The state of integrated risk management, 2020 – final report

Dr. French Caldwell, DLP
Founder and Chief of Research, FCInsight

FCInsight
Member of The Analyst Syndicate
@iTGuru
/frenchcaldwell/

Table of contents

FCInsight
Member of The Analyst Syndicate

The survey results are presented in two primary sections, one for banking and financial services and the other for other industries. The reason for this approach to the presentation of the results is that risk management within financial services is heavily regulated, much more so than other industries. As a discipline, it has also been practiced in earnest since the 1980s within financial services, and the emergence of integrated risk management with other industries is more recent.

About the survey

Purpose: This is a survey of risk management, compliance, audit, and other business and GRC leaders on the state and maturity of integrated risk management (IRM).

Participants: 272 risk management, compliance, audit, IT, GRC and business professionals qualified for the survey. Of those, *180 were in banking and financial services and 171 or those were members of the Risk Management Association*. 92 respondents were from industries other than banking and financial services.

FCInsight
Member of The Analyst Syndicate

The survey was completed in 2020 and was targeted to professionals in a number of risk-management-related roles. The Risk Management Association, primarily an organization for banking risk management professionals, shared the survey with its 80,000 members. FCInsight used Linkedin to share the survey with risk management professionals in other industries. Some GRC vendors shared the survey with customers.

Definitions and context

What is IRM?: IRM is a process that improves decision making and enhances business value by integrating risk intelligence into activities across the enterprise, such as strategic planning and strategy execution, investment decision making, project portfolio management, enterprise performance management, third party performance management, and information governance.

What is risk intelligence?: Risk intelligence is risk data or information that is applied through IRM initiatives to business activities beyond risk management, compliance, audit and other defensive programs.

How does IRM relate to GRC?: GRC is a program for collaboration and coaction among enterprise lines of defense to:

1. preserve corporate integrity,
2. protect brands and reputations,
3. provide assurance of compliance with laws, regulations, standards, and contractual obligations, and
4. ensure that directors, executives and employees have the risk intelligence to ensure exceptional business performance

IRM is implemented as initiatives, not as a program. IRM initiatives overlap with the fourth goal of GRC programs and ensure that the risk intelligence provided by GRC-related activities is proactively integrated into other enterprise functions.

FCInsight
Member of The Analyst Syndicate

Risk management became a field for study after WWII. At first, the risk management professional was understood to be the person who used insurance to hedge against accidents or in financial services to hedge against market uncertainties. In the 1980s, international regulation of financial services emerged and by the 1990s risk management became a board-level concern. By the late 1990s, the importance of governance of risk management was recognized by boards, and the role of the chief risk officer became entrenched within large banks along with the concept of integrated risk management (IRM) – a strategic view of risk management and its importance to the management of a bank's portfolio of assets.

Multiple crises over the last two decades – the dot-com bubble, 9-11 and subsequent geopolitical upheaval, the financial crisis, and most recently the covid-19 pandemic -- have illuminated the value of risk management to activities throughout the enterprise and throughout extended supply chains and value chains of the enterprise. Digital transformation and cybersecurity failures have also highlighted the importance of an extended view of risk management to include risks to digital assets and IT infrastructure, including digital assets managed by or with the assistance of third parties.

Over the last decade, IRM has evolved from primarily focusing on the assets of financial services organizations to a multi-industry discipline that supports business objectives and decision-making throughout the organizational hierarchy. Within any enterprise there are multiple risk management programs: cybersecurity, privacy, health and safety, quality management, standards compliance, anti-bribery and -corruption, enterprise risk management (ERM), many forms of regulatory compliance, internal audit, environmental, social and governance (ESG), ethics and many other programs are all examples of risk management and are sources of risk intelligence. IRM itself is not a standalone program, but rather a discipline for applying risk intelligence to other activities within the enterprise beyond risk management, compliance, audit and other defensive programs.

Banking and financial services

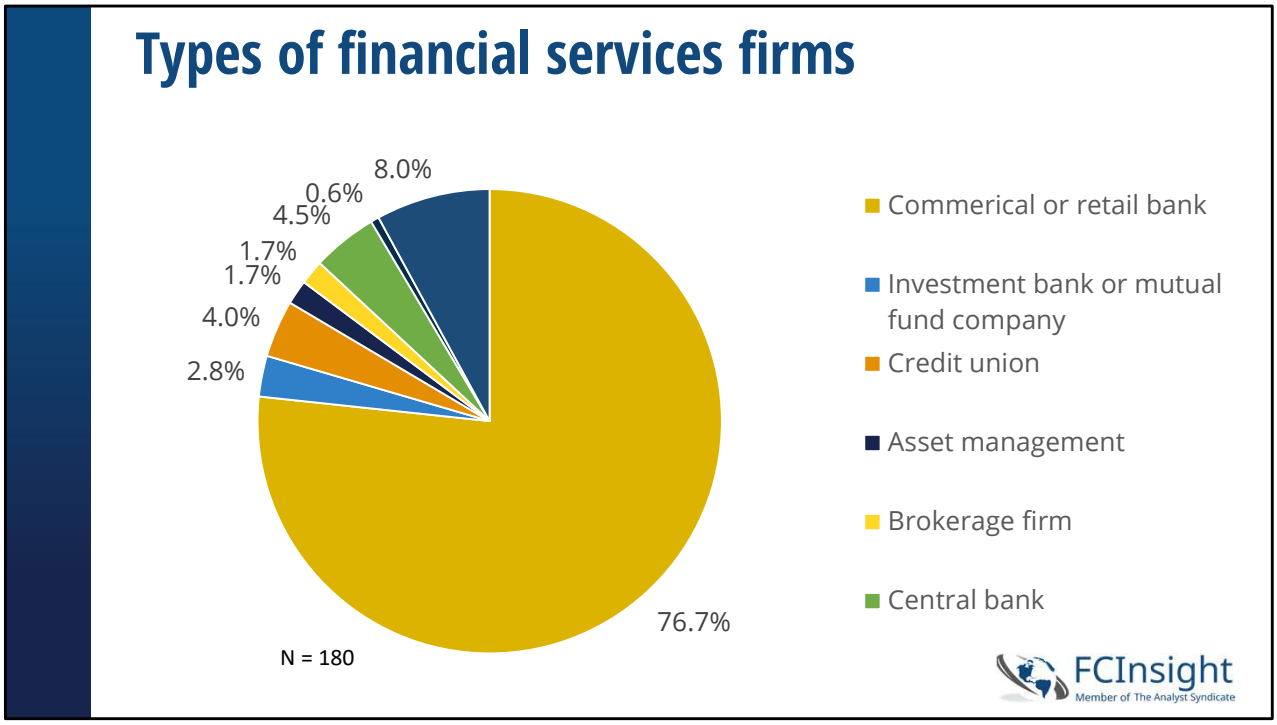
FCInsight
Member of The Analyst Syndicate

