, responsibilities, and accountabilities, can go a long way to protect organizational data and other critical and sensitive assets.

CURRENT IT AND CYBER RISK AND COMPLIANCE MANAGEMENT PRACTICES

Frequency of conducting risk and controls assessments

With the growing frequency and sophistication of cyberattacks, conducting risk and controls assessments can no longer be limited to a sporadic approach. Even a minor lapse in security controls can be exploited by bad actors, resulting in colossal losses in terms of fines and penalties, reputational damage, loss of trust of customers, or can even throw organizations out of business in extreme circumstances. Furthermore, recent incidents, such as security breaches at Microsoft and Accellion, and the SolarWinds hack, have highlighted how a security incident at one organization can affect several connected businesses in today's hyper-connected business environment.

A continuous approach to risk management and control assessment is an absolute necessity for thwarting cyberattacks. Our survey highlighted an interesting distribution in the frequency of risk and control assessment activities compared to last year. In 2020, the highest number of the respondents said that they conducted quarterly assessments while this year the highest number of the respondents (36%) said that they perform risk and control assessments on an ongoing basis (Fig.6). And the reason is very clear: the rapidly evolving cyber threat landscape has been exacerbated by the pandemic, providing low-hanging fruits for hackers. Organizations need to monitor their risk and controls on a continuous basis to ensure their preparedness for any security breach.

> *“Almost everything we do has some element of third-party in it whether we know it or not."*
>
> **- Sarah Dahlgren,**
> Head of Regulatory Relations - Corporate Risk, Wells Fargo & Company

Organizations are gradually adopting a continuous approach to conducting risk and controls assessments.

Of those organizations that conduct risk and controls assessments continuously, a majority (52%) are large organizations with more than 10,000 employees, followed by mid-sized organizations (36%). This suggests that larger organizations are adopting a more structured approach and setting up cadence for cyber risk management activities.

That said, a considerable number of organizations still have a traditional and periodic approach to risk and control assessment activities. However, given the rapidly evolving cyber realm and threat landscape, it is recommended to continuously monitor crown jewels to make sure that they are not compromised in case of of a breach

Question: How frequently does your organization conduct risk and controls assessments?

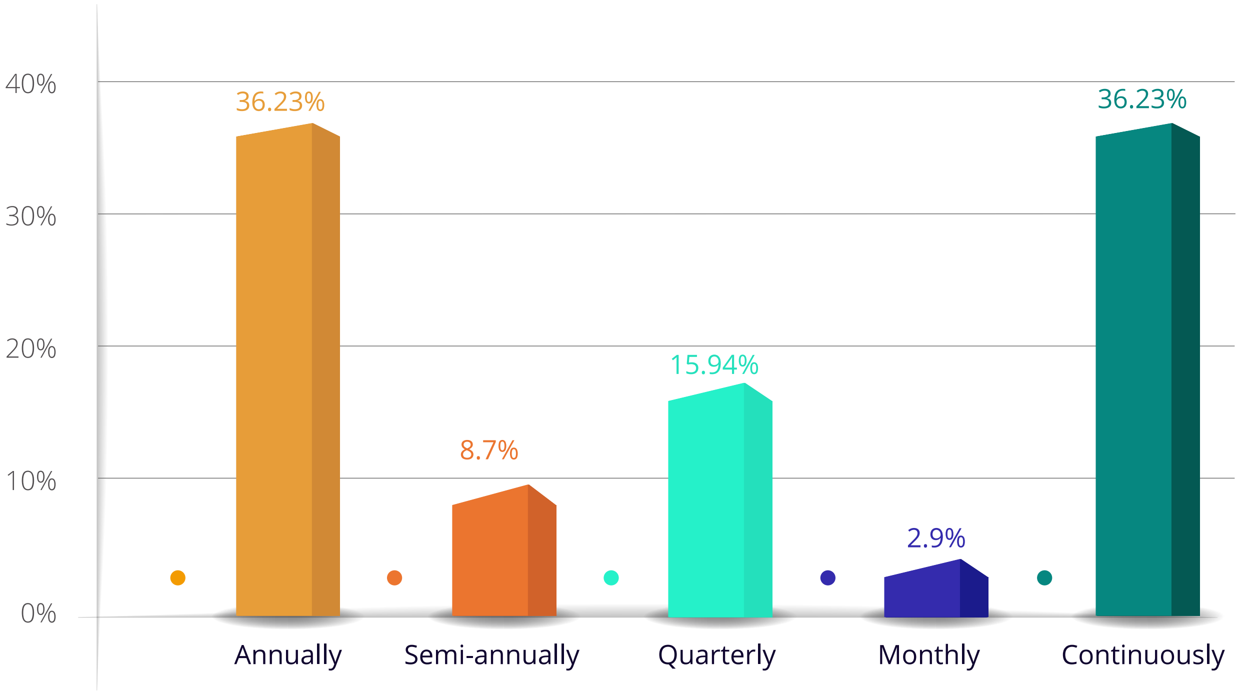


Figure 6: Frequency of conducting risk and controls assessments

Alignment of cyber risk and compliance program with the ERM program

Given the high interconnectedness of risks in this digital era, cyber risk and compliance management cannot be viewed in isolation from the overarching enterprise risk and compliance management program. Aligning cyber strategy with enterprise risk management (ERM) is vital for organizations to get buy-in from the management and achieve better return on their investments. Alignment, enforced through coordination and collaboration between these functions, can help strengthen an organization's cyber and business resilience.

