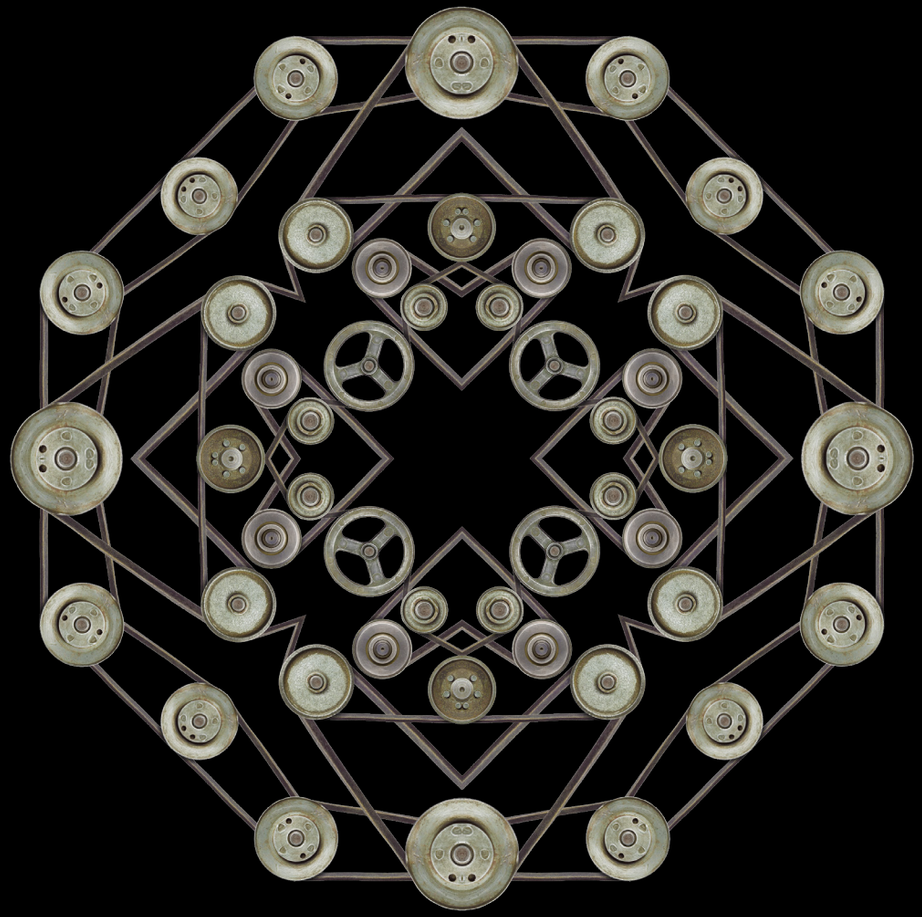
Deloitte.



All together now

Third party governance and risk management

Extended enterprise risk management global survey 2019

Foreword

Welcome to our annual global survey on Extended Enterprise Risk Management (EERM). We started this survey four years ago to share experiences, opportunities and challenges as organizations take their journeys toward EERM maturity; where the approach to third-party risk management is integrated and consistent across the organization, and led from the top[1].

I am proud to say that this year we attracted our largest number of respondents yet – 1,055[2] from 19 countries around the world[3]. This reflects an increasingly high interest and leadership focus on third-party risk management.

Our survey took place between November 2018 and January 2019, and the sentiment of this period is reflected in the results. Signs of a slowdown in global economic growth were beginning to emerge, together with an atmosphere of greater organizational uncertainty. The survey reveals how organizations are recognizing this change by making greater efficiencies.

This year's key findings are:

- The desire to reduce costs has become the biggest driver for investing in EERM maturity, followed by reduction in third-party incidents, regulatory, and internal scrutiny.
- Chronic underinvestment is making it hard for organizations to achieve their desired EERM maturity levels, and more fundamentally, hindered many organizations from doing basic core tasks well. Not being "brilliant at the basics" means the full benefits from cutting-edge initiatives and solutions can't be realized.
- The pursuit of efficiency is driving organizations to embrace a number of solutions. These include federated structures – where central senior leadership, organizational units, and country teams share responsibility; emerging technologies; shared assessments, and utilities; and managed services delivery models. Organizations are also standardizing and simplifying enabling technologies.
- Boards and executive management continue to take a deep interest in third-party risk management and want to provide more coordinated and responsive input. This is reflected in their investment in actionable intelligence and desire to pool and analyze information on all risks and across the whole organization.
- A new insight is that organizations are increasingly aware that if they are going to improve EERM, they need to spend enough money to recruit experienced, and therefore expensive, EERM leadership.

I hope the wealth of information in this report will further enhance your understanding of prominent EERM trends and developments as you navigate your organization on its EERM journey.

Kristian Park
EMEA Leader, Extended Enterprise Risk Management
Global Leader, Third-party Risk Management
Global Risk Advisory

Robust EERM governance is imperative to an organization's success

Organizations are trying to improve the management of third-party risk by investing in talent, cutting-edge technologies, and robust operating models. Dramatic shifts in the marketplace and push for efficiencies are contributing to an ever-increasing focus on EERM.

With a staggering 83 percent of organizations experiencing a third-party incident in the past three years and only a negligible 1 percent considering themselves "optimized" to address all important EERM issues, it evidently reflects underinvestment in the EERM space.