Key findings for financial services

- 74% of respondents report they are integrating risk intelligence into business activities
- Strategic planning and strategy execution are top objectives for IRM
- Most respondents spend 25% or more of their time on ERM – true for all seniority levels
- Respondents rated IRM as relatively mature, but only 12% were optimizing IRM
- Business intelligence applications are more commonly used than GRC technology in IRM initiatives
- The use of BI and GRC tools correlated to greater IRM maturity

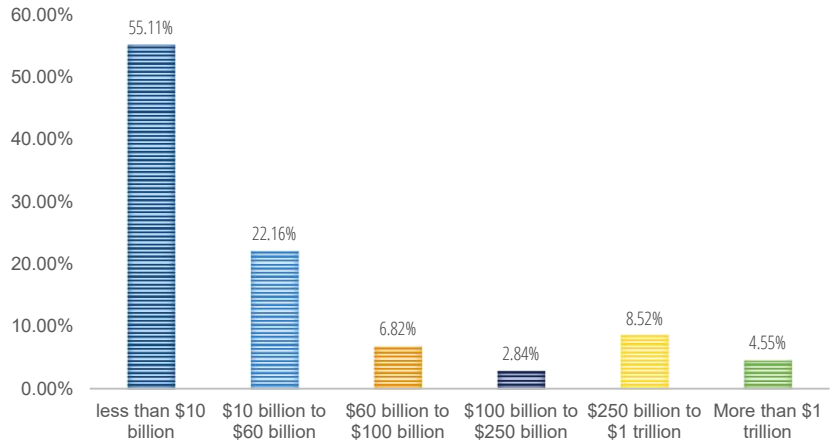
FCInsight
Member of The Analyst Syndicate

With the growing importance of good risk intelligence to business decision making, the RMA and FCInsight teamed up to evaluate the state of IRM in 2020. As early adopters of IRM, financial services organizations were expected to be at a higher level of maturity. Still, within financial services, the surveyors were surprised at the high degree of penetration of IRM with 74% reporting that they are integrating risk intelligence into business activities.



Most financial services respondents represented banks and credit unions.

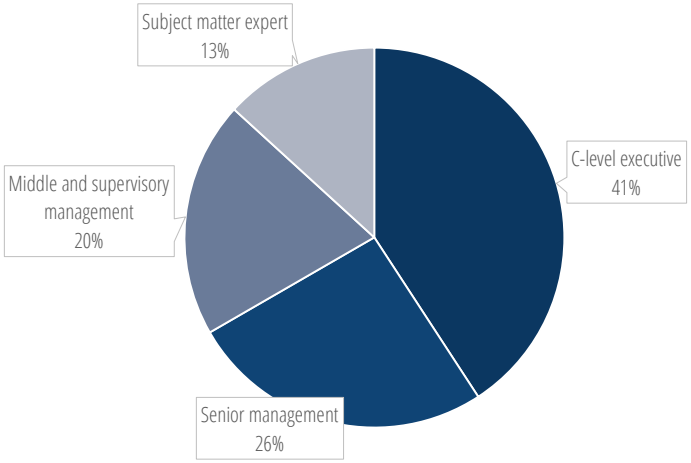
Size of firm (assets under management)



FCInsight
Member of The Analyst Syndicate

A preponderance of respondents were from small and mid-sized financial services firms.

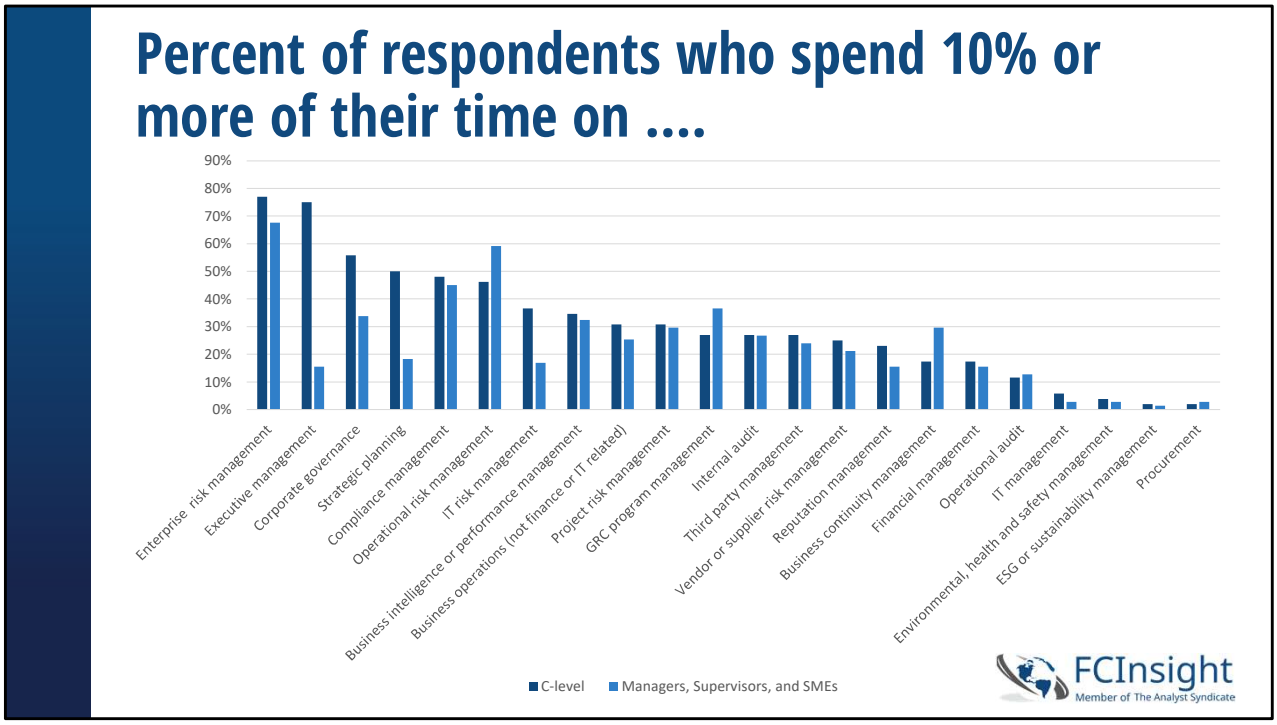
Seniority of participants – banking and financial services



C-level participants	
Chief Risk Officer	62.0%
Chief Credit Officer	12.7%
Chief Executive Officer	8.5%
Chief Compliance Officer	5.6%
Non-executive Director	4.2%
Chief Audit Executive	2.8%
Chief Operations Officer	1.4%
Chief Information Security Officer	1.4%
Chief Revenue Officer	1.4%

FCInsight
Member of The Analyst Syndicate

The relative high number of C-level and senior management participants indicates high interest in IRM.

