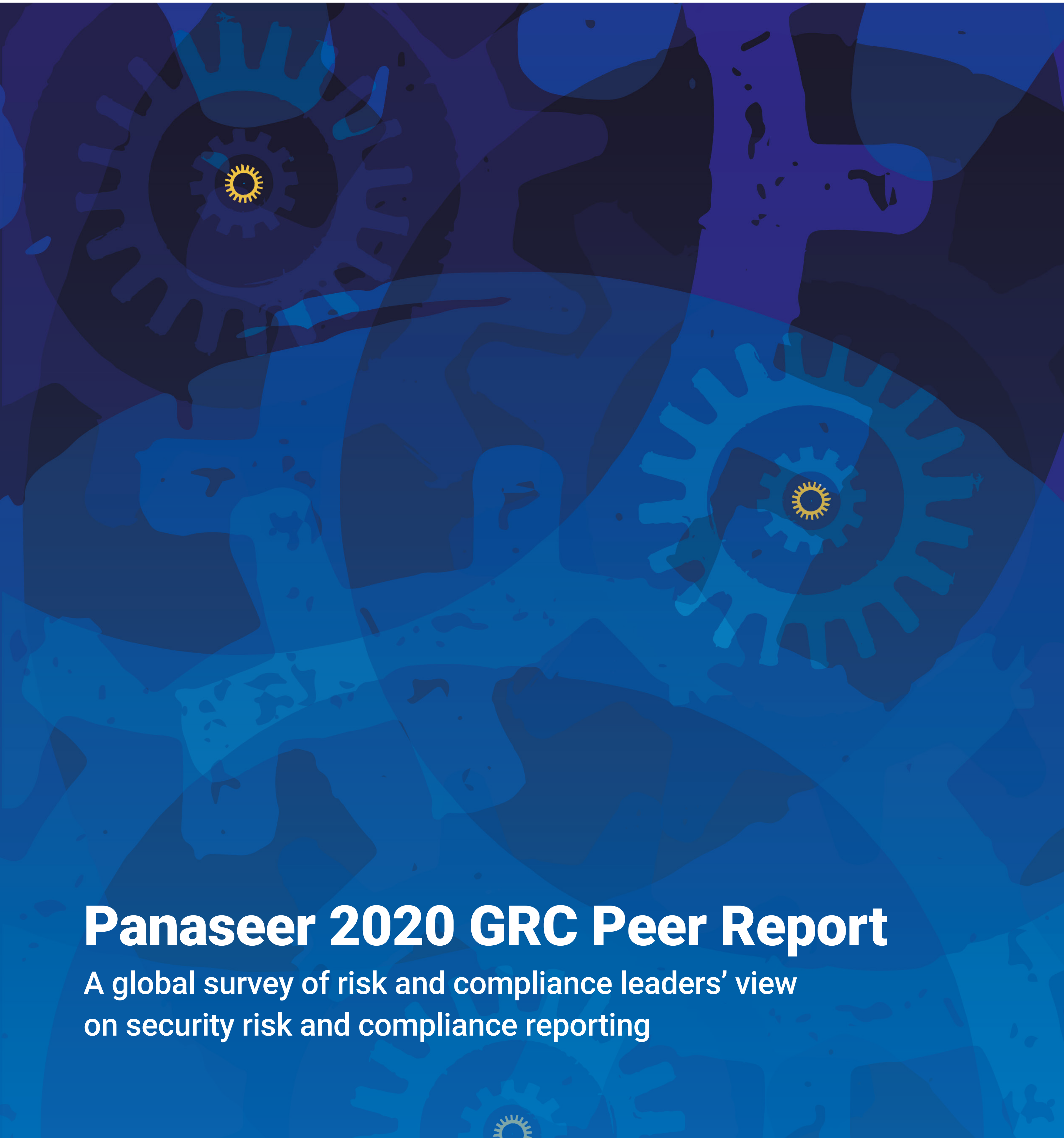
panaseer



Panaseer 2020 GRC Peer Report

A global survey of risk and compliance leaders' view on security risk and compliance reporting

Contents

SECTION 1:

Executive summary

Regulators have always wielded significant influence on the banking and financial services industries. They are heavily regulated for good reason: the entire financial system is at stake, underpinning the whole economy and the livelihoods of individuals, families, small businesses, major corporations and nation state finances.

In today's digital age where data privacy and cybersecurity loom large on the priority list of management boards, information requests from regulators can arrive suddenly and with great urgency. The institutions in question may very well be secure and following published guidelines and procedures but being able to prove as much – and their compliance with applicable laws and regulations – is a different matter entirely.

Panaseer has commissioned a study into the precise point of interaction between large (5,000 employees and over) financial businesses and the regulators who regularly demand answers to fundamental, complex and scrutinising questions.

The results suggest that the people in charge of risk and compliance at these organisations are frequently unsure if they are giving the right security data to regulators and auditors. In many cases, the banks and finance houses may be handing over information likely to be incomplete, out of date or based upon a subjective belief or representative sample of the truth. Often, even if the information can be held reliable, it will be produced later than desired and as a result of significant manual effort rather than a robust, automated process.

The implications of this are substantial. If GRC (governance, risk and compliance) leaders don't have confidence in the accuracy and timeliness of security data provided to regulators, then the same holds true for the confidence in their own ability to understand and combat cyber risks. Let that sink in for a moment. The definition of risk is 'exposure to danger', so if the path to identifying risk is flawed, then this exposure cannot be measured or mitigated, and you are ultimately left with a 'risky' risk management programme.

Put another way, if GRC teams do not have confidence in the data to communicate cyber risk externally, then they equally cannot manage the cyber risk internally and the very foundations of risk management are undermined.

For regulators, the whole concept of upholding compliance standards is based upon the assumption that the information provided to them is correct. And when this assumption becomes suspect, regulators are left with the 'nuclear' option of requesting a comprehensive audit.