While 20 percent of respondents claim they are addressing most of the EERM elements, and 50 percent put themselves in the "managed" category, our findings, however, show that these are piecemeal investments focused more on targeted tactical improvements rather than strategic long-term solutions.

Our 2019 survey reveals that boards are championing an inside-out approach to EERM, which includes better engagement, coordination, and smarter use of data. Leaders are also aspiring for greater innovation. This year we've seen the emergence of more succinct and real-time actionable intelligence, generated online, for boardroom reporting on third-party risks.

More sustainable operating models for third-party risk management are being embraced – these are characterized by federated structures that are supported by centers of excellence and shared service centers, emerging technologies, shared assessments and managed services models, and a move toward co-ownership of budget.

Our prediction around the growth of a tiered way forward for standardized technology investments in EERM has turned out to be true. Organizations prefer to streamline and simplify third-party risk management technology across diverse operating units.

We believe the severity of consequences of negative actions by third parties to an organization's reputation, earnings, and shareholder value will continue to increase, and this will drive organizations to invest in improving their EERM processes and frameworks.

A clear line of EERM governance is imperative to the overall success of the organization. Senior leadership can play a crucial role in creating an accountable EERM organization that is set up to mitigate third-party risks, improve compliance, and avert reputation damage and regulatory missteps.

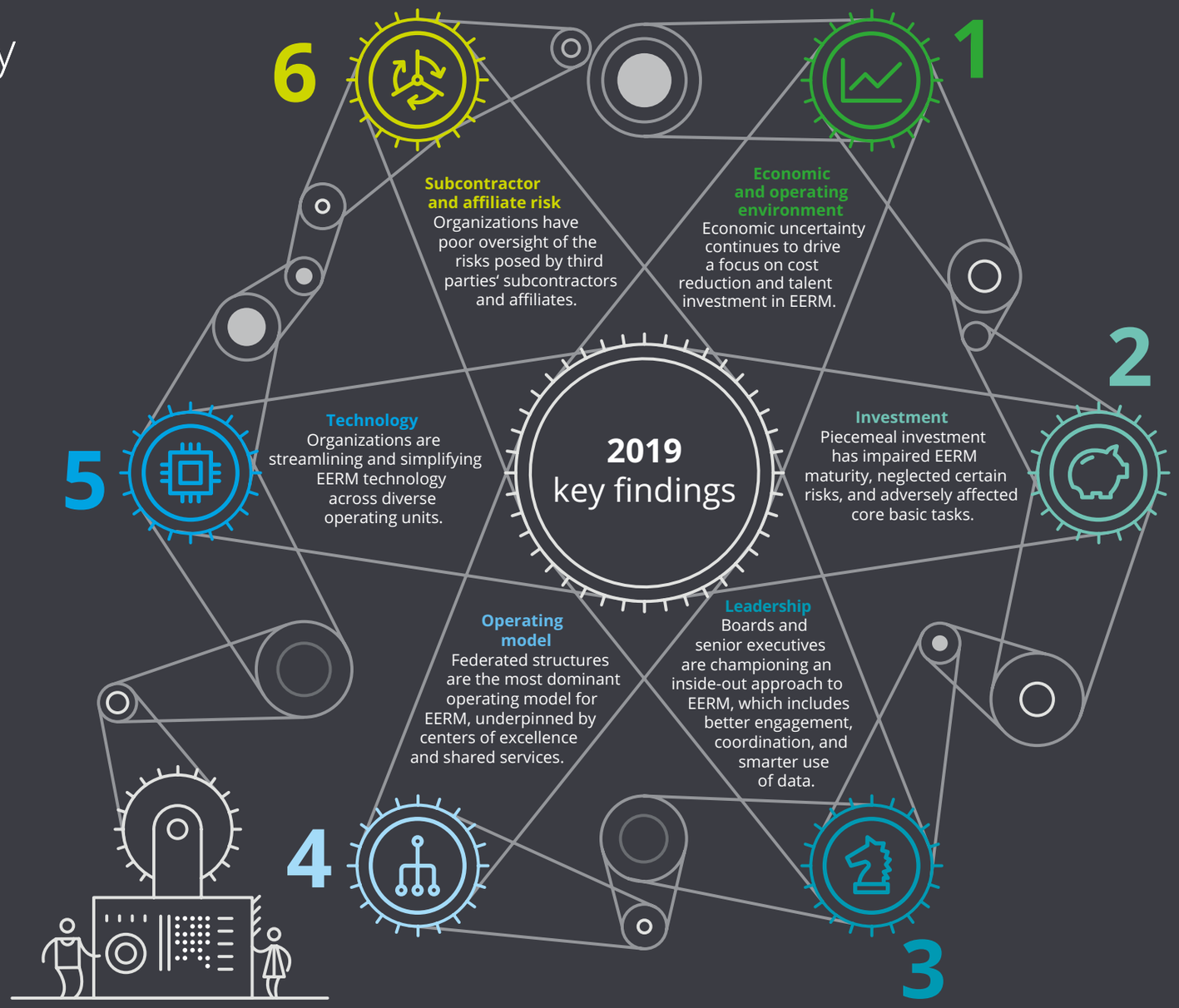
Our risk advisory professionals across the globe can help you understand more about this survey and how the findings relate to distinctive opportunities for your organization.

To learn more, please visit us at www.deloitte.com/risk.

