Modernizing Operational Risk Management Survey

OCEG 2021

OCEG®
Driving Principled Performance

SPONSORED BY servicenow™

INSIDE THIS BOOK

ABOUT

OCEG is a global, non-profit think tank and community. We invented GRC.

We inform, empower and help advance more than 100,000 members on governance, risk management, and compliance (GRC). Independent of specific professions, we provide content, best practices, education, and certifications to drive leadership and business strategy through the application of the OCEG GRC Capability Model and Principled Performance®. An OCEG differentiator, Principled Performance® enables the reliable achievement of objectives while addressing uncertainty and acting with integrity.

Our members include c-suite, executive, management, and other professionals from small and mid-size businesses, international corporations, non-profits, and government agencies.

Founded in 2002, OCEG is headquartered in Phoenix, Arizona.

Learn more at oceg.org

ServiceNow (NYSE: NOW) is making the world of work, work better for people. Our cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity for employees and the enterprise.

ServiceNow Governance, Risk and Compliance helps power your resilient business with risk-informed decisions integrated across the enterprise so your people and organization work better. By seamlessly embedding risk management and compliance into your digital workflows and familiar user experiences, you can improve decision-making, increase performance, and gain real-time visibility into risk. Only ServiceNow can connect the business, security, and IT with an integrated risk framework that transforms manual, siloed, and unfamiliar processes into a user-friendly, unified program built on a single platform.

Learn more at servicenow.com/risk

Thoughts from ServiceNow

Operational Risk Management has become a more strategic and visible element of business strategy as organizations sculpt their post-COVID recoveries and accelerate digital transformation. To keep up with demand, risk management deserves some transformation as well, according to the more than half of respondents to this survey focused on operational risk modernization initiatives in 2021.

"Do more with less" holds true as risk leaders work to support risk-informed decisions, while creating structural efficiencies that lower operational expenditures:

- 58% seek to develop new risk assessments driven by digital transformation
- 54% want enhanced executive reporting, analytics, and transparency
- 54% are requiring increased efficiency and automation
- 49% are rationalizing technologies for risk/compliance/audit/continuity

As we have seen in our work with the ServiceNow global community, a common foundation enables these objectives: a modern cloud-based platform that connects across the enterprise, and from first line to third line. More than 80% of survey respondents indicate they either are already operating in the cloud for their operational risk management data needs or are going to be there within the next few years.

Why is cloud platform adoption such a juggernaut? Because it enables the agility and confidence required for demanding operational risk programs as companies transform digitally. Expanding domains and use cases simply aggravate the "data to insights to action" challenge. Throwing more tools at the problem isn't the answer. Almost two-thirds of respondents have more than 6 tools already, impeding data synthesis. It is no wonder tool consolidation is one of the stated goals of cloud platform adoption.

More than two-thirds of survey respondents indicate that they have 20 or more data sources to pull from and 21% have more than 100 data sources. A common cloud platform with a common data model permits smooth access to more, better, and more actionable information, with less complexity and cost up front and over time. The platform approach also facilitates integrated workflows across organizational silos and transparent data collection from the first line, helping to overcome the perennial challenge of first line engagement.

A motivational finding is that respondents with high maturity – using a common platform which brings systems together with operational data with the business – were also more confident that they were providing accurate, timely information to demanding stakeholders.

We hope that these and other learnings can help you design your own journey. ServiceNow appreciates the partnership with OCEG and the community in building this knowledge base to help us all chart a course to modern operational risk management.

OPERATIONAL RISK MANAGEMENT

Risk management is essential in every organization. As internal and external business environments have continued to evolve, the threat landscape has become more complex, as have processes for identifying and managing risks. Operational risk management has become more challenging as businesses expand their products and services, use more suppliers and other third parties, and introduce new information management processes and systems. Siloed operations each managing siloed risks in siloed systems make risk management more chaotic and reduce clarity. Modernization of operational risk management is essential.

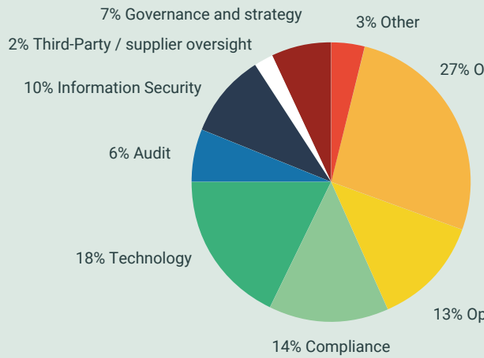
What Do We Mean by Operational Risk?