In the survey, 28% of the respondents said that their organization's cyber risk and compliance program is fully aligned with the broader enterprise risk and compliance management programs (Fig.7). Of these, 37% said that they use an integrated solution for policy, risk, compliance and vendor management, such as an IT GRC solution.

> *"The cybersecurity function has to participate in ERM or ORM. There has to be a well-defined program, well-defined reports, and the toughest part – a common taxonomy."*
>
> **- Garrett Smiley,**
> CISO & VP of Information Security, Serco Inc

Question: How aligned is your cyber risk and compliance program with the overall enterprise risk and compliance management program?

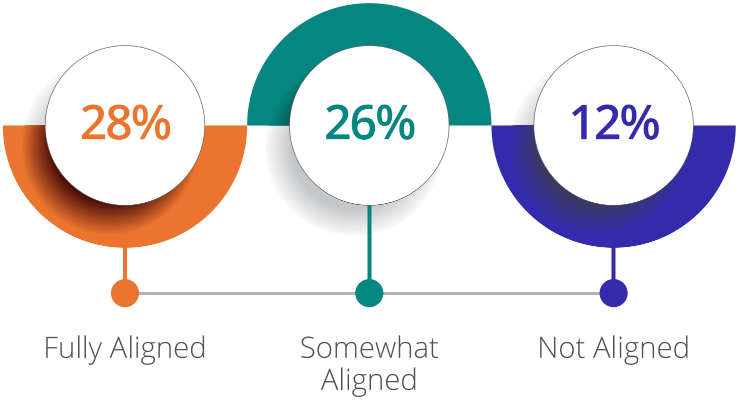


Figure 7: Alignment of cyber and ERM programs

IT and cyber risk and compliance management: Tools and technologies

The adoption of integrated IT GRC solutions by enterprises is at unsatisfactory level. Organizations still largely use spreadsheets and point solutions despite the inefficiencies associated with these traditional and manual tools.

In fact, in our interactions with organizations across industries, this is often cited as a major pain point. With different business units using their own spreadsheets, which consequently become a "isolated sources of truth", data aggregation and normalization becomes extremely difficult and time-consuming. This, in turn, obstructs an organization's risk visibility and foresight and hampers their understanding of risk relationships, thereby limiting their risk identification and mitigation capabilities.

In the survey, the highest number of the respondents (36%) said that they use basic office productivity software, including documents and spreadsheets, while 25% use knowledge management software and 21% use point solutions that are not integrated with risk and compliance systems (Fig.8). A meagre 17% said that they use one integrated solution for policy, risk, company, and third-party management.

How a Leading Sports Footwear and Apparel Company Eliminated the Use of Spreadsheets and Automated IT and Cyber Risk and Compliance Management

The global sports footwear and apparel company depended on manual processes and spreadsheets for managing IT and cyber risk and compliance. The approach limited their visibility into risks and the effectiveness of controls. The company deployed MetricStream GRC products including IT and Cyber Risk and IT and Cyber Compliance overcome these challenges. With MetricStream, they have digitally transformed their IT GRC system, making it faster, more agile, and scalable.Oxley Act (SOX), and has successfully reinforced its GRC journey.

Question: What software does your organization use for IT and cyber risk and compliance management?