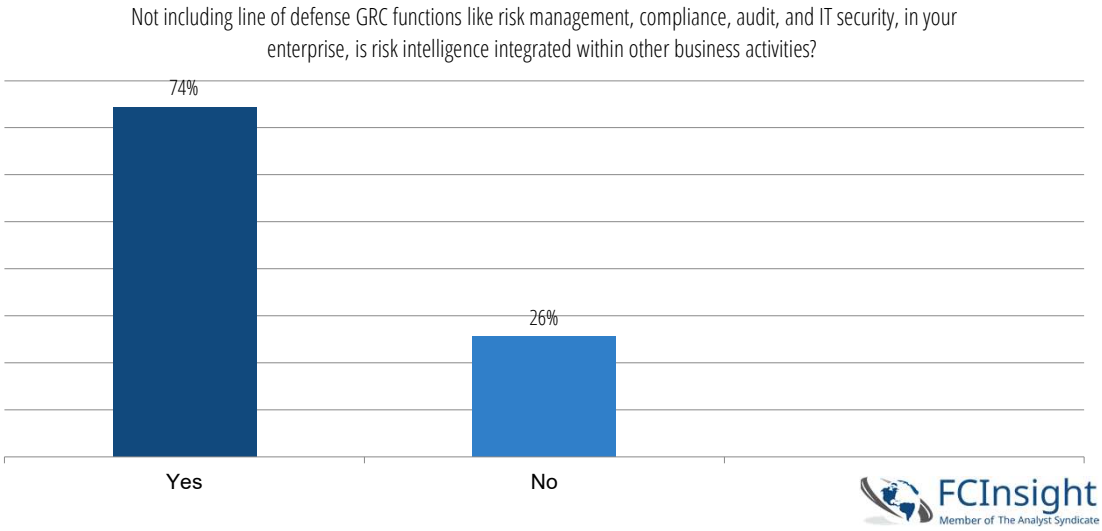


Top areas where majority of respondents spend 25% or more of their time:

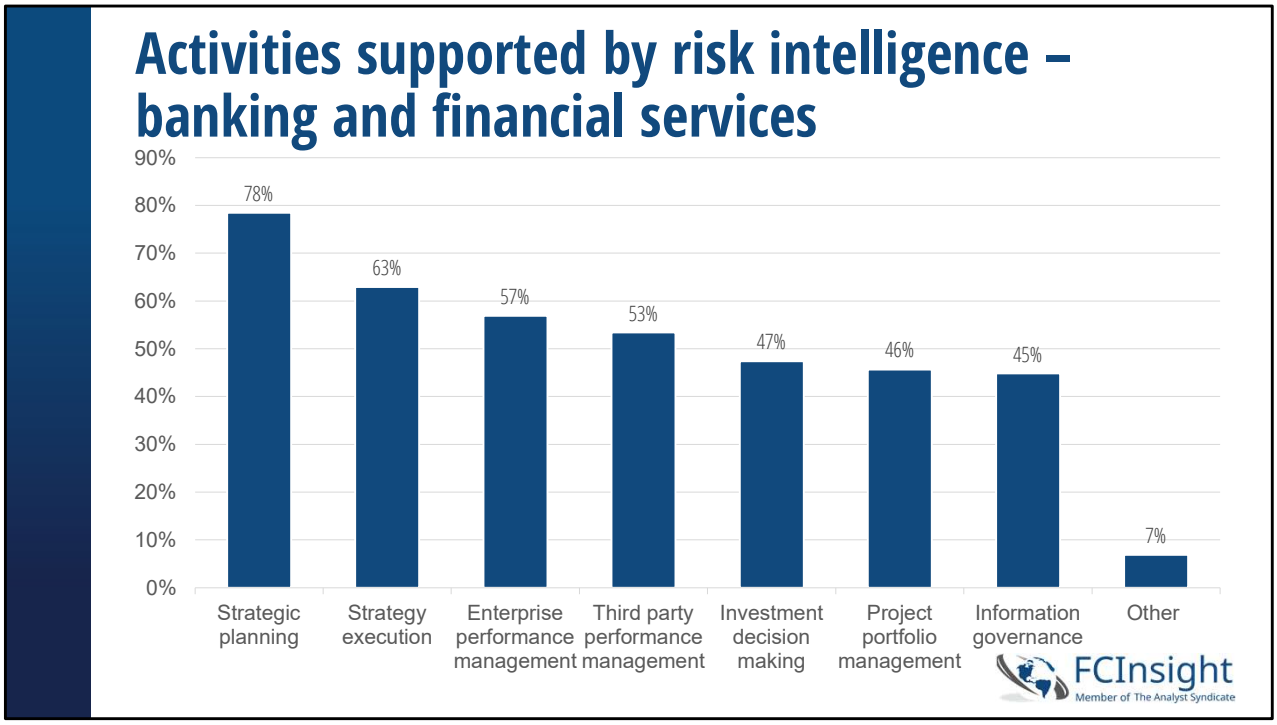
- C-level – Executive management, ERM
- Sr. managers – ERM and ORM
- Middle managers, supervisors and subject matter experts – ERM, ORM, Compliance

Despite a significant amount of C-level time being spent on IT risk management, very little time was spent by respondents on IT management. Compare the time spent on executive management to the time spent on IT management. This lack of executive and management attention on IT management may indicate that IT governance is not getting the attention it deserves.