If the prospect of being audited strikes fear into the heart of your GRC leaders, perhaps it's time to consider if their toolkit is fit for purpose. The results of this survey will help inform a fresh perspective on whether traditional GRC tools are sufficient to address tougher, time-bound questions asked by regulators. Or at least, whether they are sufficient on their own.

These issues are encouraging GRC teams to look for solutions that are driven by data in new, more comprehensive and contextual ways. The promise of any data-driven tool is its ability to make sense of it all; the same innocently simple intent that lies behind every regulatory request. What's needed is a single source of truth, continuously aware if security controls across the organisation are operating within internal policies (informed by different regulations and the organisation's risk appetite) and able to identify assets and controls that are non-compliant (especially those associated with business-critical processes), initiate remediation to mitigate risk, report on security posture in near real time and access these reports via self-service.

The widespread absence of such a capability has led to the emergence of a market category – Continuous Controls Monitoring (CCM) – that **Gartner now recognises and defines as a valuable asset in enterprise risk management strategy[1].**

This study examines the value of key functions from a CCM solution to draw conclusions about how much of a game-changer senior risk and compliance professionals think it could be.

Foreword

The fundamental foundation from which a company can build an effective, risk-based cybersecurity programme is instant access to trustworthy data.

This information must be easily available for two key reasons. First, to respond to regulators, who have a crucial role to play in maintaining industry standards and protecting consumer interests. Equally, to protect and strengthen the cybersecurity posture of the organisation itself.

This report from Panaseer provides invaluable insight for GRC leaders, giving evidence for the need to enable a new level of automation. Crucially, it outlines a solution, with details on an emerging category of security and risk, Continuous Controls Monitoring, which has just been recognised in the 2020 Gartner Risk Management Hype Cycle. With this capability GRC leaders can ensure that they comply with regulatory demands and demonstrate that compliance to all stakeholders.

By Andreas Wuchner, renowned Information Security, IT Security and IT Risk Management leader and Panaseer Advisory Board member

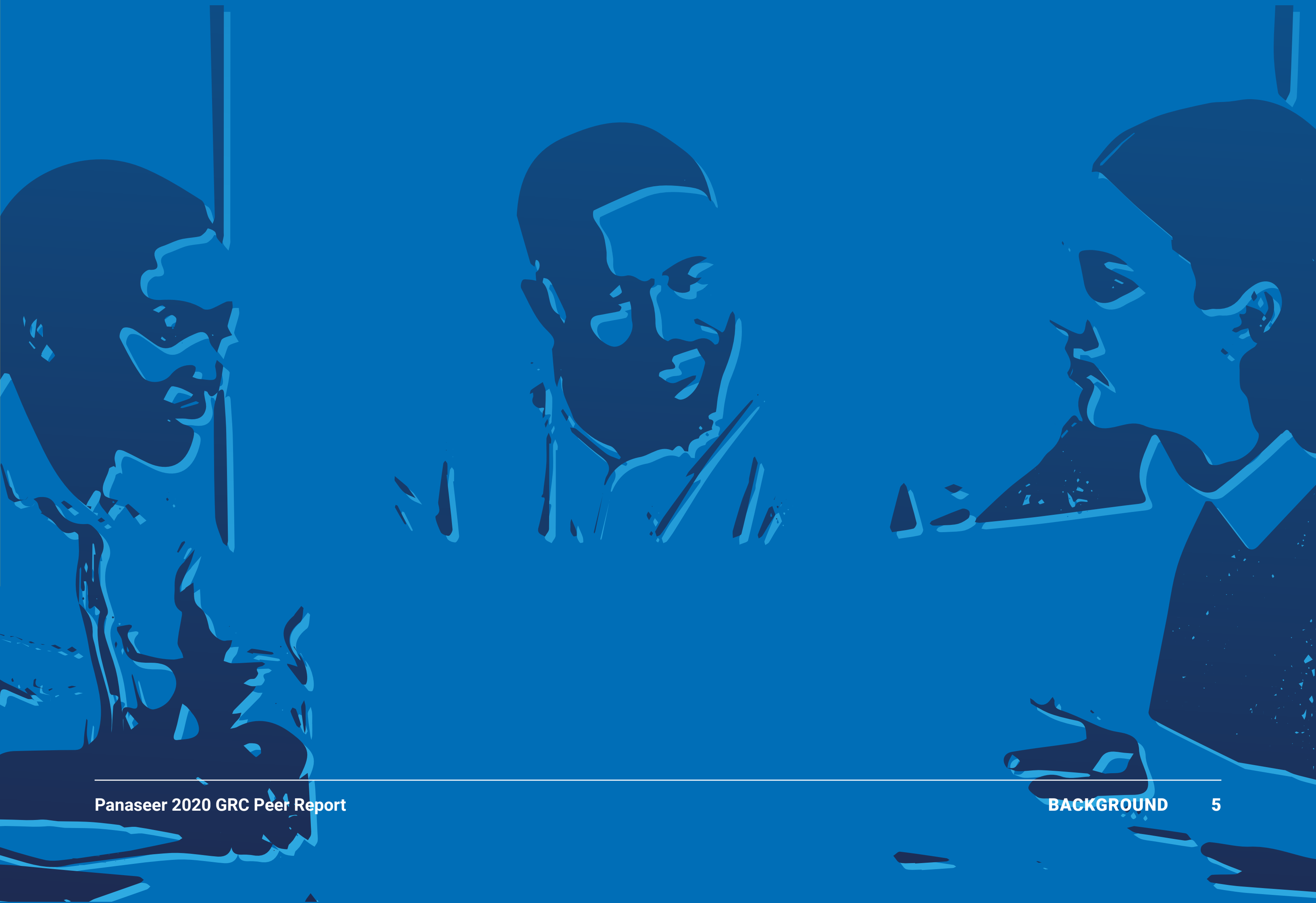
[1] Hype Cycle for Risk Management, 2020, Gartner, July 2020

SECTION 2:

Background

In April 2020, Panaseer commissioned an extensive survey of 200 senior (C-level/VP or equivalent) risk and compliance professionals working at large (5,000+ employees) financial services companies in the US and UK. **57.5%** of those questioned are Chief Compliance Officers, VPs of Compliance or Heads of Compliance. **22.5%** are Chief Risk Officers of VPs of Risk. The remaining **20%** are VPs of GRC or Directors of Cybersecurity GRC. The survey exercise was carried out anonymously on behalf of Panaseer by Censuswide.