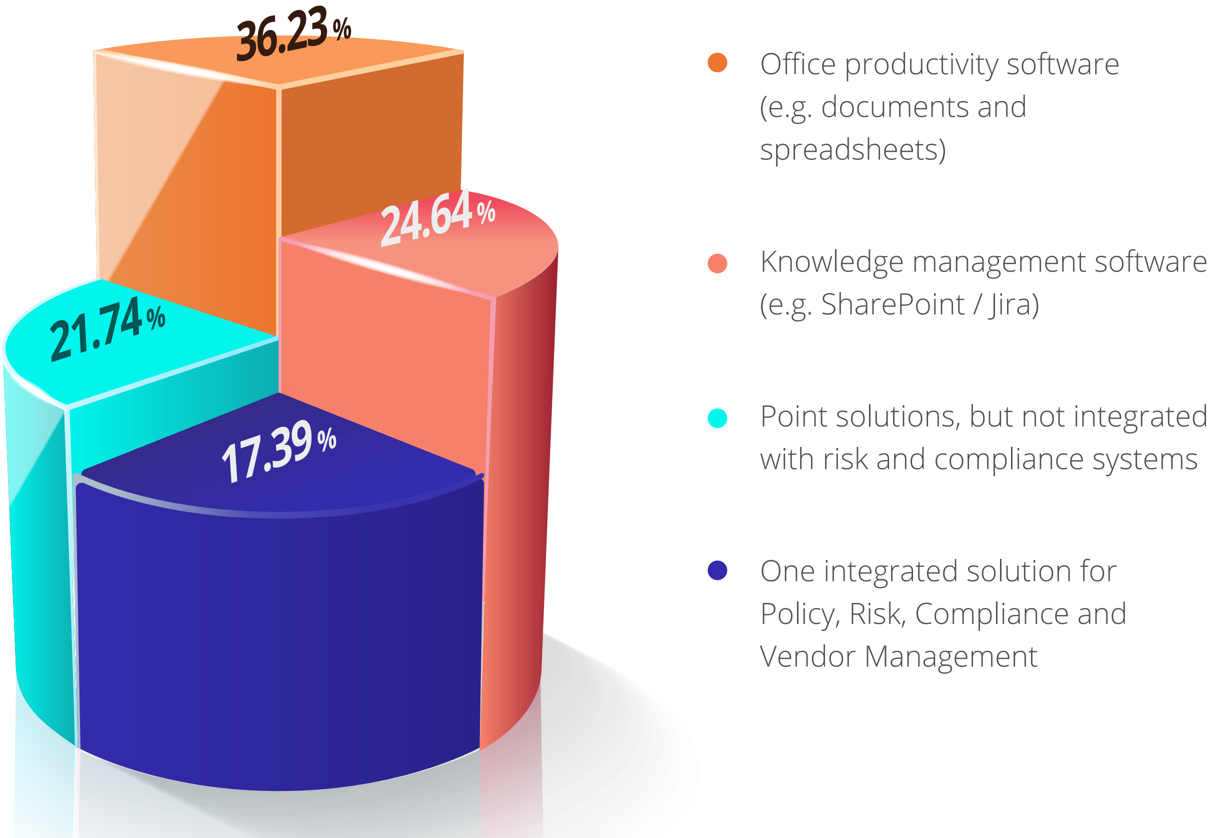


Figure 8: Tools and technologies

In fact, the implementation of an integrated IT GRC solution is at low level across all company sizes. It goes without saying that today decision-makers need faster and better risk visibility—which calls for an advanced, integrated, and automated IT GRC solution.

Adoption of IT GRC solutions is at unsatisfactory level.

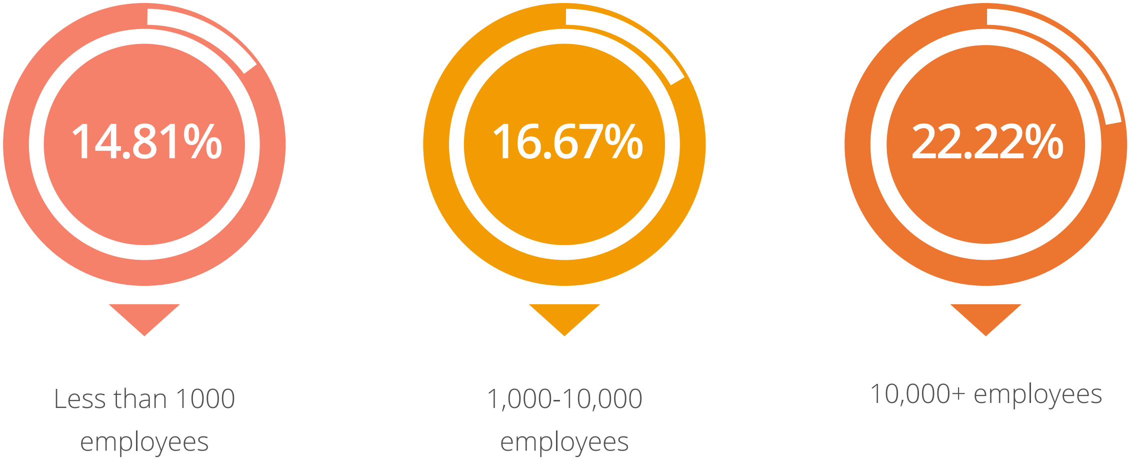


Figure 9: Implementation of an integrated IT GRC solution by company size

iv Current uses of IT and cyber risk management software

The survey highlighted a shift in the way organizations use IT and cyber risk management software. Earlier, organizations were mainly focused on avoiding security breaches and invested in technologies to identify and analyze cyber risks and have proper controls in place. However, now organizations are also increasingly focusing on other aspects related to cyber risk management, including risk rating for assets, risk prioritization, analytics and reporting, and more, and invest their effort accordingly (Fig.10).

As per the survey, identification and assessment of IT and cyber risks emerged as the top use (65%) of IT and cyber risk management software by organizations, followed by achieving a centralized system to manage processes, assets, risks, and controls (49%), and assigning risk rating for assets (46%).

Cyber risk identification and assessment is the predominant use of IT and cyber risk management software.

Question: In what ways does your organization use the software?