Donna Glass
Managing Partner, Deloitte Advisory US
Business Leader, Deloitte Global Risk Advisory

Executive summary

There is renewed focus on maturing EERM practices within most organizations. This appears to be driven by a recognition of underinvestment in EERM, coupled with mistrust of the wider uncertain economic environment.



1 Executive summary

Economic and operating environment

Executives responded to the survey between November 2018 and January 2019, a time of economic uncertainty that has made its mark on the outlook for businesses.

This uncertain economic and business outlook affects EERM by forcing organizations to:

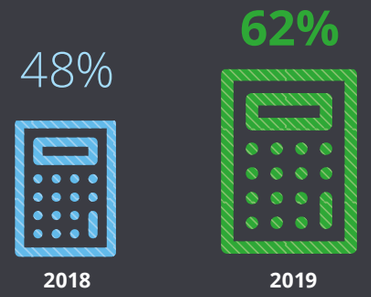
- Challenge EERM budgets and investments;
- Increase operational efficiency to reduce costs; and
- Rethink their strategy for what to engage third parties for.

There is also increased scrutiny from two directions:

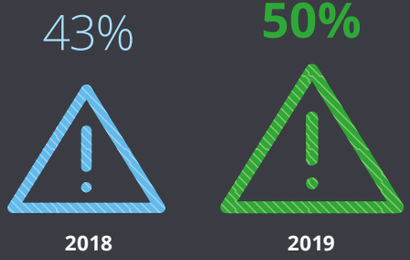
- **Externally.** Regulators globally expect organizations to have established third-party risk management frameworks and have progressed on their journey.
- **Internally.** More progressive organizations have set up internal compliance mechanisms mirroring the scrutiny applied by regulators.

Organizations have clear motives for investing in EERM:

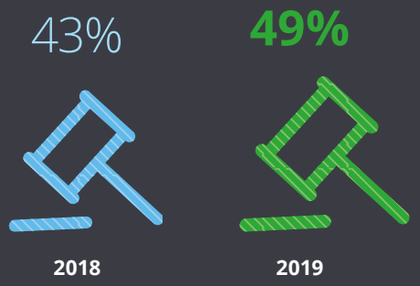
Cost reduction remains top. It was cited by **62 percent** of respondents, up from 48 percent last year.



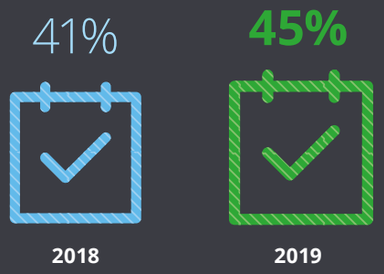
Value preservation comes second: "reduction in number of third-party related incidents" was chosen by **50 percent** of respondents, up from 43 percent last year.



Organizations are more worried about regulatory scrutiny than last year: **49 percent** cite it, up from 43 percent.

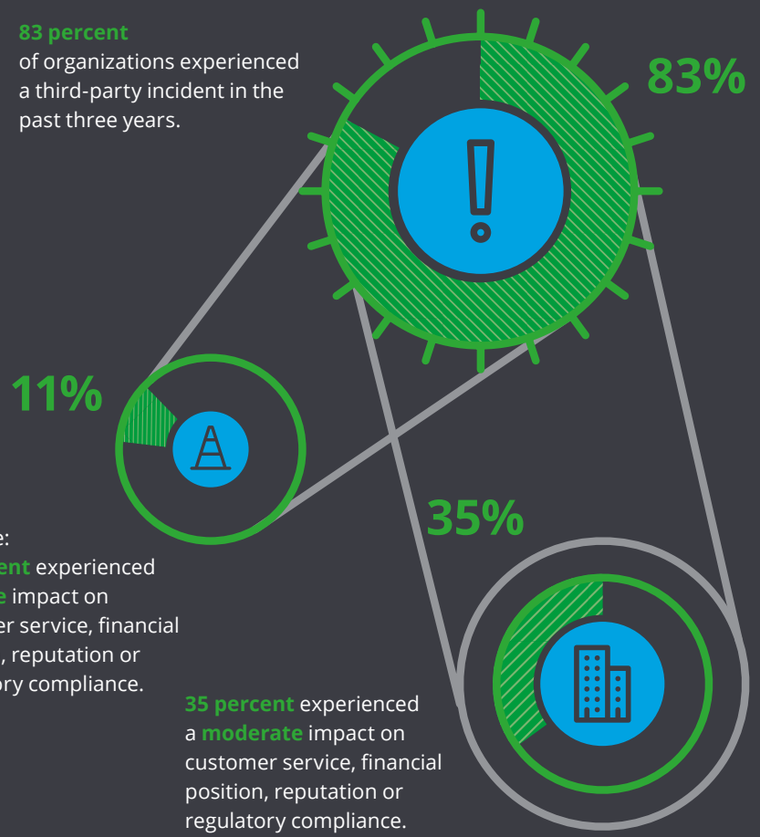


Organizations are motivated even more by internal compliance requirements than before. This was given as a reason by **45 percent**, up from 41 percent.



Third-party incidents continue to cause disruption with varying impact:

83 percent of organizations experienced a third-party incident in the past three years.



Of these:
11 percent experienced a **severe** impact on customer service, financial position, reputation or regulatory compliance.

35 percent experienced a **moderate** impact on customer service, financial position, reputation or regulatory compliance.

What is damaging confidence in an organization's EERM?

A lack of a coordinated and consistent EERM approach across organizations was cited by **53 percent** of organizations.