There are many definitions of operational risk and the simplest are the most accurate. To put it plainly, operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Operational risk is inherent in all products, activities, processes, and systems. When operational risks are realized, they can cause business disruption, failure to achieve objectives, financial loss and reputational damage.

ABOUT THE SURVEY

OCEG and survey sponsor ServiceNow undertook this survey to determine the state of current and planned efforts to modernize operational risk management ("ORM"). We looked at how people view the current state and existing challenges in ORM, their levels of confidence in current understanding and control of risks, and their plans for modernization – in particular, plans to move to cloud-based systems for ORM.

ABOUT THE SURVEY PARTICIPANTS

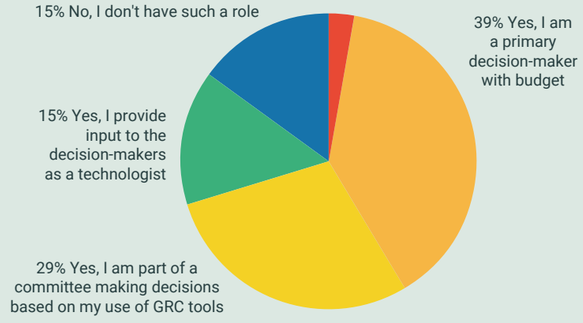


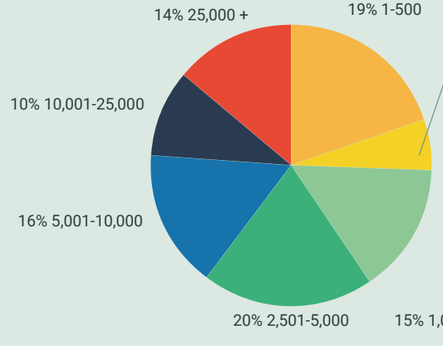
Which Area Best Describes Your Primary Responsibilities for Risk Management?

440 participants from a wide range of roles completed the survey. The majority have executive or managerial positions.

Do You Have A Role In Decisions About Acquiring or Adapting Existing Technology to Support Operational Risk Management?

Most participants have a part in decisions about technology they use or plan to use for ORM.





What is the Size of Your Organization in Employees?

Participants are located in 62 countries with 63% in the United States. They represent companies of all sizes. **We have focused this report commentary on organizations with 1000 or more employees.** All responses are in the separate full data set for the survey, available at oceg.org/research

MATURITY MATTERS

Survey respondents were asked to assess their organization's level of maturity in operational risk management based on the level of integration of processes/operations and the tools/technologies they employ.

Range of Maturity in Technology Use

17%
Common Platform brings systems together with operational data from the business

44%
Multiple, often siloed technologies. Low data and process Integration

38%
Ad hoc and productivity tools. Largely manual and siloed operations

As we review the findings of the survey, we see that level of maturity matters when assessing confidence in different aspects of operational risk capabilities and defining the level of agility in various key processes and tasks. We also see that cloud-based platform users are doing better overall. When we compare them to the rest of the respondents, we see higher risk maturity levels, better agility, and more confidence in processes and communications.

PLANS FOR CHANGE

At the end of 2019, before the worldwide COVID 19 pandemic became widespread, many organizations were already beginning to focus on the need to improve how they addressed operational risk management. They understood that they needed to establish a stronger relationship between their risk management and business continuity efforts. According to OCEG polling at that time, many intended to thoughtfully analyze and address organizational risk management changes, upgrades to procedures, and enhancements for technology to support these needs over the next two to three years.

Then everything changed, more rapidly and in more ways than they had imagined possible. Suddenly, the need to mature operational risk management became critical. Current systems for seeing and preparing for potential threats to operations were inadequate. In particular, there was a real lack of understanding how the workforce and supply chains could be suddenly disrupted, not only by a pandemic but by other potential events such as geopolitical upheaval or natural disasters. The cumulative and "domino effect" nature of risk became clearer. The need to prepare for risks deemed highly unlikely but having potentially serious impact suddenly came to the forefront. For many there was now a "save the company" demand to act fast with a greater need to view and understand consolidated risk data than ever before.