This document principally details the key findings from this survey study. Other recent research projects cited in this paper are in the public domain.



SECTION 3:

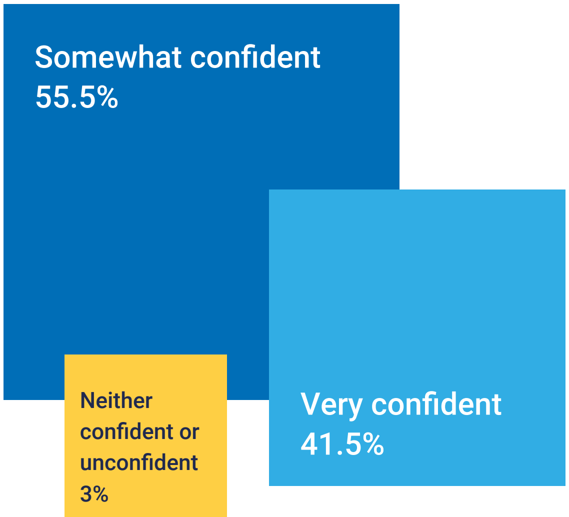
Findings

GRC teams have a number of challenges meeting regulatory demands

GRC teams are under increasing pressure to produce regulatory evidence at speed and scale. For example, the number of jurisdictions with data privacy laws continues to rise (120 countries as of 2020, plus cross-border protocols such as GDPR), as does the depth and coverage of other specific regulatory requirements.

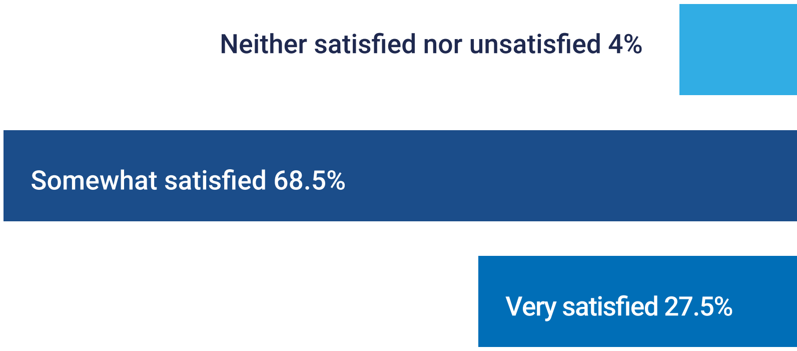
Major financial sector corporations are among the most well-resourced and technologically advanced organisations in the world, fully accustomed to the realities of coping with regulatory frameworks. But, far less than half (**41%**) of the most senior risk and compliance professionals at these businesses sampled in our research were 'very confident' in their ability to fulfil the security-related requests of regulators in a timely manner.

The level of confidence in fulfilling security related requests of a regulator in a timely manner



Organisations must ensure the ongoing confidence of regulators in their capacity to provide evidence on request. This in turn rests not only on timing but also accuracy. Worryingly, barely over a quarter (**27.5%**) of respondents were 'very satisfied' that their organisation's security reports align to regulatory compliance needs like GDPR and CCPA.

The level of satisfaction with how organisation's security reports align to regulatory compliance needs



Clearly something is not right, and the most logical cause is the lack of performance and currency of widely used GRC tools.

Traditional GRC tools were not designed for current challenges

Behind the specificity of every request from a regulatory authority is the core objective of ascertaining the organisation's true security posture. But standard GRC tools do not provide complete insight into the current status of security controls coverage, performance and importantly, gaps in controls coverage.

The lack of consolidated visibility into all assets, such as devices, applications, people, accounts and databases, across the enterprise make it hard for GRC teams to pinpoint control coverage gaps and external regulatory policy compliance.

Compounding this is the issue of incomplete or unreliable information as to whether the relevant controls are deployed and operating on all assets.

The answers to regulators' questions lie in data scattered across the organisation. Typically, the way this is gathered by GRC teams is subjective; collated via qualitative rather than quantitative questionnaires that build an approximated picture from representative samples rather than reflecting the undeniable truth. With GRC teams overstretched, and let down by their existing toolsets, such an approach is understandable, if suboptimal.

Qualitative questionnaires are manually intensive and may not reflect true technology risk compared to quantitative data pulled directly from controls, but the latter arguably requires an even greater and sustained manual effort adding to heavy workloads and resulting in errors and bias.

Aside from manual constraints, standard GRC scanning tools even struggle with auditing assets that are offline. Some organisations use asset discovery tools to populate GRC and there is a possibility that these tools might miss some assets if the firewalls block the asset discovery tool's scanners. These challenges make it difficult to accurately report on-the-ground status.

In our study, 92% of senior risk and compliance professionals responded positively to the value of harnessing both quantitative and qualitative security controls assurance, reflecting the strong appetite for an improved toolset.