Followed by fears about processes, technology, and real-time management information for EERM, at **49 percent**.

Respondents feel an urgent need to be coordinated and consistent in EERM across their organization and improve processes, technologies and real-time management information across all significant risks.

An interesting new insight is that leadership realizes that, despite budget pressures, EERM ambition requires talent investment: spending money now to save money later. This is largely about recruiting expertise. The survey identifies different orders of priority:

- Recruiting more experienced and expensive EERM leaders to coordinate initiatives is higher.
- Recruiting for junior EERM skills is lower. This is probably due to the rise and availability of third-party services and utility models. Only 30 percent cited this as a priority this year.

30%

2 Executive summary

Investment

Most organizations believe they are underinvesting in EERM:

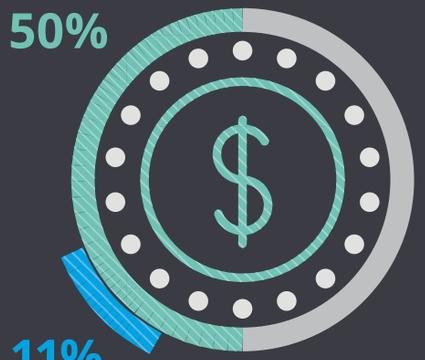
Fewer than **three** in 10 think that their capital expenditure on EERM is the ideal amount or more.

Fewer than **three** in 10 think they are spending the ideal amount or more on EERM staff and other operating costs.

Annual operating expenditure on EERM varies significantly between organizations:

Annual operating expenditure on EERM activity has varied significantly, depending on industry, management, EERM delivery models, and so on.

50 percent spend more than US$1 million[5].



The top **11 percent** spend more than US$10 million each and employ more than 100 FTE staff.

Piecemeal investment has impaired EERM maturity:

We have tracked organizational investments in EERM maturity over the last four years. This longitudinal study shows that many organizations have made limited piecemeal investments focused on targeted tactical improvements, rather than investing more strategically in longer-term solutions.

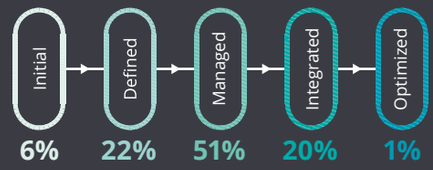
Only **1 percent** of organizations consider themselves "optimized", addressing all important EERM issues.

Another **20 percent** say they are "integrated: they are not best in class, but have addressed most EERM elements.

51 percent put themselves in the "managed" category: they have considered all important elements, but see room for improvement.

22 percent consider themselves "defined", some elements are addressed but with limited effort.

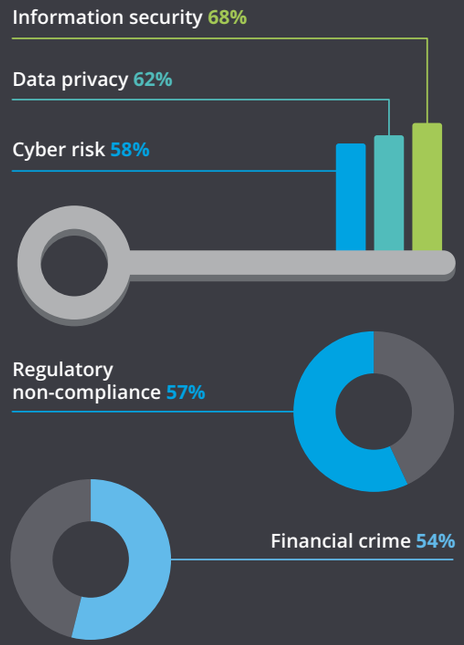
6 percent say they are "initial", none or very few of elements addressed.



See figure 2.5 for Deloitte's EERM maturity model.

Investment is skewed towardcertain risk domains:

Annual investments have typically focused on the largest regulatory issues of the year. For example, information security, data privacy, cyber risk, and financial crime in 2018 and 2019. Organizations most commonly allocate EERM budget to:



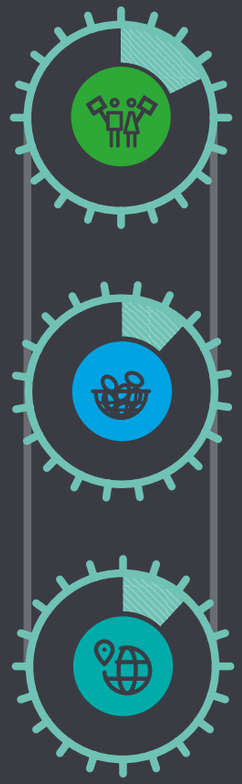
This piecemeal approach has neglected certain areas of risk:

Organizations are failing to review critical areas annually:

Almost half of organizations do not review concentration risk every year. This tends to be reviewed reactively via reporting as opposed to proactively as part of the EERM process.

More than **60 percent** of organizations do not review exit plans for critical third parties every year.

Organizations are underinvesting in certain areas:



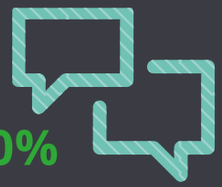
Only:

18 percent invest in labor rights

12 percent in concentration risk

12 percent in geopolitical risk

Underinvestment in EERM has weakened the ability to be "brilliant at the basics":



50%

50 percent of organizations do not understand the nature of individual third-party relationships.