At the same time, many organizations are recognizing the impact of digital transformation on their risk profiles. When we asked survey respondents to identify the top areas of digital transformation affecting them, there were four that were most commonly chosen.

Top Areas of Digital Transformation Impacting Risk Profile

49%
New employee engagement models

44%
Evolving regulations

43%
Increased cybercrime exposure

41%
New business processes

The worldwide pandemic has accelerated digital transformation. The need to ensure associated risks are identified, assessed, and controlled must similarly be addressed sooner than many had originally planned.

OPERATIONAL RISK INITIATIVES AND RESOURCE ALLOCATION

More than half of respondents to this survey are focused on modernization initiatives in 2021 that improve visibility into operational risk and response, while lowering operational expenditures. Four goals stand out.

Goals for Operational Risk Modernization in 2021

58%
Develop new risk assessments driven by digital transformation

54%
Enhance executive reporting, analytics, and transparency

54%
Increase efficiency and automation

49%
Rationalize technologies for risk/compliance/audit/continuity

As they strive for these outcomes, resource allocation priorities are being adjusted to address concerns about disruption and information security. There is recognized need to address risks from digitalization of business.

Top Areas for Increased Resource Allocation In 2021

58%
Business Continuity

57%
Remote Workforce

56%
Privacy and Data Protection

The top areas for resource allocation present interrelated risks. About a third of respondents also highlighted focus on supply chain, ESG, and mobile apps/devices.

PLANS FOR MOVE TO THE CLOUD

One aspect of modernization is improvement in technology for managing risk data. Today, the best risk management systems enable integration of multiple technologies, including business systems that store data needed for effective risk assessments, understanding of business impact, and determination of internal and external reporting needs. The most modern platforms supporting such integrations are now cloud-based, and so we asked survey respondents about their plans to move to the cloud. Thirty-eight percent indicated they are already using cloud-based platforms and another 43% indicated they have plans to do so as well.

These are striking numbers – more than 80% of survey respondents indicate they either are already operating on cloud-based platforms for their operational risk management data needs or are going to be there within the next few years.

Top Reasons for Moving to a Cloud-Based Platform

50%
Real time continuous monitoring and visibility

44%
Reduced complexity and tool consolidation

44%
Easier expansion to new use cases

37%
Better integration with enterprise and third-party apps and data

36%
Improved access to data and reporting for better decision-making

The reasons for the move are varied, but overall point to a desire for getting better information with less complexity and cost.

COMMUNICATION AND REPORTING

Communications about operational risk are needed in many directions and for many purposes. Challenges in getting the right information to the right people at the right time remain significant, despite many efforts over recent years to improve information flow. In the survey, we sought to identify the primary challenges and the reasons for them.

Challenges in Engaging the Front Line

Respondents indicate that they face challenges in getting information they need from front line business operations. This is also referred to as the "first line" in the three lines of defense model for risk management. They identify six primary reasons for this challenge.

Top Challenges in Engaging the Front Line

45%
Slow speed of response

41%
A perception of risk and compliance as "overhead" or a drain of time and resources

35%
Difficulty getting the attention of front line managers

33%
Poor accuracy or quality of responses

32%
Knowing who to request information from

32%
Explaining value and need for information

Why would this be? Risk managers seeking information from the front line are trying to ensure that operational risks are properly identified and controlled based on the impact they may have to operations and the criticality of those operations. We would think that operational managers would be anxious to help in that effort, but that appears not to be the case in many organizations. These challenges are likely driven by the workforce overall not understanding the value of managing operational risk or the relationship between risks and controls.

In organizations with more mature operational risk capabilities, about half of respondents say they are confident that their workforce understands operational risk. In less mature organizations, fewer than 30% are confident that their workforce has that understanding.

This points to a need for better communication with the workforce, and with operational risk managers in particular, to ensure that they see how uncontrolled or poorly controlled risks can create real problems for them in doing their jobs and meeting their objectives. They need to know that by asking for information, the risk team is trying to help them do their jobs without disruption. There is also benefit in providing views into how the information can be used, through dashboards and reports that enable operational managers to see risk information in conjunction with their own strategic planning and operational action decisions.