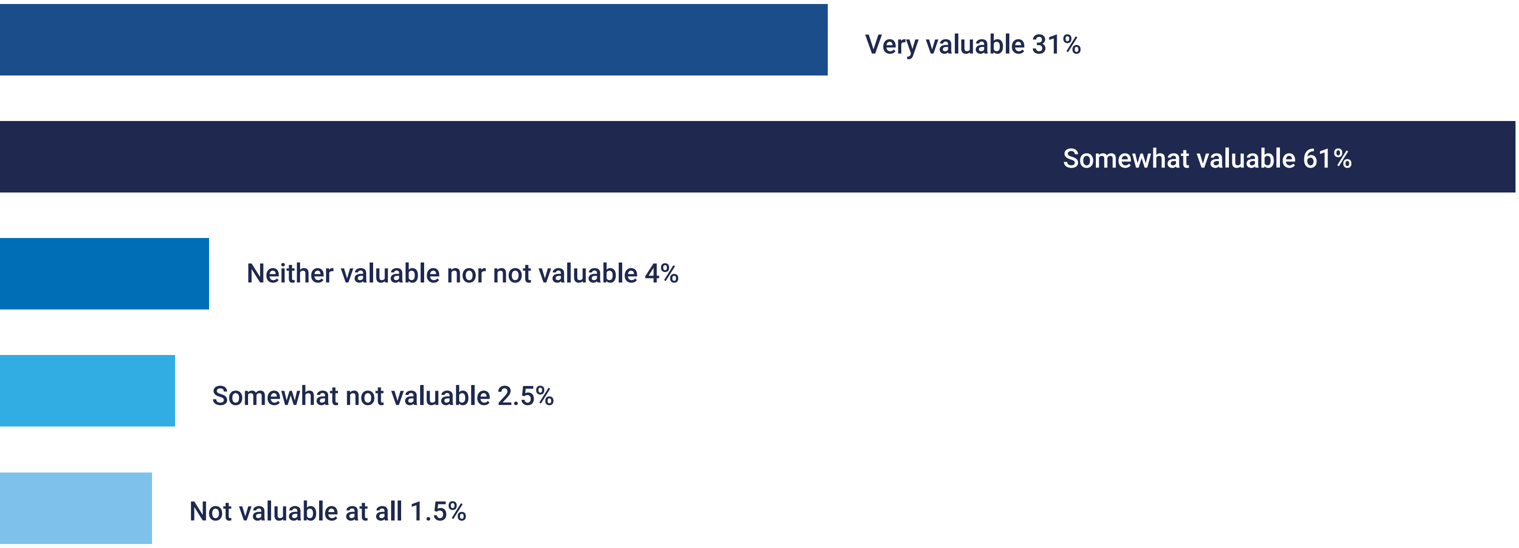
53% stated the measure would be 'very valuable' compared to **33%** across the whole survey base.

GRC tools are not designed for quantitative assessment. Therefore, when there is a need to substantiate regulatory compliance with quantitative data, much of the manual work is often outsourced to security operations teams to pick up the slack.

In another Panaseer study commissioned earlier this year[2], CISOs and other security leaders at large financial institutions reported GRC teams requesting metrics from security on average once every 16 days, consuming upwards of 5 days per month of valuable cyber fighting resource.

[2] Panaseer 2020 Financial Services Security Metrics Report, May 2020

How valuable is it to have quantitative security controls assurance reporting?



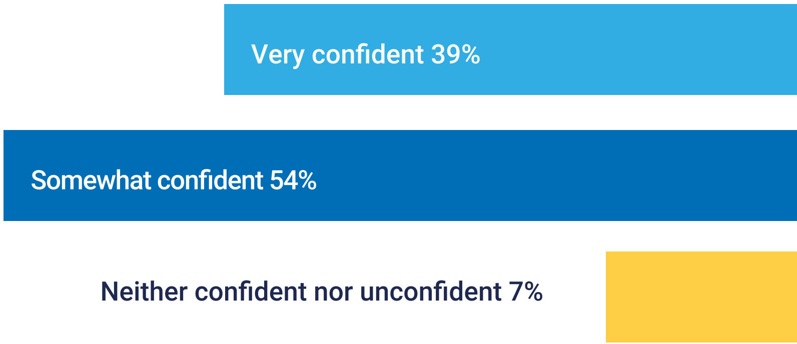
Without addressing these manual processes with a better, more complete and automated set of qualitative and quantitative measures, traditional GRC tools will continue to lack the ability to provide the necessary continuous monitoring and controls assurance for proactive and ongoing risk identification, prioritisation and remediation.

GRC teams face significant issues with data accuracy and request overload

At the heart of regulatory requests is what appears to be a straightforward demand: “tell us what we don’t know about your organisation.” And yet dealing with the frequency of requests from multiple quarters, in the context of highly complex technology estates and with acceptable levels of data accuracy, is far from simple.

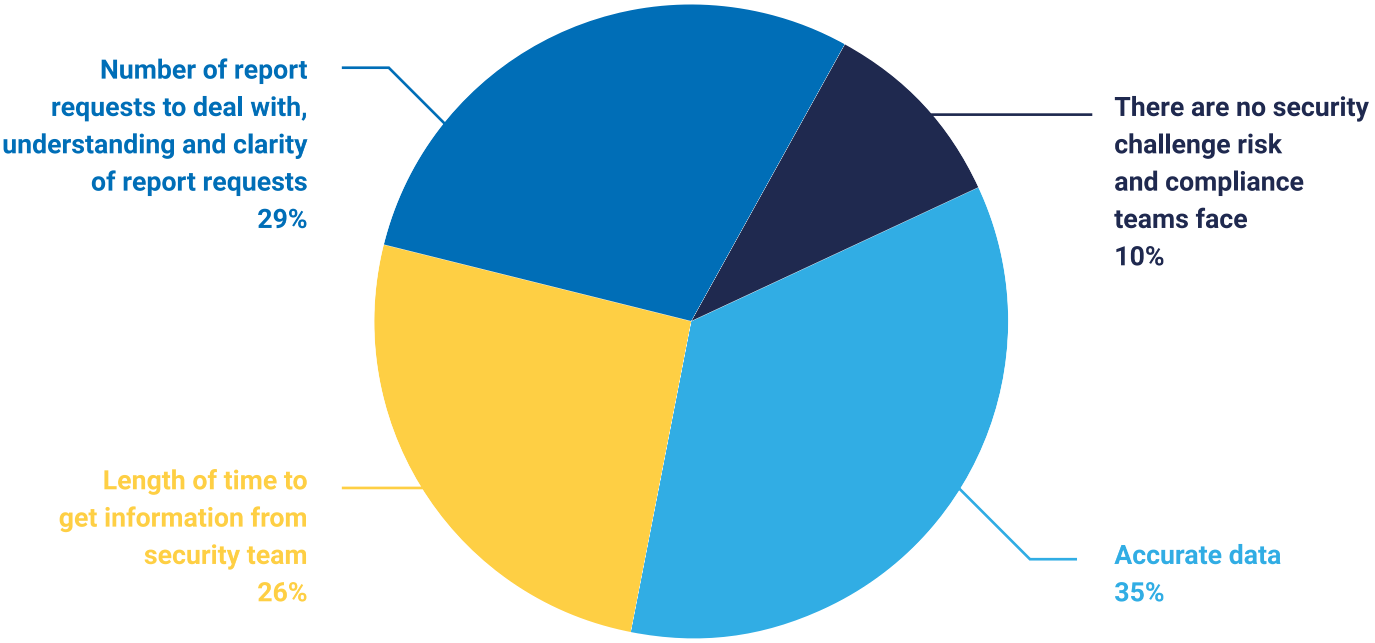
The survey findings reflect this fact with an underwhelming vote of confidence in the state of the information presented to regulators. Beneath the headline figure of **93%** being “confident” (to some degree) in the accuracy of security data provided on request, only a total of **39%** commit to being “very confident”. The missing **7%** of respondents stated only that there were “neither confident not unconfident” which, while not in itself a mea culpa, it is nevertheless hardly a ringing endorsement of any risk and compliance function endeavouring to satisfy the statutory obligations of a large financial institution.