43%

43 percent lack enough knowledge of contract terms.

41%

41 percent do not monitor third parties based on their risk profile.

This limits the benefits from more cutting-edge solutions and hampers attempts to ensure risk management efforts are proportionate to the risk.

3 Executive summary

Leadership

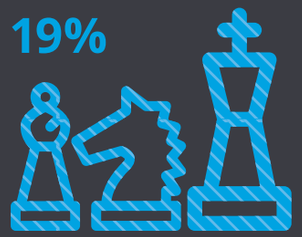
Boards and senior executives are ultimately accountable for EERM in the vast majority of cases as organizations continue to recognize third-party risk management as an integral part of strategy setting.

Responsibility rests most commonly with the chief risk officer – in **24 percent** of cases.

24%

Board members are responsible in **19 percent** of organizations.

19%



The CEO is responsible in **17 percent** of organizations.

17%

Leaders are raising the bar through emerging technologies:

Last year's survey identified that senior leadership were favoring red-amber-green (RAG) dashboards to inform their discussions at board and executive committee meetings. At that time, most organizations used static RAG reports, analyzing related third-party data periodically.

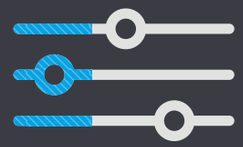
The latest survey, however, shows that senior leaders are moving from using periodically generated data to more succinct and real-time actionable intelligence, generated online.

New risk intelligence tools are assimilating, aggregating, and examining real-time automated information on all risks across an entire organization. The tools provide alerts, trend analysis, enable scenario analysis, and use emerging technologies such as the cloud, robotics process automation, and artificial intelligence.

This is happening at a time when regulators are starting to encourage innovation in risk management and oversight.

56 percent of organizations are using or intend to use cloud-based platforms for EERM.

56%



45 percent are using or intend to use robotics process automation.

45%

36 percent are using or intend to use visualization techniques to create actionable intelligence.

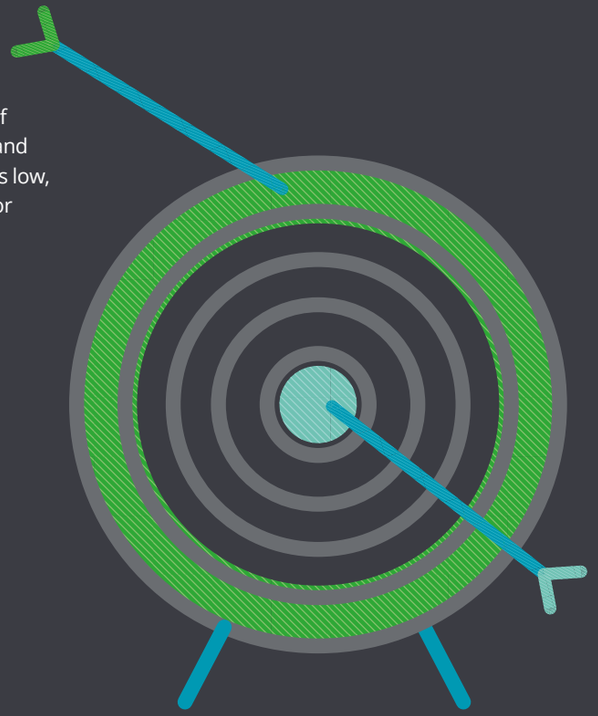
36%

Boards are now championing an inside-out approach to EERM in addition to the historical outside-in approach. This starts with better engagement and coordination within the business, encompassing organizational units, geographies, risk domains, and subject matter experts.

Many organizations admit to poor engagement and coordination among their internal EERM stakeholders...

35%

35 percent say the level of engagement and coordination is low, insignificant, or unknown.



16%

Only **16 percent** of organizations believe it is high.

... but they want to make it better:

Two in three organizations list better in-house engagement and coordination as a priority action item in EERM.

37%

37 percent make it the top priority.

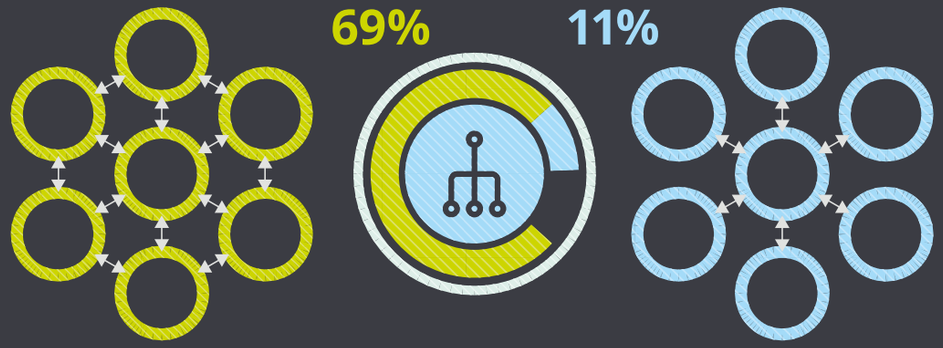
4 Executive summary

Operating models

Federated structures are becoming the most dominant operating model for EERM. The majority of respondents said their organization has now adopted this model, where strong central oversight is combined with accountability held by organizational units or leaders in different countries, reinforced by a combination of central policies, standards, services, and technologies.

69 percent say they are adopting a federated model.

Only **11 percent** of organizations are highly centralized, down from 17 percent last year.