Integrating risk intelligence into business – banking and financial services

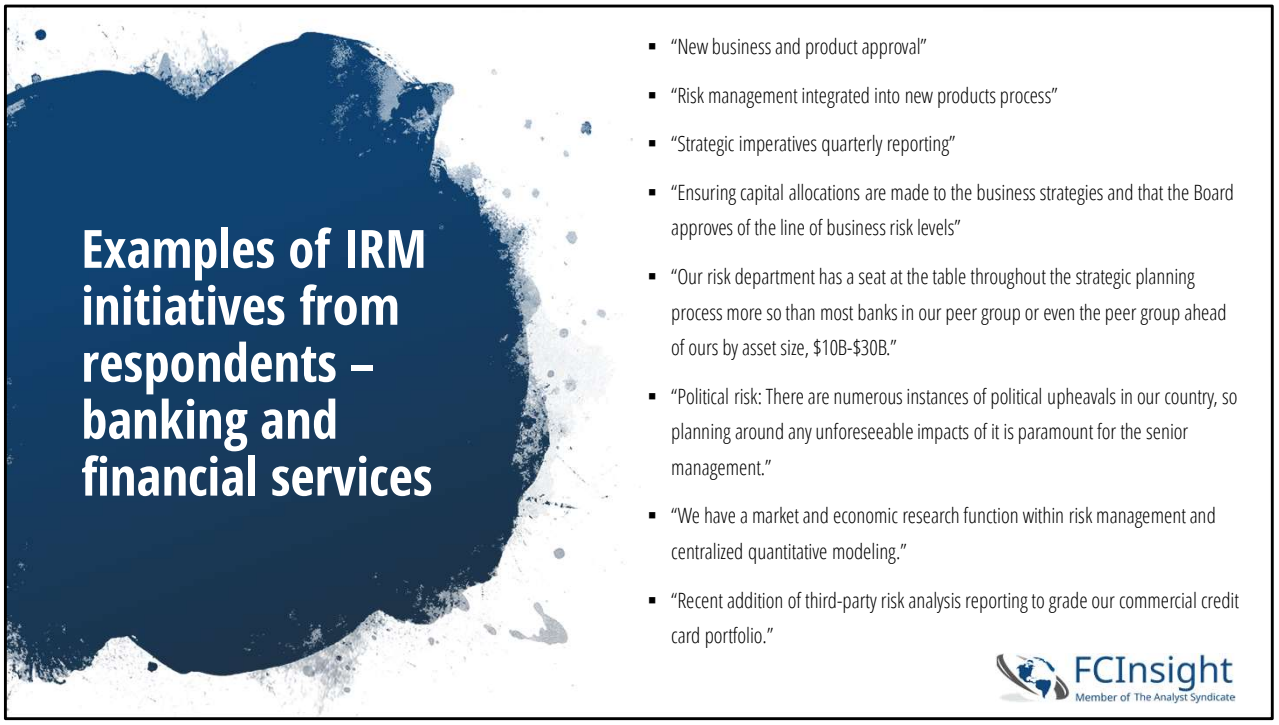


74% of respondents reported that they are integrating risk intelligence into other business activities beyond line of defense type functions. This is a very large number as compared to just 6 years ago when similar surveys reported percentages in the single digits and teens. Within financial services, some of this dramatic increase can be accounted for from the increased emphasis on risk management by the OCC and other financial services regulators.

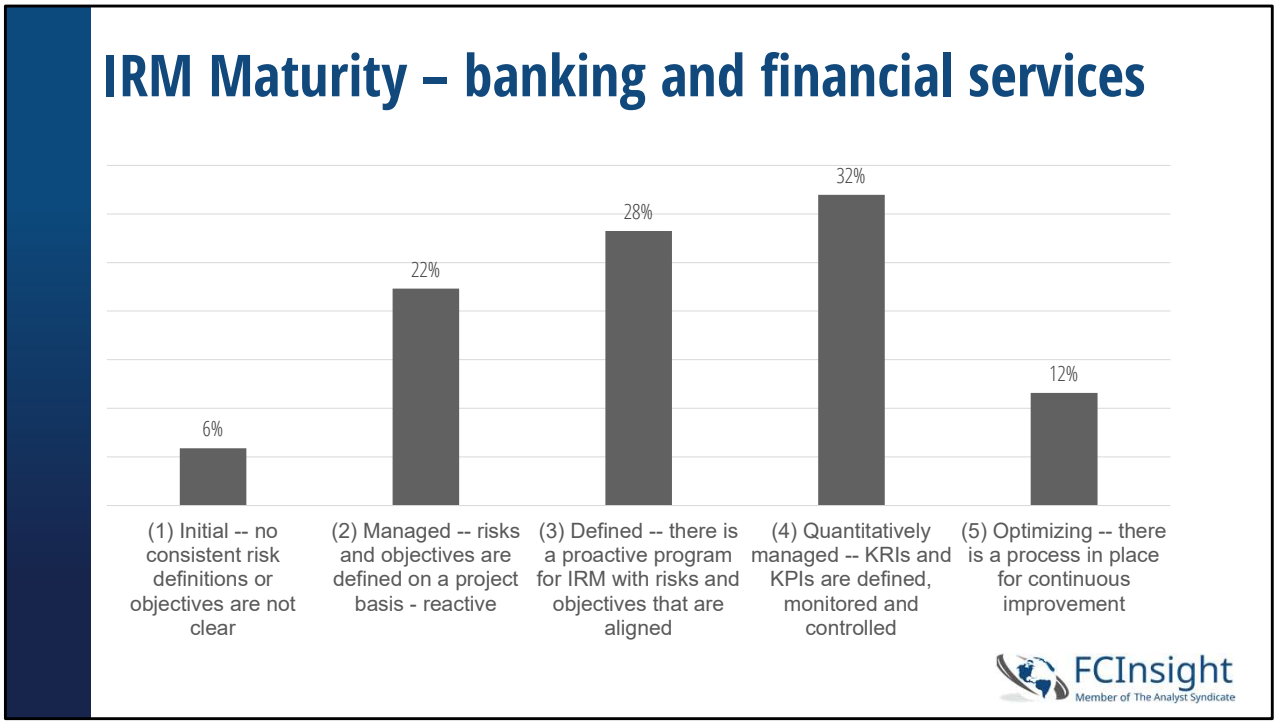


With board attention on risk management and strategic initiatives, strategic planning is a likely area of focus for IRM. It is also the easiest area in which to get started on IRM.

Risk intelligence is often not as timely as business intelligence. Much risk intelligence is often collected quarterly, annually or even less frequently – that is it is collected from compliance testing and auditing. However, when it comes to strategic planning exercises, which are done annually with at best quarterly updates, dated risk intelligence is adequate. Getting timely risk intelligence for operational objectives such as strategy execution and enterprise performance management is another matter. For example, EPM reporting occurs monthly, weekly and sometimes even on-demand, which requires sources of business and risk intelligence that are updated as rapidly as possible.