The level of confidence in the accuracy of the security data provided when answering a regulatory request



This state of affairs is also borne out with the revelation that “access to accurate data” and “number of report requests to deal with” have emerged as the top two security challenges for senior GRC professionals questioned in the survey.

The top security challenges for risk and compliance teams



Looking closely, the number one issue is accurate data (or rather, a lack of it), cited as the single most significant security issue by more than one-third (35%) of respondents.

The challenge is amplified among risk and compliance leaders working at the smaller financial institutions surveyed, with **40%** of those employing between 5,000 and 9,999 people placing it first versus **33%** at those with 10,000+. While these levels are broadly similar, it reflects the fact that the same difficulties in grappling with complexity and sprawl afflict smaller institutions despite having fewer endpoints, applications and systems than their larger peers.

“Number of report requests to deal with, understanding and clarity of report requests” was cited the greatest security challenge by **29%** of respondents.

Here, the impact is felt more by the larger cohort of organisations, with **31%** of the 10,000+ employee bracket reporting it top versus **25%** of the 5,000 - 9,999 employee bracket.

This somewhat surprising finding highlights that the largest organisations are not spared from request overload even though – in theory – they possess greater internal resources.

Increasingly time-sensitive issues are compounded by manual processes

As stated above, current GRC toolsets are overly reliant upon manual processes that compromise the integrity of results as well as delaying request turnaround times. Qualitative research is at best a guess, and it is proven not to be objective enough.

There is much anecdotal evidence to support the view that regulatory requests are becoming more time sensitive, with regulators increasingly expectant that properly functioning governance processes will be able to respond satisfactorily.

One such example is the Monetary Authority of Singapore (MAS) Notice 655 on Cyber Hygiene, effective August 2020. Among its requirements is for banks to attest to having endpoint detection and response (EDR) software deployed and operational on every asset. Again, on the surface a straightforward request, but in reality, necessitating a highly detailed examination of both assets and security controls, most of which may only be currently achievable with significant manual effort.

Even then, the information reported to the regulator may only be a point-in-time assessment, when in fact what is required is an up-to-date assessment accurately validated at all times. The reporting and compliance with the regulation is only one part of this. The goal behind the regulation is to ensure that the endpoints are actually protected from threats, something that the business should be monitoring continuously.

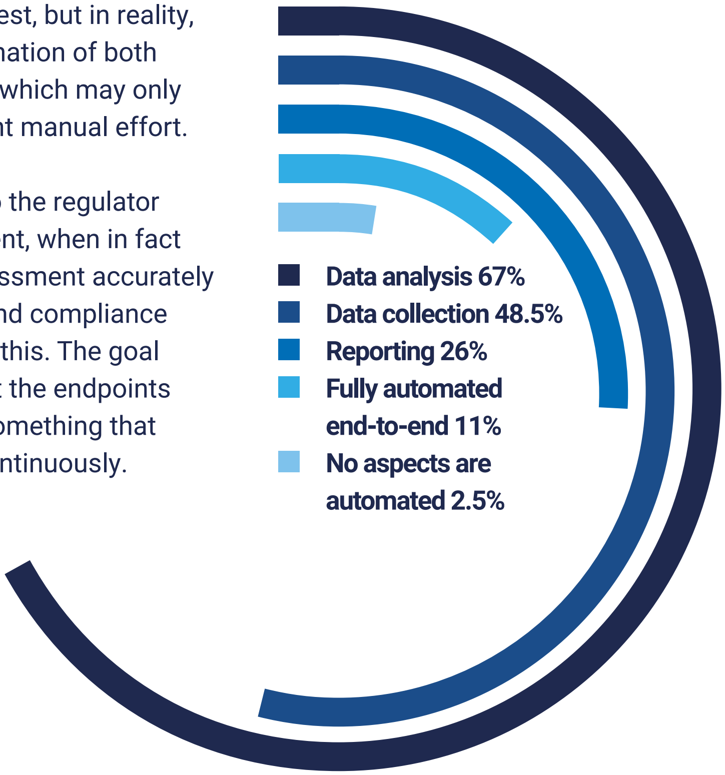
Automating processes would help to solve these challenges, but our survey found a widespread lack of automation.

For example, only **26%** of security risk and compliance reporting has end-to end automation. Even data collection (**48.5%** automated) and data analysis (**67%** automated) processes still have some way to go to be consistently free of the problems associated with manual error, bias and lack of pace and scale.

A small number of respondents (**2.5%**) stated that no aspects of their processes were automated – a very troubling state of affairs.