POOR COMMUNICATION WITH THE BOARD AND SENIOR MANAGEMENT

The challenges in getting reliable information from the front line contribute to a lack of confidence that reporting to the executive team, board and external stakeholders is reliable, accurate and timely.

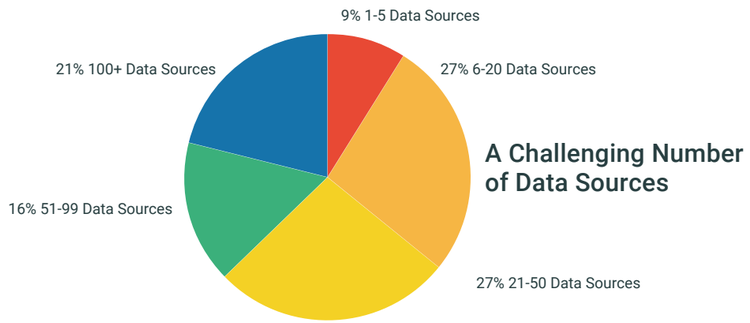
Maturity in operational risk management capability appears to make a real difference in confidence about reporting and communications, largely due to better data management and quality overall.

Maturity in Operational Risk Management Makes a Difference in Confidence

Notably, even in organizations with more mature operational risk management capabilities, the level of confidence is still lower than we would hope. Almost half of the responses from more mature organizations still have concerns about whether they are providing – or are able to provide – useful, accurate, actionable information to decision-makers and stakeholders. The reasons for this lack of confidence appear to be based on issues raised by having disconnected data sources, even if overall there is greater maturity in the management of operational risk.

DISCONNECTED DATA CAUSES PROBLEMS

Beyond the challenges of getting information from the front line operations due to lack of understanding and trust, the way data is maintained contributes to lack of confidence and poor agility.

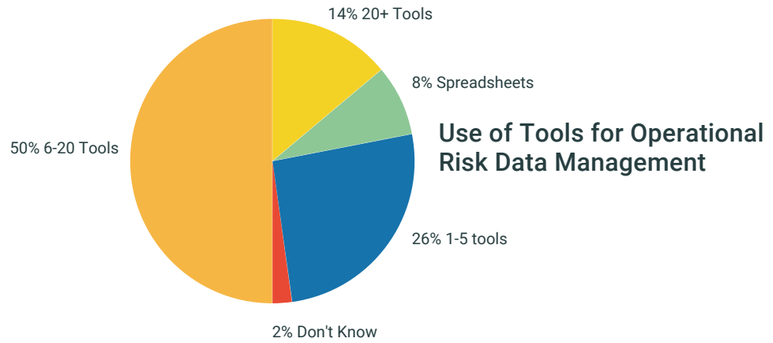


These challenges start with finding all of the needed data. It will always be the case that data needed for complete risk management resides in many locations, even in mature organizations. More than two-thirds of survey respondents indicate that they have 20 or more data sources to pull from and 21% have more than 100 data sources. The 9% who indicate they have only 1-5 data sources don't have more mature risk management and they aren't doing a better job. They are, instead, most likely failing to consider all of the sources of data, both inside and outside of the organization, that must be mined for information that is useful in identifying and assessing operational risks.

During the webinar on the results of this survey, Vasant Balasubramanian, Vice President and GM of Risk BU at ServiceNow, noted "Those who indicate fewer than 20 sources of information are missing the mark. They simply are not able to fully identify and consider information about risks that are present or predicted[1]."

Negative Effect of Data Silos

The survey indicates that collected information is most often being managed in different, disconnected technologies for different purposes. This means that in some cases the same data is being categorized differently in different parts of the organization. About two-thirds are using six or more tools to manage operational risk data and 14% have twenty or more tools in place.



Even those with higher levels of maturity, including some of those with cloud-based platforms in place, are using large numbers of tools, and this may continue to be the case.

The failure to use a common platform that can connect operational risk systems and share data based on common taxonomies, vocabularies, and forms of data entries, is creating many problems.

Respondents indicate that there are too many people they have to get data from and the use of different vocabularies and taxonomies for the data reduce confidence in the usefulness of what they are able to get.

[1]The recording of the full webinar is available on both the OCEG and ServiceNow websites.