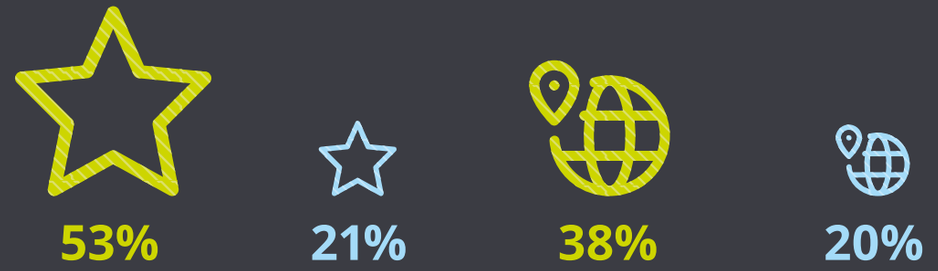
Federated structures are often:

- Underpinned by a center of excellence or shared services capability
- Increasingly supported by a managed service (which reduces both headcount and capital spending), emerging technologies, and shared assessments and utilities.

Organizations increasingly use centers of excellence and shared service centers:

53 percent of organizations use centers of excellence, and a further **21 percent** intend to create them.

38 percent have shared service centers, and a further **20 percent** aspire to establish them.



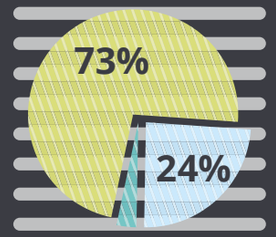
Managed services are an emerging trend:

18 percent of organizations use an external managed services provider with **staff on the premises.** A further **13 percent** intend to.

18 percent of respondents use managed services to **acquire risk intelligence,** another **21 percent** plan to.

11 percent use managed services solutions that deploy **EERM as a service,** another **14 percent** plan to.

The growing use of technology, managed services, and utility models will drastically reduce capital spending (capex):



73 percent of organizations think cumulative capital costs should not exceed their annual operating cost, once these next-generation solutions are adopted.

A further **24 percent** believe they should come down to two or three times annual operating costs.

This is a sharp decline from respondents' estimate last year that cumulative EERM capex is typically three to five times annual operating cost.

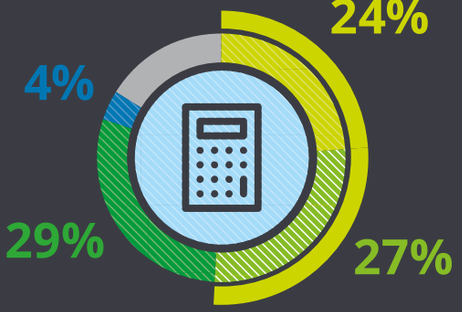
The remaining **3 percent** believe that this will still remain more than three times annual operating costs.

Co-ownership of budget is another new trend:

Ultimate budget control is retained by organizational leaders and other central first-line functions such as procurement. More than half (**51 percent**) of organizations said it was retained by the CEO/executive leadership/board (**24 percent**) and procurement (**27 percent**)

But it is increasingly being co-owned by organizational units (**29 percent**) and geography leadership (**4 percent**). These areas have a say over EERM budgets specific to their fields.

This approach is enabling organizations to be agile and consistent.

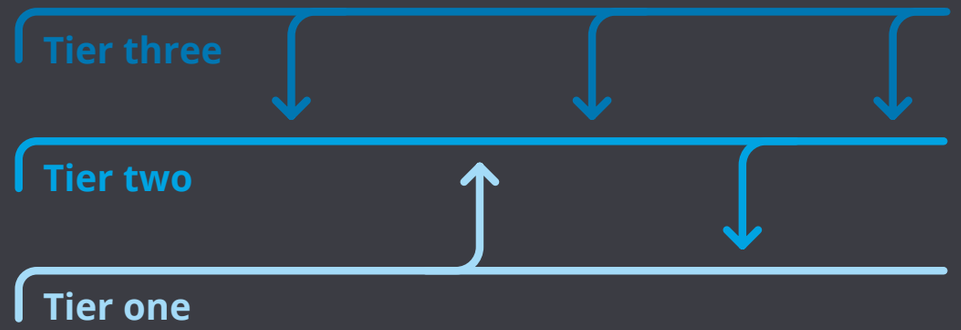


5 Executive summary

Technology

Last year we predicted that organizations will begin to take EERM technology decisions centrally and we highlighted the emergence of a standard three-tiered technology architecture. This year's survey shows that both of these stand true and that within the three-tiered technology architecture, organizations are increasingly streamlining and simplifying specific technology solutions for EERM.

The evolving tiered architecture for EERM tools and technologies



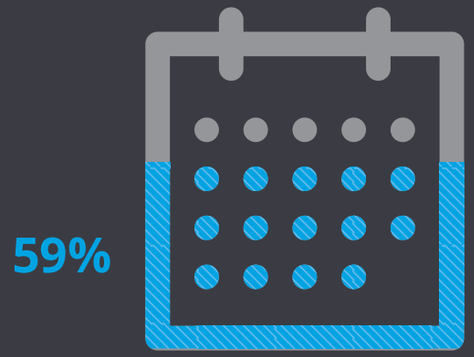
Three-tiered technology architecture comprises:
Tier one: Enterprise Resource Planning (ERP) or procurement platforms that establish a common foundation and operational discipline for EERM.