Encouragingly, **11%** have fully automated their processes end to end, demonstrating that it is achievable and worthwhile. Instances of end-to-end automation were found to be almost three times higher among US-based respondents than their UK-based counterparts.

The aspects of security risk and compliance reporting that are automated

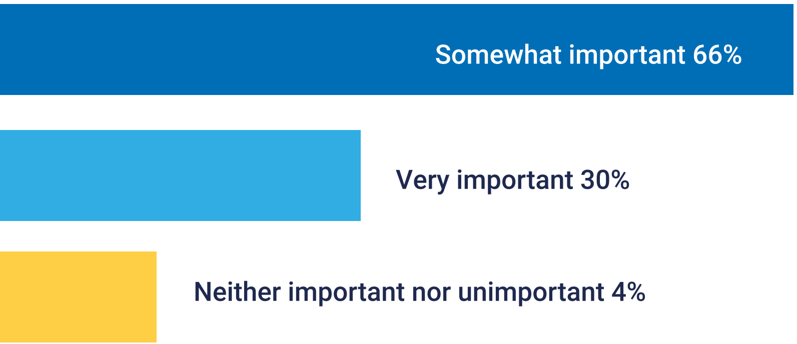


Overconfidence in understanding the business impact of risk and prioritising remediation accordingly

As outlined in some of the specific findings already covered in this report, it is taking a worrying amount of effort to report to regulators in an accurate and timely fashion. The immediate conclusion is that good visibility of risk is obscured or missing, creating significant knock-on effects to the overall risk management process; it becomes in effect 'risky' in that so much uncertainty implicitly introduces risk. This is often precipitated by overconfidence, which has been evidenced in independent analyst studies including **this one by Forrester Research[3].**

96% of the risk and compliance professionals asked in this survey were supportive of the importance of prioritising risk remediation based on impact to the business.

The importance of the ability to prioritise security risk remediation based on impact to the business



However, a perennial issue among organisations is insufficient visibility into how risks impact entire business processes and their unique combinations of applications, devices and people. So, while 97 percent of our sample believe they have this ability, our conversations and assessments with security and risk leaders across the industry indicate that very few actually do.

What's commonly missing is the ability to isolate and identify applications associated with particular business processes, as well as the interrelationships between assets i.e. the infrastructure that supports the applications (such as devices, databases) and the people and accounts that interact with them. To put it another way, what's missing is context.

We know through conversations with industry experts that missing context is a major problem, but one that can be addressed and even automated through Continuous Controls Monitoring (CCM), (of which more later) a category of solution that Gartner has recently recognised and which – while adoption is growing rapidly – is used among a limited cohort of businesses in highly regulated markets such as banking and financial services.

Without a full understanding of context, it is incredibly difficult to accurately assess the total, cumulative risk generated by 'toxic combinations' of risk factors. For example, a user that has failed a phishing test will present a certain degree of risk and it may be possible to establish comparative severity according to their access privileges/user profile. However, far trickier to correlate is if/when the user is also using a device that doesn't have the latest patch deployed. Without context, the data would show two different measures of risk, scored against different assets (in this case, the user and their device). The total risk of the 'perfect storm' is overlooked, compromising both security and compliance.

[3] Cybersecurity Requires Continuous Controls Monitoring To Ensure Complete Asset Protection, Forrester Consulting, September 2019

Understanding the context that surrounds risks is crucial to being able to prioritise them and make fast, effective decisions. Get this right and organisations are set up to commit resources and respond appropriately to the risks that stand to make the biggest impact on their business.

A new level of automation would be hugely valuable

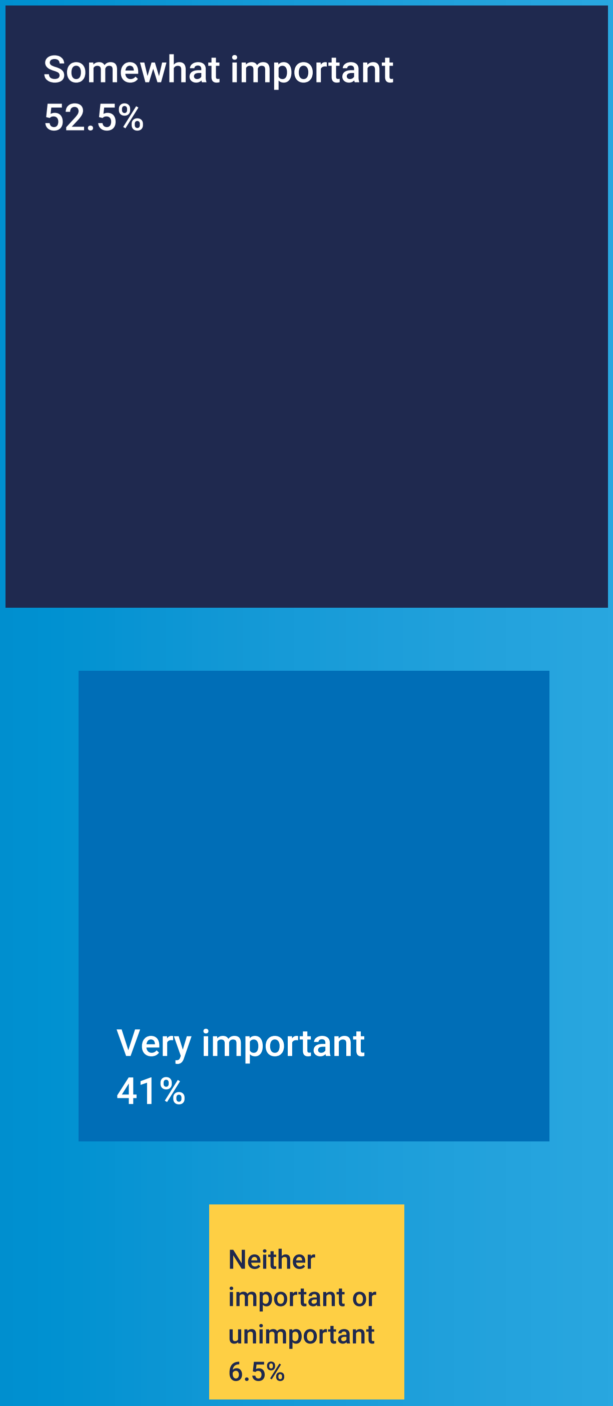
We have established that, based on the sample used for this research, organisations rely heavily on manual processes and lack the end-to-end automation that would support faster and more accurate turnaround times for responding to regulatory requests.