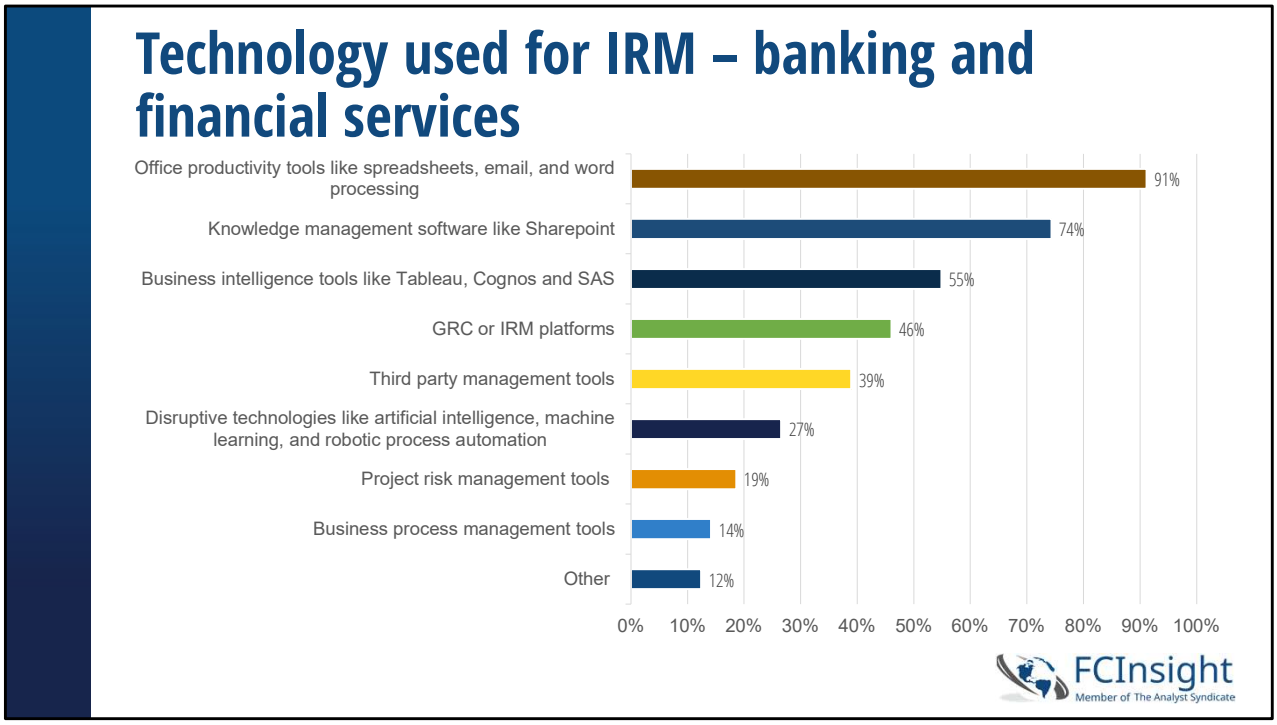


Respondents were asked to cite examples of IRM within their own enterprises. New product processes and strategic planning were often cited.



72 % of respondents claimed that IRM maturity was at level 3 or higher on a 5-level scale – that is, it was relatively mature. Rather than being a program like ERM or cybersecurity, IRM is initiative based. That is, provisioning of risk intelligence to other business activities or programs becomes a part of that other activity or program, that than being a standalone program itself. Being initiative based, the low number optimizing is not surprising.

Risk management and business professionals seeking to optimize IRM should consider standing up a cross-functional center of excellence that includes members from ERM, cybersecurity, and other compliance and risk management programs, as well as members from business activities that benefit from IRM. For large enterprises that center could include a small number of full-time professionals.



Office productivity tools and KM tools like SharePoint are commonly used in many disciplines and IRM is no exception to that. Note that BI tools are more commonly used than GRC. Respondents also rated fitness for purpose of BI tools higher than GRC.

Some GRC vendors have re-labelled themselves as IRM vendors, and most others claim to have IRM solutions. However, automating IRM reporting requires that risk intelligence be integrated with business intelligence. BI tools are much better than GRC tools for pulling data from multiple sources and visualizing it for analytical and reporting purposes. This is unlikely to change in the next 5 years, and in fact, to truly support IRM, it is not necessary for GRC vendors to focus on the analysis of business and risk intelligence. Rather they should focus on provisioning timely and high-quality risk intelligence, and seamless integration with a variety of analytical and BI tools.

In financial services industries, the use of BI and GRC correlated to higher IRM maturity. Overall, 72% of respondents reported IRM maturity as level 3 or higher on a 5-point scale. For those using BI tools, level 3 or higher was also 76%, for GRC tool users, it was 79%, and for those using both BI and GRC, 82% reported IRM maturity at level 3 or higher.

Other industries

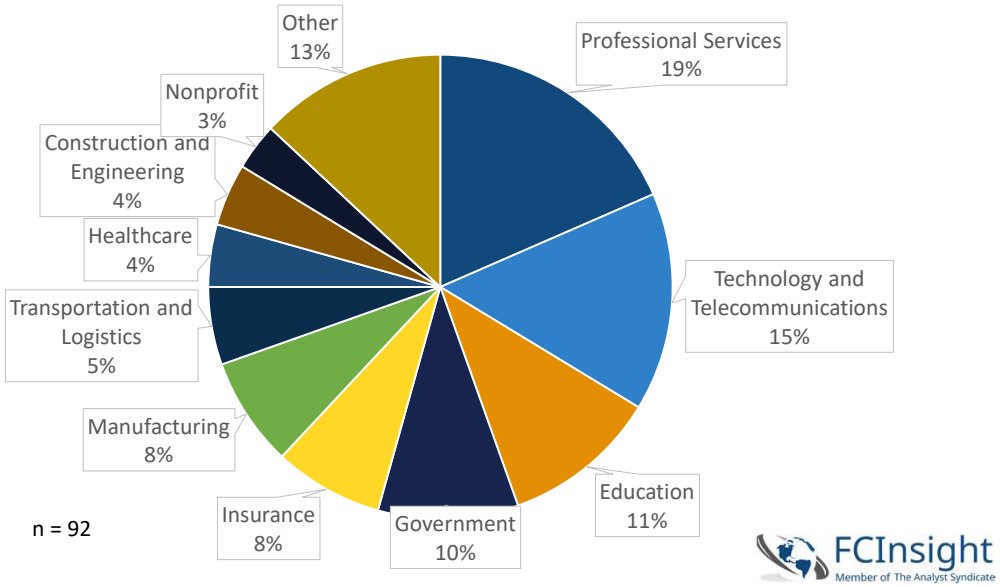
Key findings – non-financial services

- 66% of respondents report they are integrating risk intelligence into business activities
- 80% report strategic planning as a top objective for IRM, but only 45% report strategy execution as one
- Most respondents spend 25% or more of their time on ERM – true for all seniority levels
- Respondents rated IRM as relatively mature, 16% claim to be optimizing IRM
- Business intelligence applications are just as likely as GRC technology to be used in IRM initiatives
- The use of BI and GRC tools did not correlate to greater IRM maturity.