Supported by:
Tier two: Either EERM-specific risk management packages tailored to an organization's third-party management requirements, or generic governance, risk management and compliance (GRC), or controls management platforms that include EERM capability; **and**

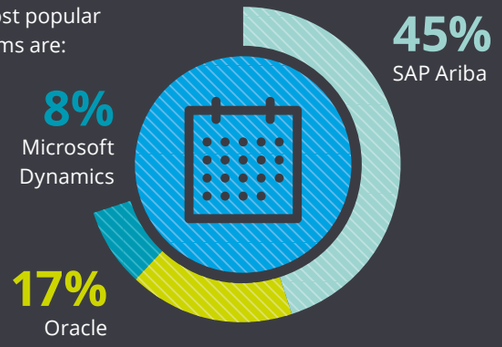
Tier three: Niche packages for specific EERM processes or risks providing feeds from specialized risk domains such as financial viability, financial crime, contract management, and cyber threats.

Tier one

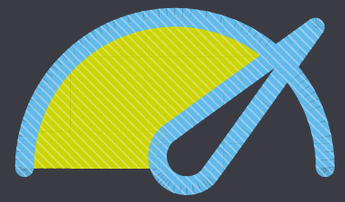
The majority of respondents (**59 percent**) adopt an ERP or procurement platform as a foundation system for EERM.



The most popular platforms are:



Tier two



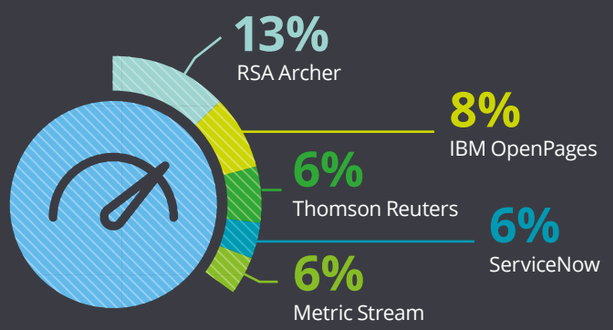
An even greater majority (**75 percent**) adopt risk management solutions for EERM.

There is debate about the choice between:

- EERM specific packages. Currently **18 percent** of organizations use these; and
- Generic integrated risk management solutions tailored for EERM use. Currently **57 percent** of organizations use these.

While integrated risk management solutions are more prevalent across respondent organizations, this does not necessarily mean they are the preferred solution. Commentary from respondents suggests that some organizations may choose to use these generic risk management platforms because they already exist in their organizations and can most easily and cost effectively be leveraged to support EERM activities.

The most common solutions are:

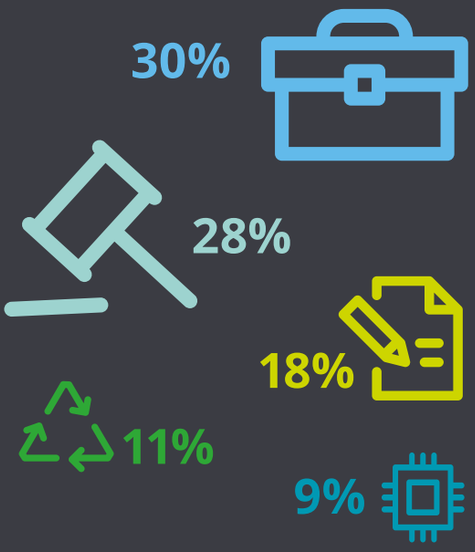


Tier three

Organizations are increasingly using niche packages for specific EERM processes or risks with feeds from specialized risk domains.

This includes:

- Financial viability **(30 percent)**,
- Financial crime **(28 percent)**,
- Contract management **(18 percent)**,
- Sustainability **(11 percent)**, and
- Cyber threats **(9 percent)**.



6 Executive summary

Subcontractor and affiliate risks

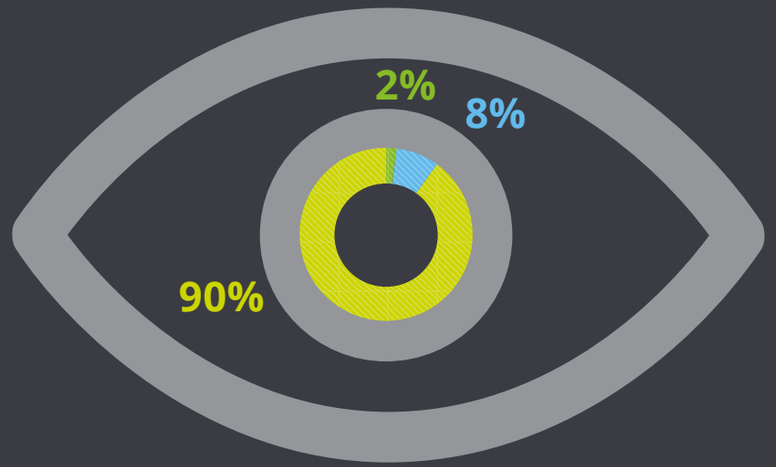
Two key aspects of third-party risk management are not being adequately addressed: i) subcontractors; and ii) affiliates.