Challenges To Identifying, Analyzing, And Reporting On Operational Risks

56%
Excessive time to collect, combine and compare data sets

50%
Too many people who need to be asked for data

40%
Too many vocabularies and taxonomies to be reliable

Top Challenges to Performing Risk Assessments

53%
Employees lack understanding of risk

42%
Incomplete or outdated data

41%
Data in emails, spreadsheets, etc.

40%
Difficulty quantifying business impacts

37%
Lack of consistent, repeatable process

The above challenges are a microcosm of the data collection, contextualization, synthesis, and actioning issues we have called out in the survey. These challenges represent areas where people have to get involved to overcome gaps and conflicts, and this model doesn't scale to the range of risks and fast pace of digital business.

The problems in data management lead to poor agility in performing needed – and increasingly diverse – risk management tasks and reduce confidence in decisions and outcomes.

Data weaknesses make it virtually impossible to have meaningful audit of the risk assessments that are undertaken. Looking at these practices, the difference that maturity makes is clear. In each case, those from mature organizations have far greater confidence that they are using these best practices.

MATURITY MAKES A DIFFERENCE

Overall, organizations with more mature operational risk capabilities report greater application of best practices, leading to stronger confidence about risk identification and assessment. They have a broader and more accurate view of risk information and more consistency in application of assessment methodologies.

Maturity Makes a Difference in Risk Identification And Assessment

Mature 76%
Immature 38%
Integration of risk systems with business information systems for identification of risks

Mature 69%
Immature 48%
Integration of risk systems with business information systems for risk assessments

Mature 55%
Immature 36%
Well-documented operational risk identification and assessment

Looking at the responses from a different angle, it becomes even clearer that lack of maturity leads to lack of confidence in operational risk management processes and understanding:

Minimally or Not at All Confident There is

Mature 5%
Immature 31%
Operational Risk Identification and Assessment

Mature 11%
Immature 36%
Workforce Understanding of Operational Risks and Relationship to Controls

Taken together with the survey data discussed earlier about confidence in quality and timeliness of reporting, the value of maturing and integrating processes with modern technology support is clear.

CLOUD-BASED PLATFORMS MAKE A DIFFERENCE

As noted earlier, 38% of respondents are using a cloud-based platform for management of operational risk and another 43% have plans to do so within the next few years.

Confidence Levels in Risk Management are Higher With a Cloud-Based Platform

Cloud Platform
No Cloud Platform

OPERATIONAL RISK MANAGEMENT OVERALL

Highly Confident
55%
33%
Minimally Confident
8%
15%

BUSINESS CONTINUITY

Highly Confident
53%
32%
Minimally Confident
8%
15%

CYBER

Highly Confident
57%
38%
Minimally Confident
5%
15%

When we take a closer look at responses from those who are already using such platforms, we can see the value added.

We see differences in confidence in the quality of risk management across a range of topics.

Confidence Levels in Risk Management are Higher With a Cloud-Based Platform

Cloud Platform
No Cloud Platform

PRIVACY

Highly Confident
59%
39%
Minimally Confident
7%
22%

ESG

Highly Confident
46%
26%
Minimally Confident
15%
32%

REGULATORY

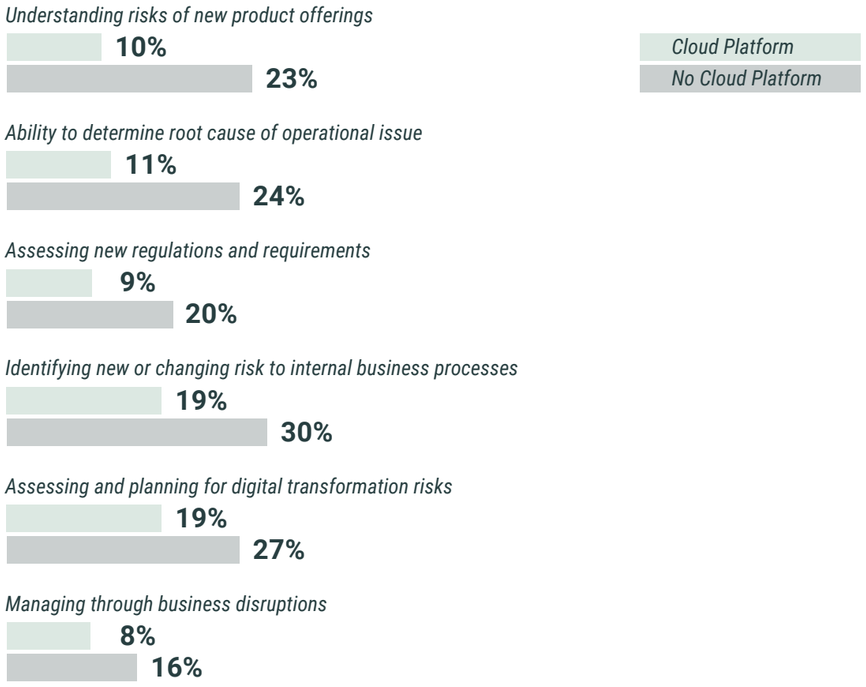
Highly Confident
62%
41%
Minimally Confident
5%
10%