FCInsight
Member of The Analyst Syndicate

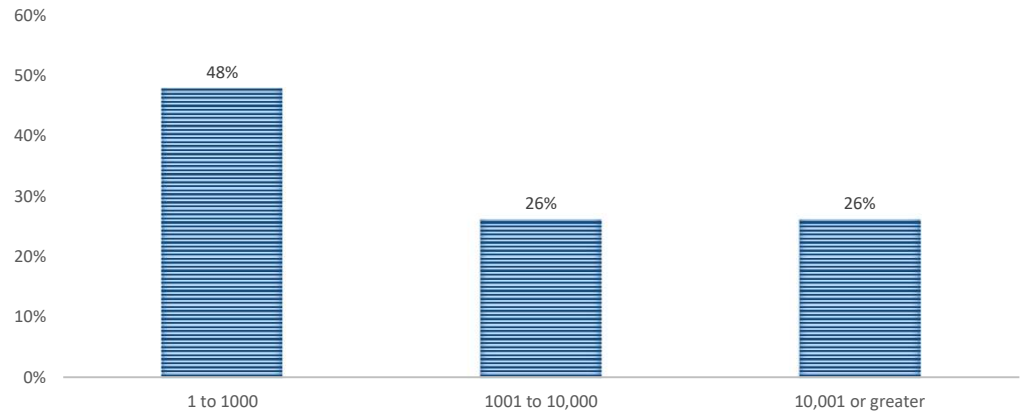
A separate analysis of survey results was conducted for industries other than financial services. While financial services was expected to have a high degree of IRM activity, with 66% of non-financial services respondents reporting that they are integrating risk intelligence into other business activities, the results for non-financial-services industries were high as well.

Industries of non-financial services respondents



Professional services, technology and telecommunications, education, government, insurance, and manufacturing had the most survey respondents, but no single industry dominated the non-financial services respondents to the survey.

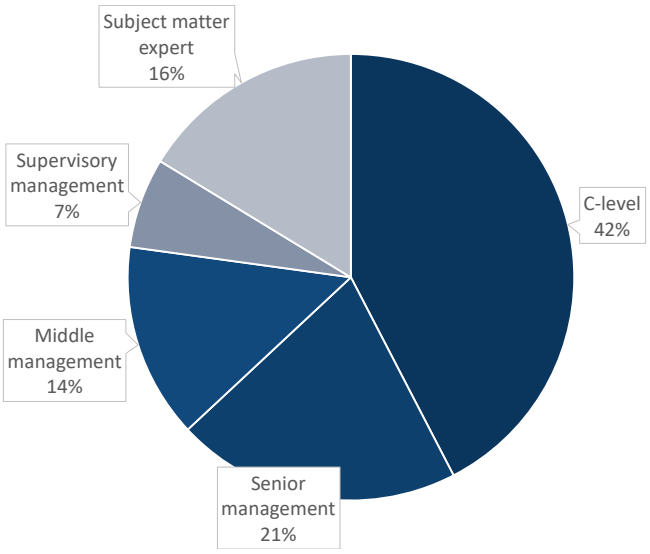
Size of firm – non-financial services (number of employees)



FCInsight
Member of The Analyst Syndicate

Small, mid-sized and large enterprises were all well represented in the survey, though small businesses were almost half of the respondents.

Seniority of participants -- non-financial services

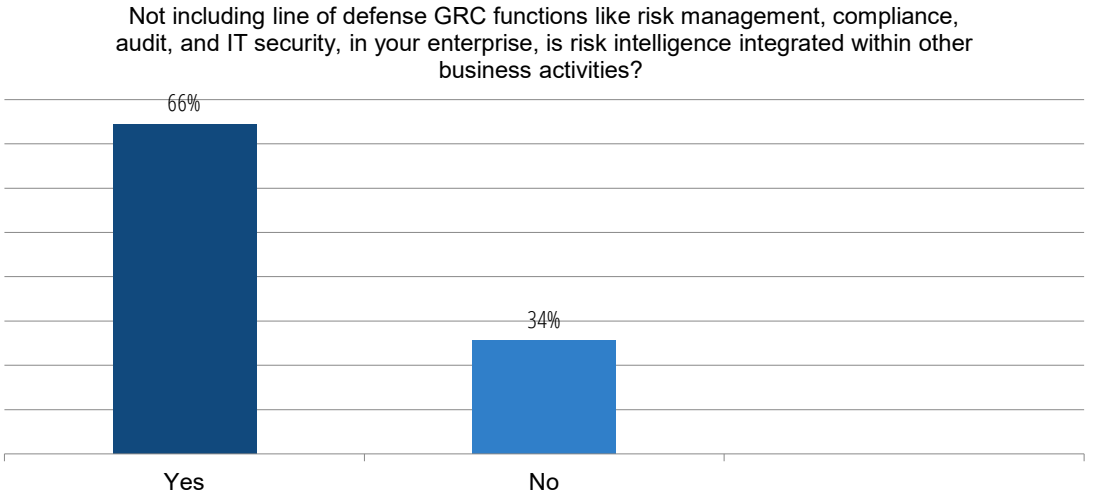


C-level respondents	
Chief Executive Officer	23%
Chief Risk Officer	18%
Chief Audit Executive	18%
Chief Information Officer	13%
Chief Information Security Officer	8%
Chief Operations Officer	3%
Chief Compliance Officer	3%
Non-executive Corporate Director	3%
Other	13%

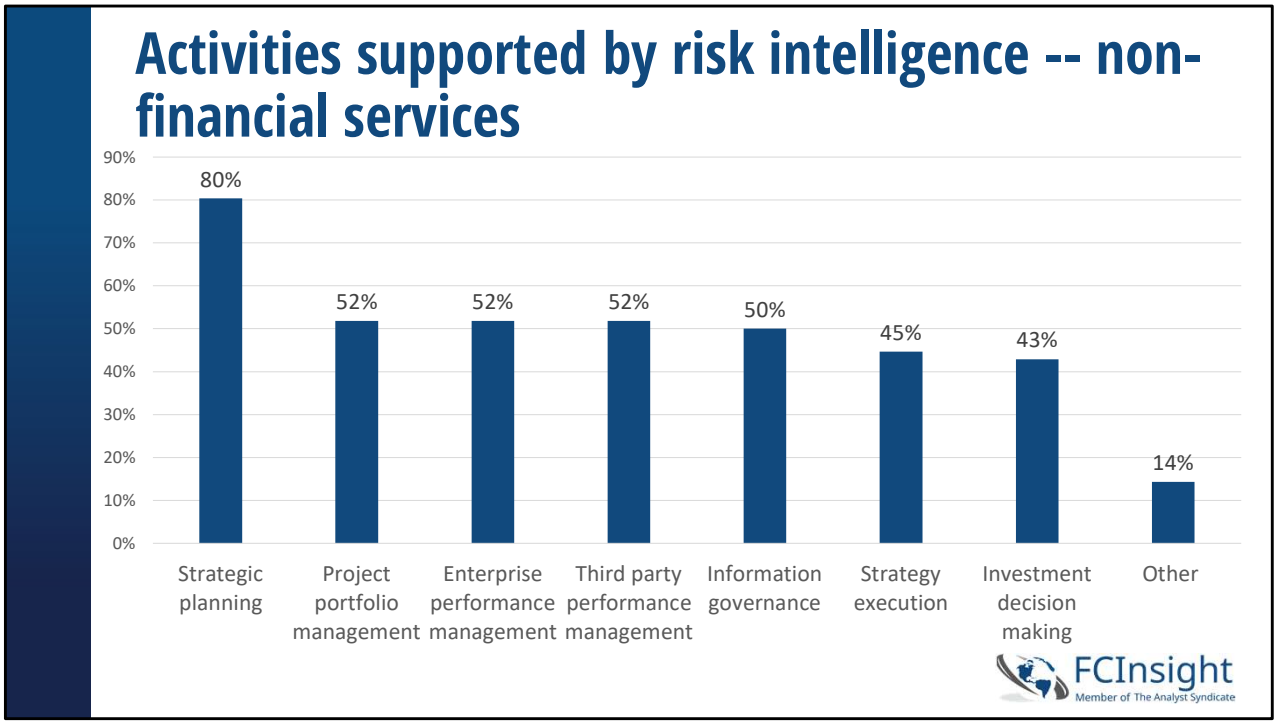
FCInsight
Member of The Analyst Syndicate