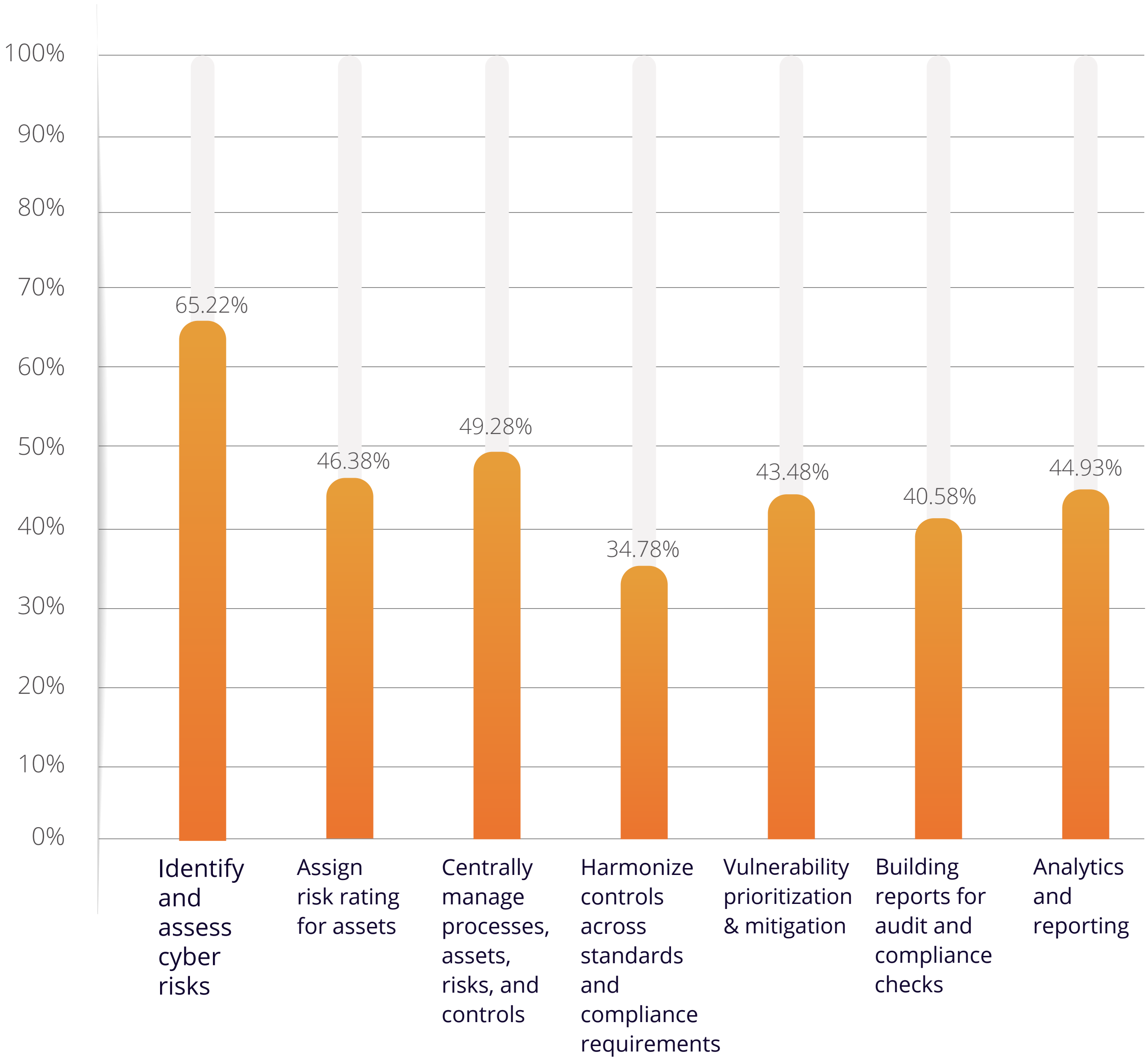


Figure 10: Top uses of IT and cyber risk management software

IMPACT OF COVID-19

As the business and operational landscape underwent a major transformation due to the pandemic, organizations rushed to industry 4.0 technologies, such as cloud computing, artificial intelligence, and the Internet of Things, to navigate these unchartered territories. The sudden shift to working from home beyond office firewalls, coupled with a pivot towards digital business model in a hurried manner, became a lucrative target for cyber adversaries to capitalize on.

Accordingly, organizations identified the need to revamp their cyber strategies to ward off cyberattacks. Most of our survey respondents (45%) said that they changed their plans and approaches to cyber risk and compliance management and reprioritized their activities, while 33% of the participants said they deployed new tools and systems to enhance their efficiency (Fig.11).

A considerable number of the respondents (42%) believe that pandemic has increased the scope of IT and cyber risk and compliance programs. The cyber risks and compliance requirements associated with the new working conditions can no longer be dealt with effectively with a siloed and manual approach. The onus has fallen on the security teams to convince the executive management and board to adopt an IT GRC solution that is aligned with the overall ERM program, boost employee awareness on cybersecurity measures and threats such as malware (worms, spyware, adware, computer viruses, etc.), phishing emails, etc., assess cybersecurity risk exposure and effectiveness of controls on an ongoing basis, and more.

Only 20% of the respondents said that they did not change their plans, approaches, and activities related to cyber risk and compliance management.

Only a few organizations did not alter their cyber strategy in the wake of the pandemic.

Question: How has Covid-19 impacted your organization?