THIRD PARTY/SUPPLIER

Highly Confident
35%
18%
Minimally Confident
20%
35%

Second, those not using cloud-based platforms are significantly more likely to indicate that agility is lacking in key areas of risk management. The following chart shows some comparisons

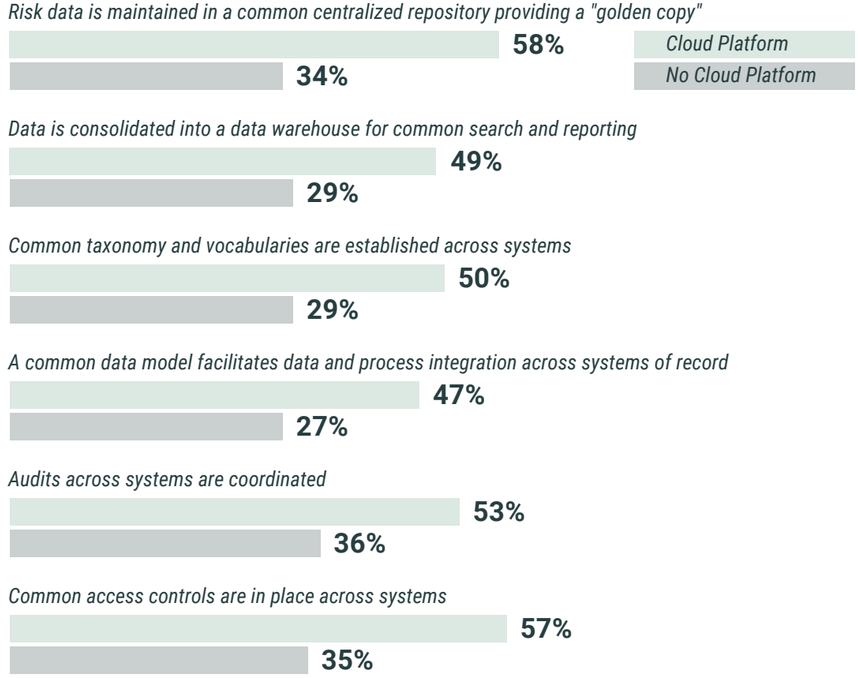
Areas Where Agility Needs a Lot of Improvement



In large part, it would appear that the higher levels of confidence and agility in those using cloud-based platforms derives from the higher levels of integration between risk tools, which leads to clearer information.

Across the board, one-third or fewer of those without the use of cloud-based platforms indicate that their risk data is managed through tool integrations using common best practices, while half or more of those using a cloud-based platform are fully ensuring most such practices are in place. The following chart demonstrates this difference.

Fully Integrated Risk Tools and Best Practices



CONCLUSION

Maturing of operational risk management capabilities is top of mind in many organizations. The challenges presented by ever changing conditions, lack of standardization in processes, and disparate data sets are affecting agility and confidence in every aspect of operational risk management. Without improvement, it is difficult to see how decision-makers can engage in risk-aware strategic planning or expect to reliably achieve the objectives they establish. Plans for near term improvements are encouraging, but it remains to be seen if the urgency driven by the global events of 2020 and 2021 continues or fades away as conditions improve.

Now is the time to take advantage of the focus on operational risk management. The findings of this survey support a business case for commitment of resources and leadership needed to develop mature processes and implement the technology to support those processes.