As with the financial services part of the survey, the relative high number of C-level and senior management participants from non-financial services enterprises indicates high interest in IRM.

Integrating risk intelligence into business -- non-financial services

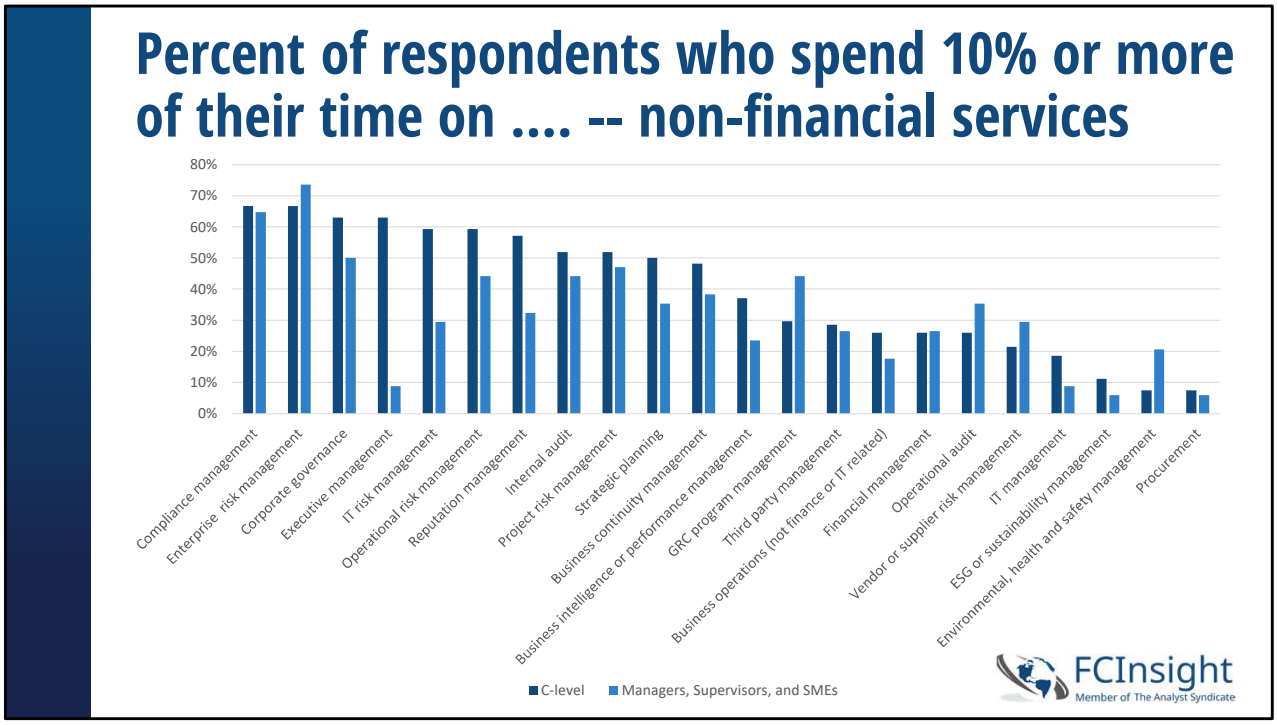


66% of respondents in non-financial services enterprises reported that that risk intelligence is being integrated into business activities other than line of defense type functions, such as audit, compliance, and cybersecurity. This is lower than the 78% of respondents in financial services, but still represents a significant amount of IRM activity.



80% of respondents reported that strategic planning was supported by risk intelligence, while only 45% cited strategy execution. This gap could indicate that risk management professionals in many enterprises are not involved most of the time in ensuring that strategic objectives are well executed.

Frankly, there is little point in supporting strategic planning with risk intelligence if risk intelligence is not also provisioned to those activities that are essential to executing on the business strategy. Unfortunately, in many enterprises, risk intelligence is dated and therefore of minimal use to those who are accountable for the decision making on execution of the strategy. Risk management leaders should focus on improving the timeliness and quality of risk intelligence.



Areas where majority of respondents spend 25% or more of their time

- C-level – ERM, compliance, corporate governance, executive management
- Sr. managers – ERM, Corporate governance, compliance
- Middle management, supervisors, subject matter experts – ERM, compliance, internal audit