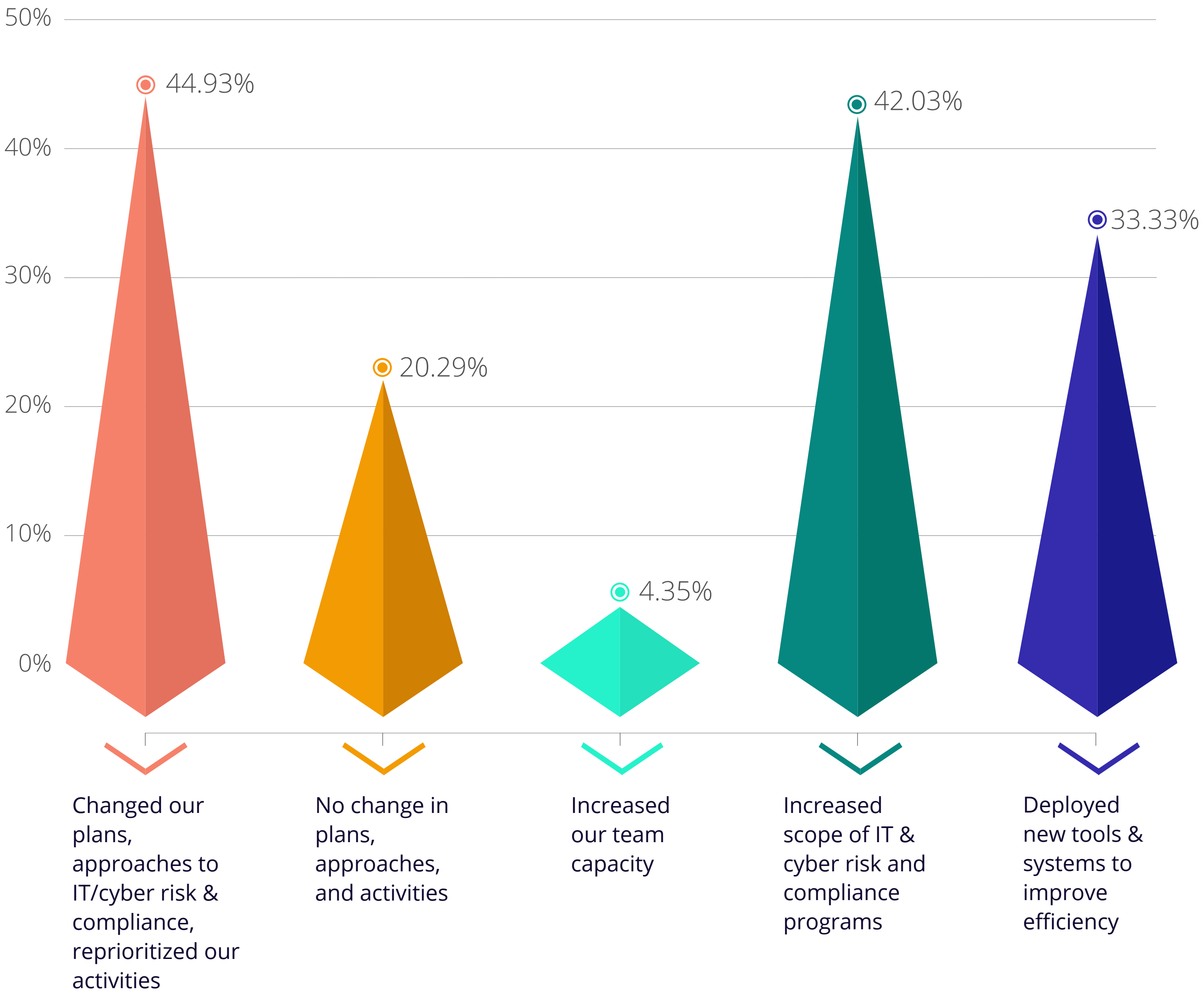


Figure 11: Impact of COVID-19 on IT and cyber risk and compliance management approach

CISO:
A BUSINESS IMPERATIVE

Growing awareness of CISO's role

Organizations are increasingly realizing the need to have a dedicated Chief Information Security Officer (CISO) to take care of their security needs. Previously, the responsibility fell on Chief Information Officer (CIO) or Chief Technology Officer (CTO). However, with the evolution of the cyber risk and regulatory landscape, it has become imperative to have a dedicated executive who safeguards the data stored, mitigates cybersecurity threats, ensures compliance with IT regulations, standards, and policies, and reports to the board on existing and emerging risks, challenges, and opportunities.

In the survey, 39% of the respondents said that their organizations have CISOs in place to overlook IT and Cyber Risk and IT Compliance Management (Fig.12). This shows an improvement compared to the previous year, where only 29% of the respondents said that their IT and cyber risk program rolls up to the CISO.

Still, 43% of organizations depend on CIOs, CTOs, and Chief Risk officers (CROs) for this job and don't have a dedicated CISO to manage their IT and cyber risk and compliance program.

> The CISOs of tomorrow will need to gain sustained support and focus from the top management if they want to succeed in their cyber-fortification efforts. They will also need to ensure that cybersecurity strategies are evolving in line with the business and its wider financial and strategic objectives. The most critical question is not 'are we doing enough today,' but rather, 'are we thinking enough about tomorrow?'
>
> - Towards A More Secure Cloud: Five Areas Of Focus For The CISO

Question: Who is responsible for the overall IT and cyber risk and compliance management in your organization?