It's clear that 'automation' is seen as positive. A total of **93.5%** agreed that it is important to automate security risk and compliance reporting.

Despite this however, organisations are still way short of where they aspire to be. A total of **97.5%** had automated some aspect of their security risk and compliance reporting, but the scale of automation for a single aspect was no greater than two-thirds (**67%**, for data analysis).

Moreover, definitions of 'automation' differ and can be applied partially and subjectively. The CCM definition of automation is no more manual intervention, beyond initial setup, for all the different stages in this process – from data collection and unification, to metrics generation, analysis and reporting. Ultimately, CCM delivers complete end-to-end automation so that an organisation can perform quantitative assessment of security posture with no manual effort.

The importance of automating security risk and compliance reporting



In the context of cybersecurity GRC, CCM automation naturally involves a continual process of maintaining data accuracy and relevance rather than simply using automation as an on/off mechanism to satisfy point-in-time requirements.

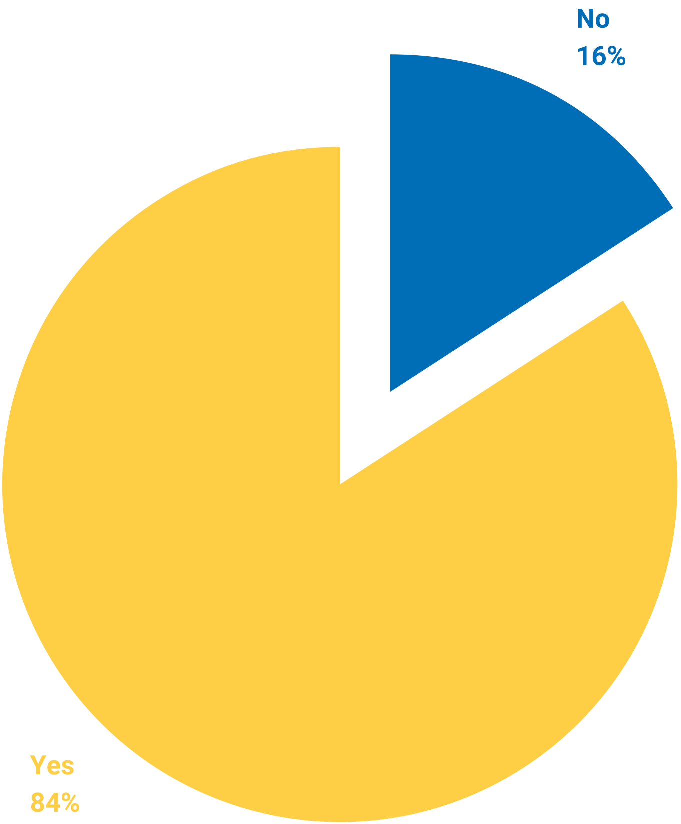
One such example of continuous automation is timestamping of historical security control data to substantiate performance and provide proof for regulatory responses.

For example, if an organisation is required to perform regular antivirus scans on all of their endpoints, rather than just saying, "yes, our policy requires weekly scans," with an automated record, you could report that, "of our 10,000 devices, 9,832 of them were scanned during the week of 3 August 2020."

Almost **85%** of respondents believe that timestamped historical security control data would be helpful in substantiating due care to regulators.

The reason this instance is so high is likely because risk and compliance leaders do not currently employ such a feature in a sufficiently complete and time-efficient way. The sentiment is greater among US-based senior risk and compliance professionals (**91%**) than their UK peers (**78%**).

Would time stamped historical security control data be helpful in substantiating due care to regulators?



SECTION 4:

Introducing Continuous Controls Monitoring

Risk and compliance professionals face significant difficulties providing regulators with accurate, timely information about their security posture despite the widespread availability and use of GRC tools. Data collection and reporting processes are too reliant upon manual work, resulting in turnaround delays and greater likelihood of human error, not to mention employee stress.

The Gartner Hype Cycle for Risk Management[4] has identified an emerging area of security and risk that addresses this – Continuous Controls Monitoring (CCM).

Gartner defines CCM as, ”a set of technologies that automates the assessment of operational controls' effectiveness and the identification of exceptions.” Also that it is "runtime and transaction-level monitoring, and is most useful for operational controls."

However, it is in the realm of GRC management that CCM really comes into its own.

Panaseer's CCM platform provides GRC teams with the quantitative data they need about their security controls.

It does this by sitting on top of an organisation's security controls, determining which are deployed on which assets, whether they are switched on and operating as expected.

Using CCM, organisations can:

- **Create a comprehensive asset inventory including devices, applications, people, accounts and databases.**
- **Uncover gaps in security controls deployment coverage.**
- **Adhere to internal policy compliance.**
- **Isolate risks to mission-critical parts of the business.**
- **Integrate with GRC tools to automatically populate them with security controls assurance data.**
- **Gain access to facts that can be substantiated with data instead of subjective questionnaires.**
- **Map controls data to regulatory frameworks such as CIS or NIST.**

[4] Hype Cycle for Risk Management, 2020, Gartner, July 2020

CCM is proven to save time and resource costs by automating security compliance monitoring and controls assurance. Visibility into remediation status and documentation of internal policy adherence in turn breeds complete confidence in demonstrating to regulators that adequate safeguards were in place.