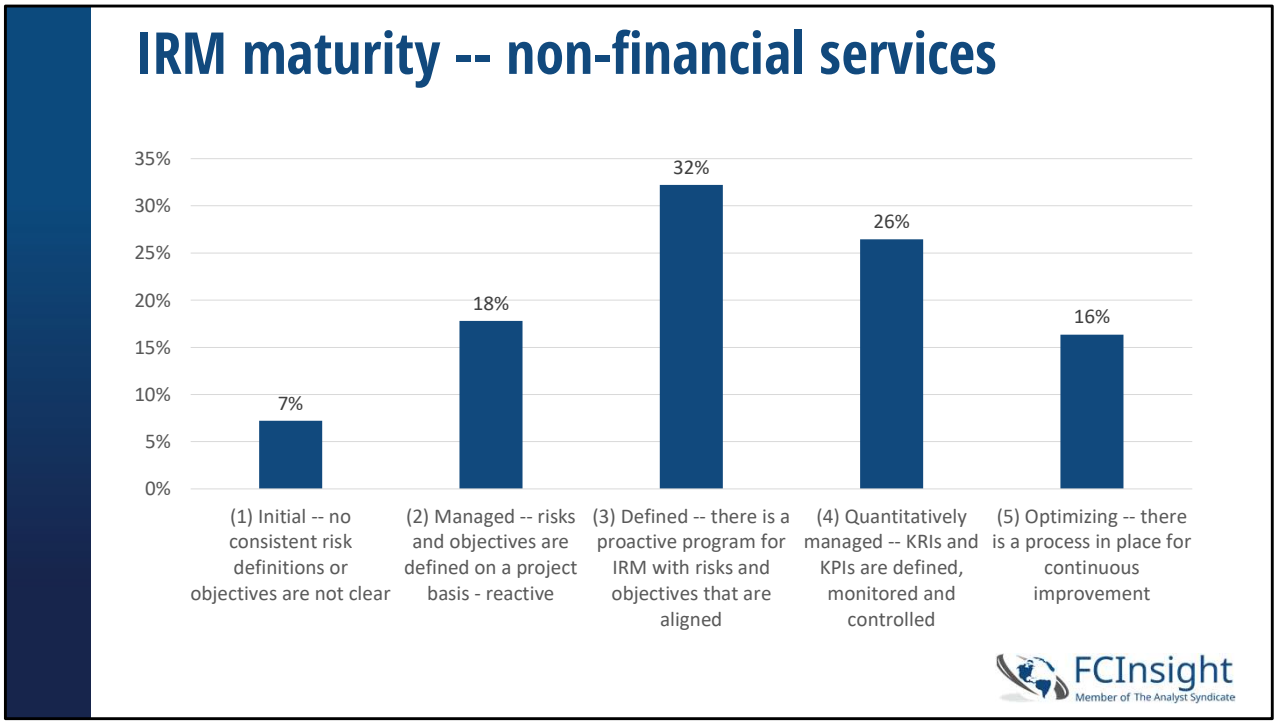
The high amount of time spent by respondents on compliance could indicate less emphasis on IRM and more on risk management as a compliance activity.

Examples of IRM initiatives from respondents -- non-financial services

- "Corporate governance, investor relations, compliance risk and security, budgeting and CSR teams are working together to measure the Enterprise wide strategic, sustainability, operational, financial and cyber risks "
- "We directly utilize processes and our platform to be integrated with specific business objectives and further tie those business objectives to compliance and security mandates. Additionally, we utilized our adaptive governance model to gain intelligence from vulnerability management, threat management and are able to do predictive analytics in real-time"
- "Enterprise-wide risk identification and assessment program conducted by ERM that supports enterprise risk reporting to Board and capital planning activities"
- "Stress testing/scenario analysis to determine optimal share buy-back, dividend payment and other strategic liquidity needs"
- "Continuous monitoring/management of risk in a large digital transformation program"
- "Embedding risk into strategic project assessments"
- "Strategic plan assessment"

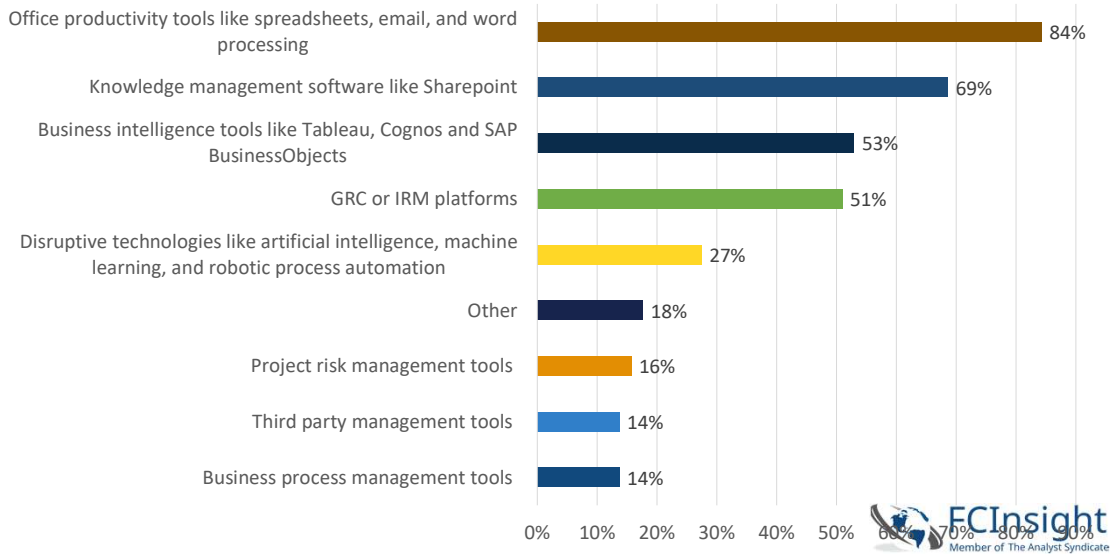
FCInsight
Member of The Analyst Syndicate

Respondents were asked to share specific examples of IRM in their enterprises. Answers emphasized the alignment with enterprise strategic and business objectives.



74% of respondents reported that IRM maturity was at level 3 or higher on a 5-level scale.

Technology used for IRM -- non-financial services



Office productivity tools and KM tools like SharePoint are commonly used in many disciplines and IRM is no exception to that. Note that BI tools are more commonly used than GRC. Respondents also rated fitness for purpose of BI tools higher than GRC.

Some GRC vendors have re-labelled themselves as IRM vendors, and most others claim to have IRM solutions. However, automating IRM reporting requires that risk intelligence be integrated with business intelligence. BI tools are much better than GRC tools for pulling data from multiple sources and visualizing it for analytical and reporting purposes. This is unlikely to change in the next 5 years, and in fact, to truly support IRM, it is not necessary for GRC vendors to focus on the analysis of business and risk intelligence. Rather they should focus on provisioning timely and high-quality risk intelligence, and seamless integration with a variety of analytical and BI tools.

In non-financial services industries, the use of BI and GRC tools did not correlate to higher IRM maturity. Overall, 74% of respondents reported IRM maturity as level 3 or higher on a 5-point scale. For those using BI tools, level 3 or higher was also 74%, for GRC tool users, it was 78%, and for those using both BI and GRC, 77% reported level 3 or higher.

While there was no statistical correlation between tool usage and IRM maturity, it should be noted that the proportion of respondents applying IRM for strategy execution was much lower in non-financial-services than it was in financial services organizations. This could mean that non-financial services organizations are not relying as heavily on business analysis of risk and business intelligence.

Charitable donations

Thanks for your participation

- In gratitude for your participation, we have made donations to three charities
- Respondents designated donations to the following charities:
  - Australian Wildfire Fund -- $500
  - Hurricane Dorian Recovery Fund -- $300
  - Red Cloud Indian School -- $200

FCInsight
Member of The Analyst Syndicate

Follow-up

Follow-up

- Benchmark your organization or discuss results
  - french@fcinsight.com
  - Schedule a call: IRM survey follow-up

FCInsight
Member of The Analyst Syndicate