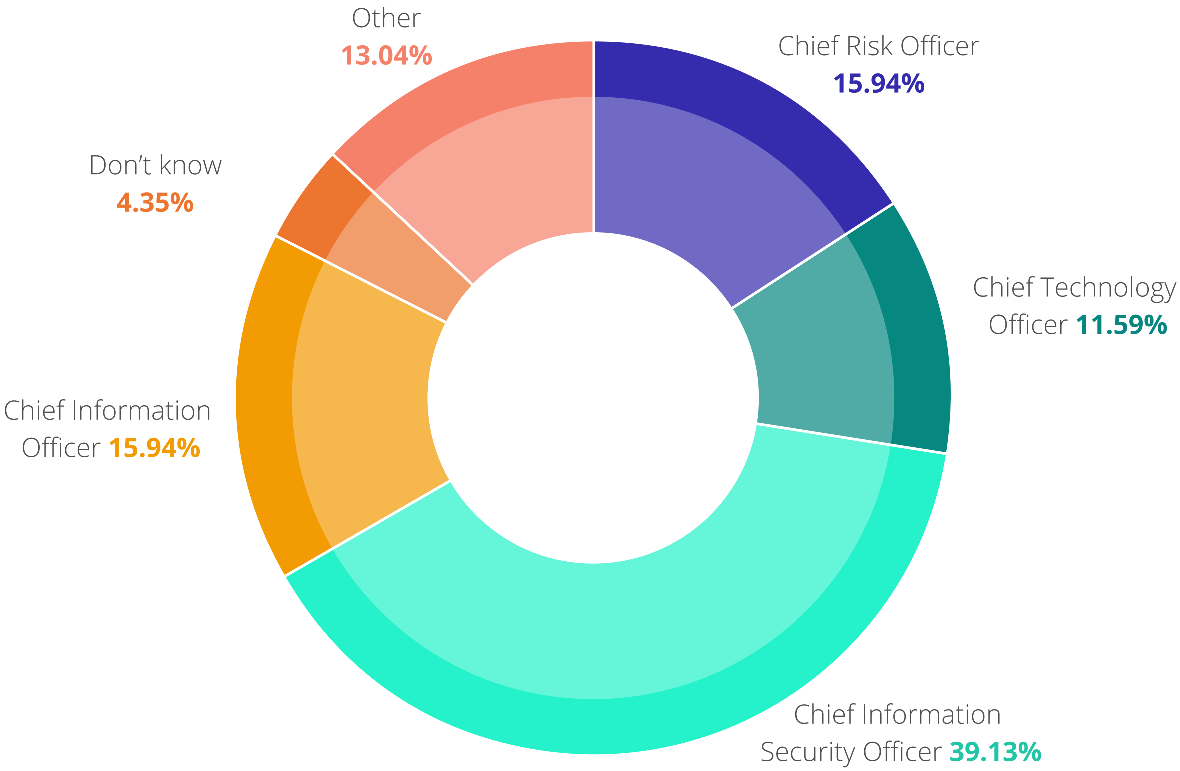


Figure 12: Executive responsible for overall IT and cyber risk and compliance management

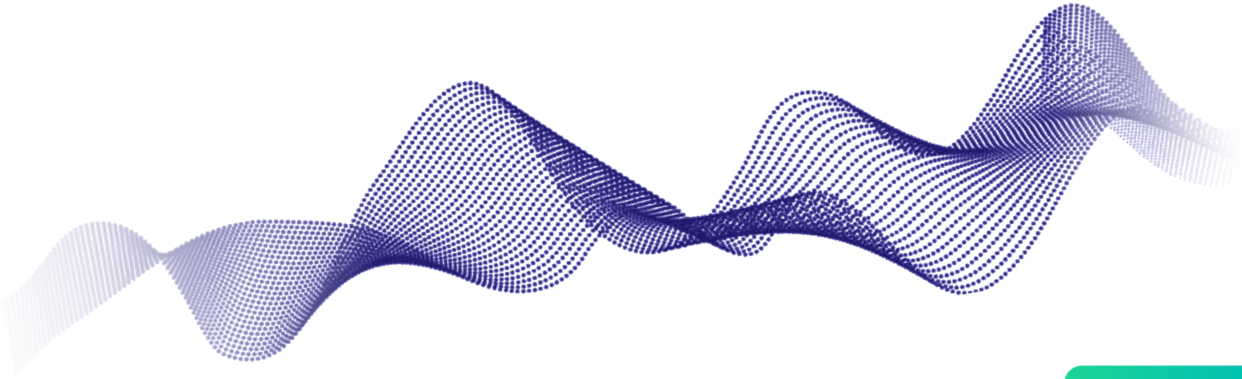
LOOKING AHEAD INTO 2021

Top IT and cyber risk priorities in 2021

Addressing the top challenge as identified in the survey – lack of visibility on cyber risks across the organization – has been cited as the top priority for this year by a majority of the respondents (55%). It is followed by continuous monitoring of IT and cyber controls (48%) and harmonizing and rationalizing controls across standards and compliance requirements (41%). (Fig.13)

In today's fast-paced operational environment, quick and comprehensive access to risk information is critical to ensuring well-timed mitigation and remediation measures. Organizations can leverage integrated and technology-based IT GRC solutions, which provide real-time visibility of risk and compliance posture, facilitate continuous monitoring of IT and cyber controls, offer aggregated risk view to the executive management and board, simplify cyber risk quantification for better prioritization, and more.

The top cyber risk priorities can be met by implementing IT GRC solutions.



Question: What are your organizations top IT and cyber risk priorities in 2021?