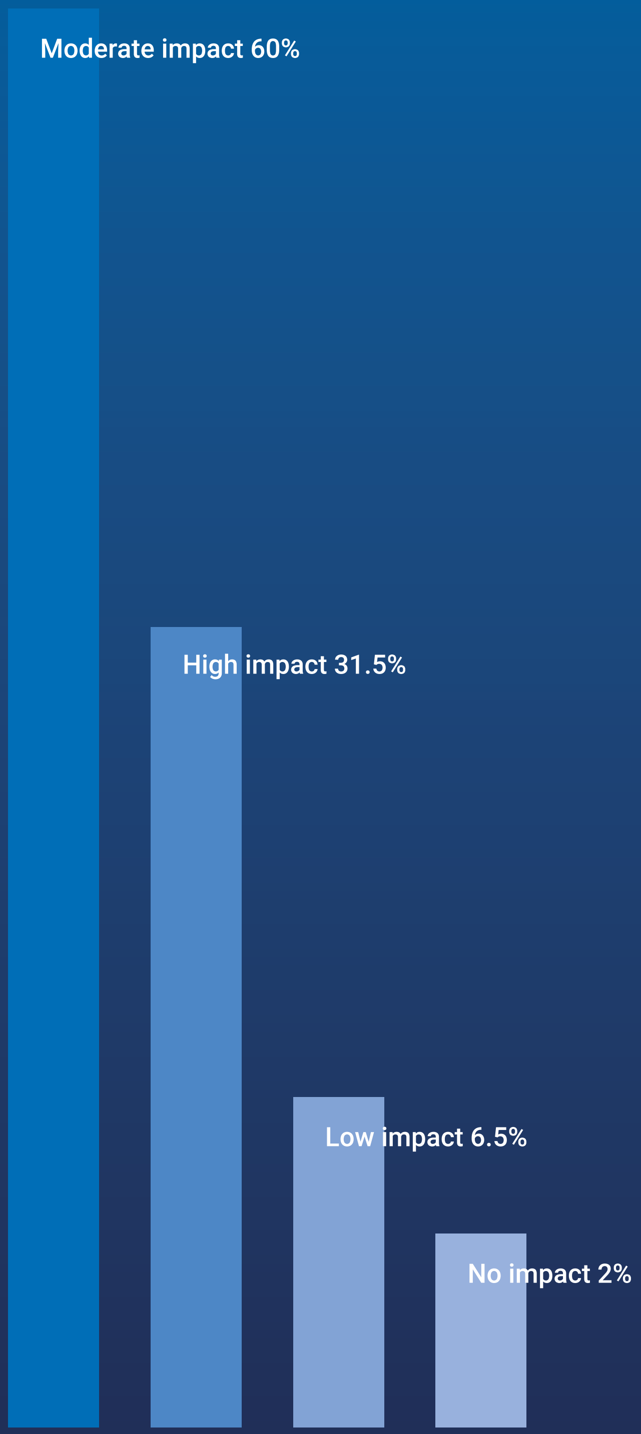
At its heart, CCM is a single source of truth, utilised to address multiple regulatory requirements, providing the ability to prioritise risk aligned to critical business operations, and restore trust among all stakeholders in the accuracy of risk metrics and data.

Crucially, the platform provides self-service access to current and historical data so that time-bound regulatory requests can be accurately and efficiently fulfilled, without relying on intermediaries.

According to the survey results, nearly one-third of the sample believes a self-service security reporting capability would have a high impact on their business.

This capability helps GRC teams answer regulators' questions about controls implemented in the business, making it a key market requirement. GRC tools can then automatically access the information and transform it into different formats aligned with the demands of different regulators.

How impactful would self-service security reporting capability be to your organisation?



Continuous Controls Monitoring adds value to IRM processes

One example of CCM and GRC tooling working together seamlessly can be found in **the integration between Panaseer and RSA Archer's market-leading Integrated Risk Management (IRM) platform[5].** This enables security teams with complete and accurate visibility of assets, control gaps and risks – both on-premises and in the cloud.

By integrating CCM, IRM practices that require data to be collected and analysed can be automated with near real-time insights that are easily scalable.

This significantly reduces the cost of risk management and associated data collection and analysis. Other benefits include:

- Leveraging automation to increase efficiency and minimise cost as large teams doing manual assessments are no longer required.
- Improve accuracy with data based on facts versus subjective opinions.
- Perform complete rather than sampling-based assessments as testing of every control instance is available automatically.
- View continuous assessments with a consistently up-to-date view of control deployments.

[5] Panaseer Platform Integration, RSA, January 2020

SECTION 5:

Conclusion

At the heart of this report is compelling evidence that the quest for accuracy, timeliness and context in addressing regulatory requests is far from over. Indeed, as regulatory scrutiny increases, in step with the rising frequency, intensity and variety of cyber attacks, the challenge of not only mitigating security risks but being demonstrably proven as compliant with relevant laws and regulations will become steadily more difficult unless new data-driven solutions are found.

For accuracy, timeliness and context – read 'performance'. Because performance matters in the management of governance, risk and compliance. Not least because regulators expect it, as do all other stakeholders in large financial institutions.

Our research shows that GRC leaders are enlightened to the issues at hand; principally the uncertainty created by over-reliance upon time-consuming, inefficient and error-prone manual processes.

They understand that manual processes cannot be expected to maintain a continuously aware single source of truth able to validate if security controls are operating within internal policies and external regulations, identify assets and controls that are non-compliant, and prioritise and initiate remediation to mitigate risk based on business impact.

This is about more than faster response turnaround times on regulatory requests – as important as these are. This need for greater performance is fundamental to the certainty and confidence financial institutions need to manage their risk and compliance effectively.

And so trusted, real-time automation emerges as a critical overarching feature of a new toolset, together with self-service reporting both of overall security posture and in giving straight, fast, unequivocal answers to difficult, searching questions. All point to a new area of risk management: Continuous Controls Monitoring.

To learn more about how you can use the Panaseer's platform to enhance your GRC capabilities, contact us at **success@panaseer.com**, or request a demo at **panaseer.com**

We’ve got you covered

Continuous Controls Monitoring for enterprise security