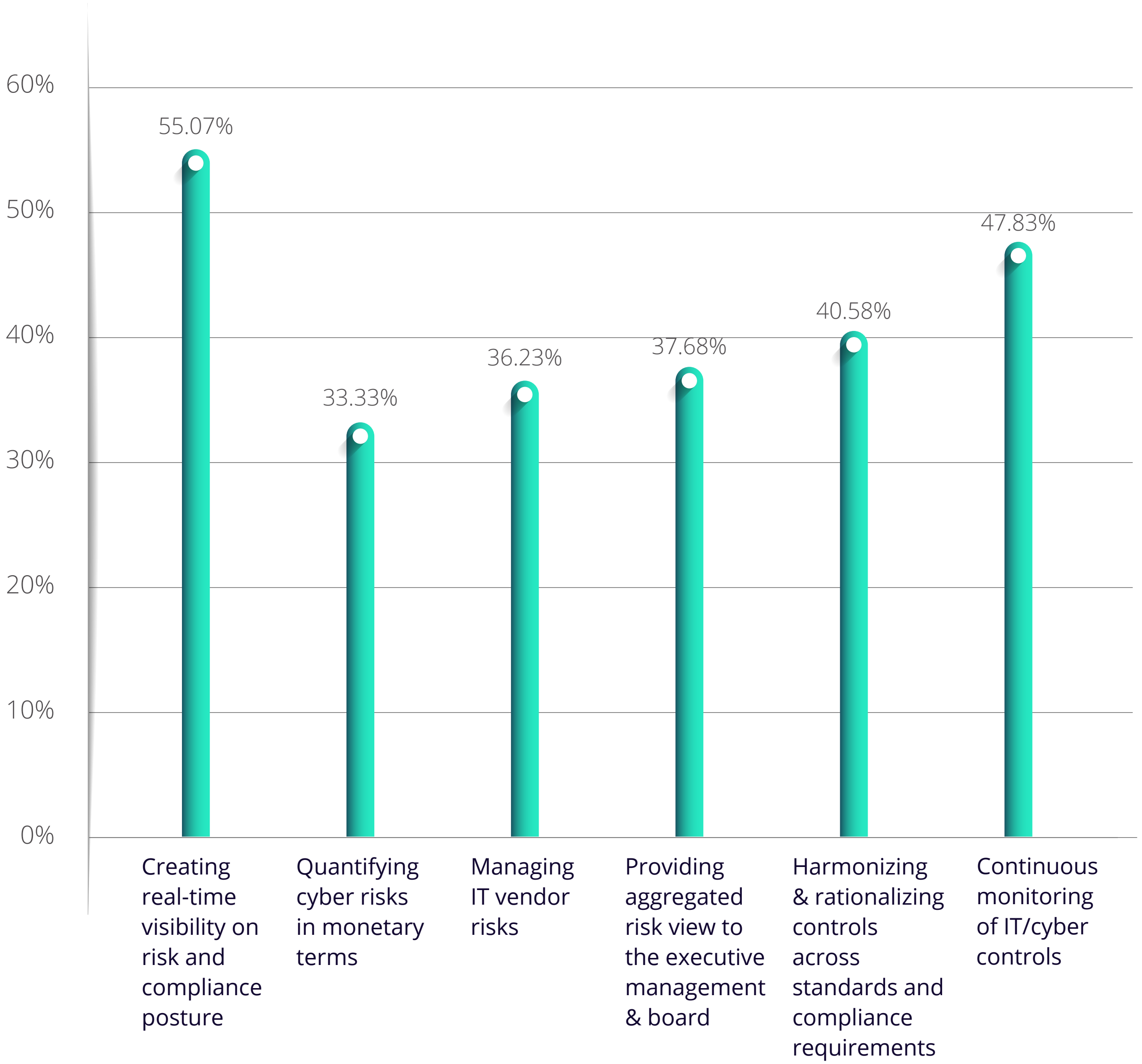


Figure 13: Top IT and cyber risk priorities

Future areas of investment

Going forward, regulatory compliance is going to be a key area for organizations to invest in. 41% of the respondents said that they are going to implement specific solutions in FY 2021 to ensure compliance with regulatory requirements and standards (Fig.14). This is a good sign as ensuring compliance is the first step to achieve confidence with auditors, regulators, and customers.

38% of the respondents said that they are looking to adopt tools for IT and security data aggregation and analytics, while 30% of the respondents said that they are interested in implementing a centralized cyber risk and compliance solution. This suggests a growing awareness in organizations to switch to automated and centralized solutions for ensuring an efficient and robust approach to IT and cyber risk and compliance management.

"Develop a trusted relationship with regulators – when things start to escalate – it's good to have a pre-existing relationship."

- Jordan Rosenfeld,
Global Chief Compliance Officer, Mercer

Question: Where does your organization plan to invest?

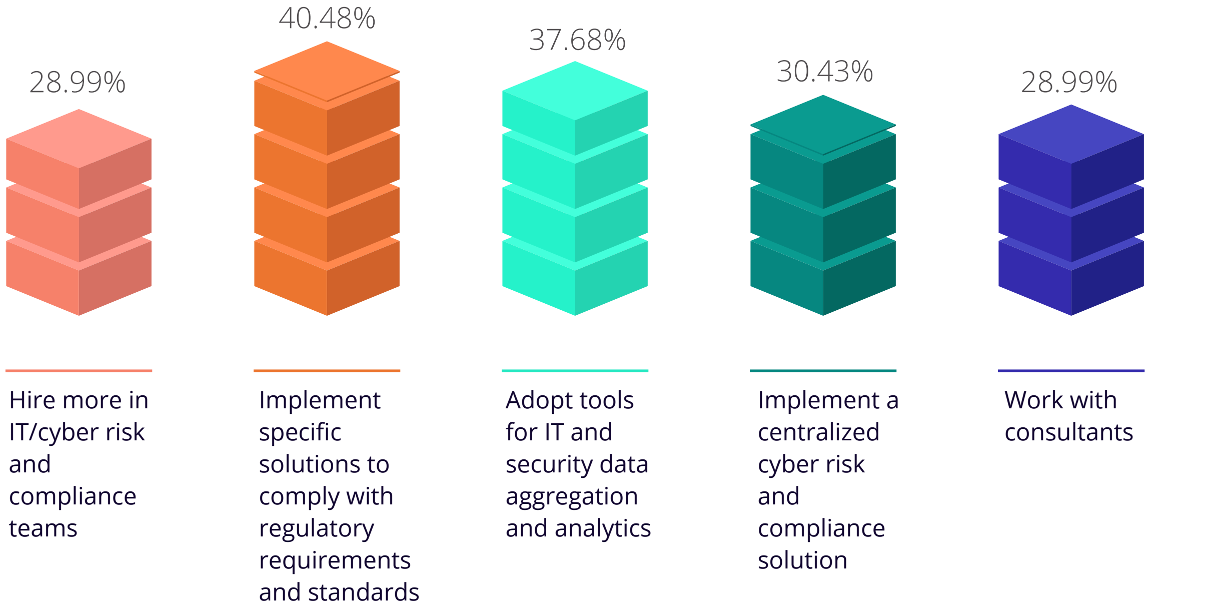


Figure 14: Areas of future investment

CONCLUSION

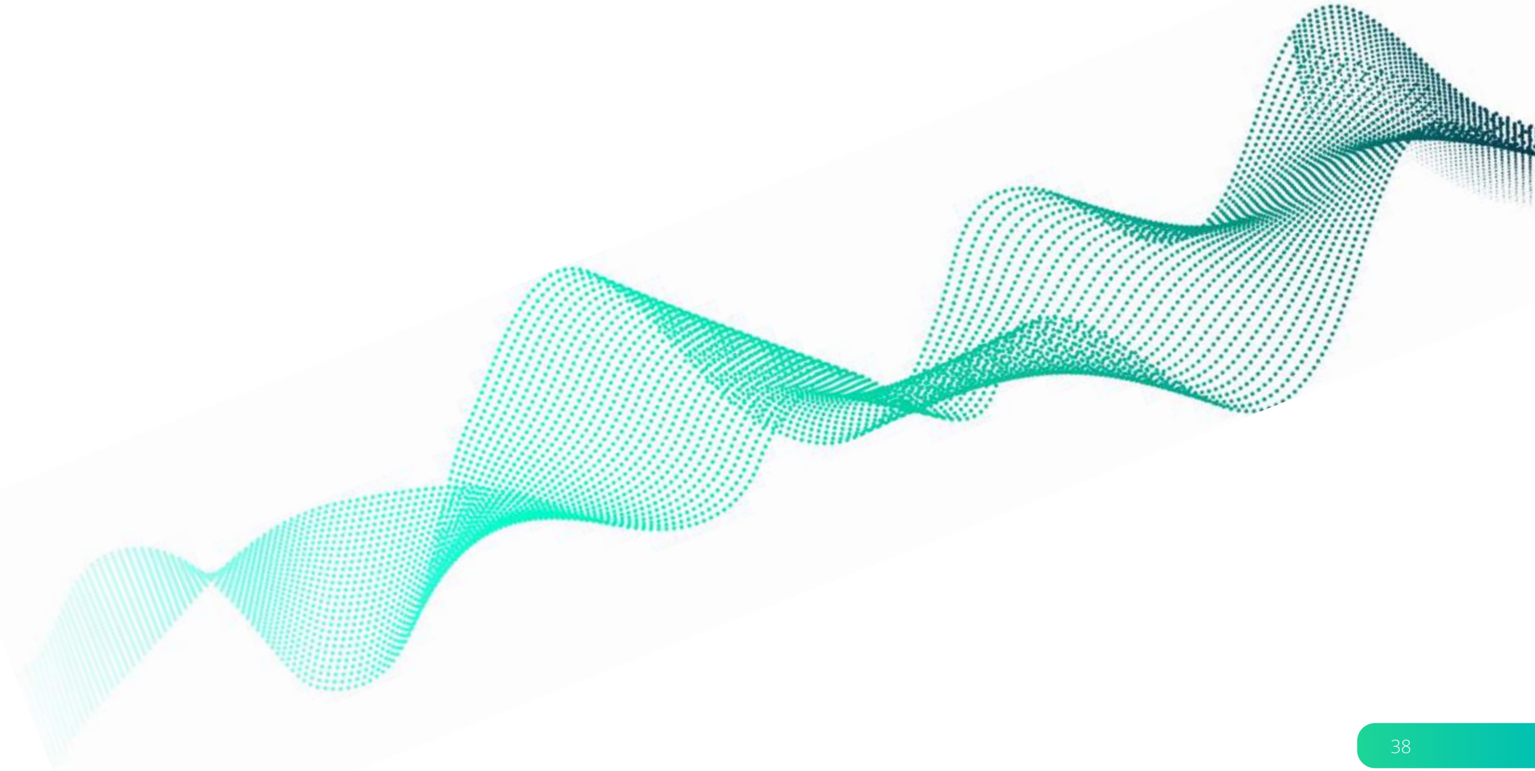
A stable and sound IT environment is a key enabler of innovation in products and services and business in general. As organizations are increasingly going digital and becoming data-dependent and interconnected, cyber risk has moved up the priority list and taken the center stage in boardroom discussions. The pandemic has only exacerbated the threats and the business disruption that has ensued has caught the attention of cybercriminals to exploit the vulnerabilities. In these turbulent times, ensuring robust cyber defense infrastructure to protect critical assets is of paramount importance.

Although a considerable number of organizations currently have an inefficient and manual approach to cyber risk and compliance management, it is encouraging to see that switching to digitized and centralized GRC solutions is among their top priorities this year. These solutions can help improve risk visibility and foresight, facilitate continuous monitoring of IT and cyber controls, and streamline overall cyber risk and compliance management. Innovative features, such as support for mobility, real-time reporting, advanced risk analytics, regulatory notifications, and more, further assist executive management and board in quick and efficient decision-making.

While adopting IT GRC solutions is crucial in today's digital era, organizations can become over-dependent on tools and technologies and overlook the importance of well-governed processes and people with the right expertise. This was reflected in the survey as a majority of organizations still depend on CIOs, CTOs, and CROs to manage their IT and cyber risk and compliance programs instead of a CISO. That said, there is an improvement in the numbers compared to last year, suggesting a growing awareness of organizations to have a dedicated CISO in place.

The survey also highlighted that a number of organizations had to alter their cyber strategy and implement new tools and systems in the wake of the pandemic. The underlying reasons could be evolving organizational risk profile due to the crisis and inefficiencies of existing systems and approaches to tackle emerging risks.

Having said all that, the ultimate goal isn't to avoid cyber risk but rather transforming it into strategic advantage—because things can and will inevitably go wrong at some point. But if organizations build their cyber resilience—the ability to not just prevent cyberattacks but also minimizing the impact of security incidents and ensuring continued business operations in the aftermath of attacks—that's when they can truly thrive and create business value.



CONTACT US | REQUEST A DEMO

Email: info@metricstream.com

metricstream