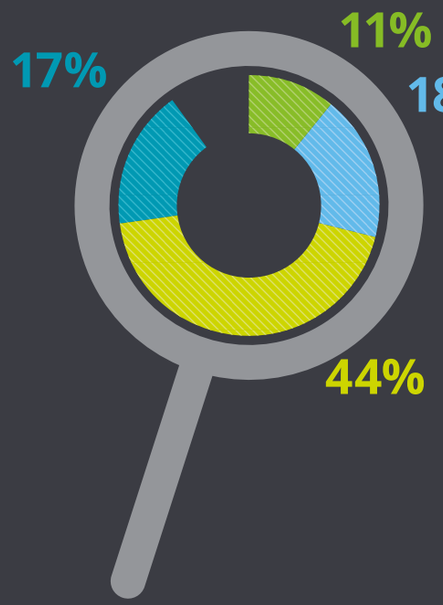
Subcontractor risk (also known as fourth/fifth party risk):

Organizations do not know enough about the subcontractors engaged by their third parties. This makes it difficult for organizations to determine how to manage subcontractor risk, and to apply this strategy with discipline and rigor.

Only **2 percent** of organizations identify and monitor all subcontractors engaged by their third parties, and only **8 percent** (down from 10 percent last year) do so for their most critical relationships.

The remaining **90 percent** do not recognize the need or have appropriate knowledge, visibility, or resources to monitor subcontractors.





11 percent assess subcontractors only when taking on a new third party (up from **8 percent** last year).

18 percent identify and assess subcontractors ad hoc.

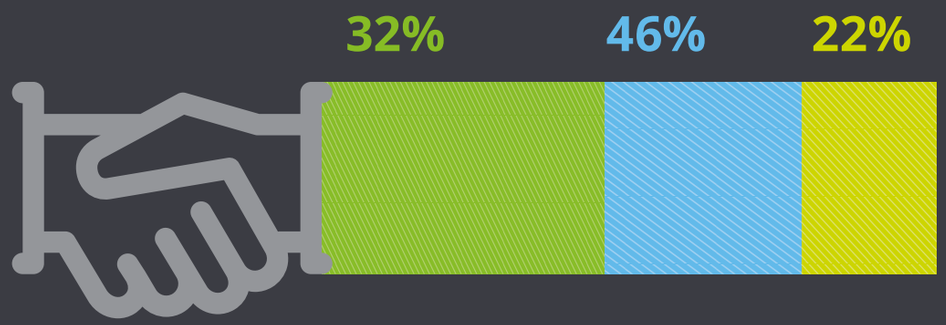
44 percent rely on third parties to check their contractors, but monitor the way third parties do this.

17 percent do not identify, assess, or monitor subcontractors at all.

This challenge is particularly relevant in regulated industries such as financial services, where systemic concentration risk is a concern for regulators. The challenge, however, is not isolated to regulated industries given broader laws and regulations such as the UK Modern Slavery Act and EU's GDPR.

Affiliate risk

Less than a third (**32 percent**) of organizations evaluate and monitor affiliate[6] risks with the same rigor as they do other third parties. A higher proportion (**46 percent**) take an alternative, typically more simplified, approach to affiliate risk management and the remaining **22 percent** said they do not have affiliates.



Pre-screening, due diligence, and monitoring appears to be much lighter touch for affiliates than other third parties. This is acceptable if proportionate to the risk involved, but the approach must be clearly defined and consistent.

Another development is the emergence of global business services (GBS) structures. These aim to integrate governance mechanisms and good practice across all third parties, as well as internal shared services delivery teams. However, the scope of these structures, as well as the entity in which they sit, varies across organizations. This creates multi-layered challenges for third-party, risk management.

Executive summary

Future predictions

Business case drivers

Cost reduction as a driver for investment in EERM is likely to be short term. We should expect other drivers that ensure profitable top-line growth to be more prominent in the medium to longer term. This includes EERM investments that can use the skills and capabilities of third parties to:

- Access new markets
- Generate new revenue streams
- Establish competitive advantage

Regulators

Regulators already have significant expectations on how organizations manage third-party risk. We expect regulators to become more powerful and broaden their area of responsibility to address emerging risks as seen by recent laws and regulations, such as the Modern Slavery Act and GDPR.

We also anticipate regulators will encourage innovation in risk management and compliance. For instance, in December 2018 the Federal Reserve, one of the bodies regulating financial services in the US, suggested innovative approaches ranging from building sophisticated financial intelligence units to embracing artificial intelligence for transaction monitoring. We expect the European Banking Authority and UK Financial Conduct Authority to adopt similar stances in the future.

Operating models

Organizations have invested in changes to EERM operating models to gain efficiencies and a more consistent approach across various risk domains proportionate to the risks involved. We predict that this will begin to pay dividends by the end of 2020 or 2021 – in line with respondents' realistic assessment that it takes two to three years for investment benefits to crystallize.

We also expect that favored models for EERM delivery will continue to change as the functionality of technology solutions develop and confidence and comprehensiveness of market utilities and managed delivery solutions evolve.

Technology

The desire to streamline technology will continue.

In response to this:

- Major ERP vendors are increasing the functionality of their tools
- Third-party risk management tools will evolve into broader third-party management tools, where performance, contracts, and commercial matters are managed in conjunction with the risk.

We also expect the evaluation criteria for technology solutions to evolve beyond "cheaper, faster, better" to include:

- Support in emerging markets
- Robotics and cognitive automation
- A consideration of what the shared utilities and managed services platforms of the future can provide.

Expenditure

We anticipate that 2019 and 2020 will see more EERM capital expenditure on transformation initiatives and related design and implementation work to make the shift to platforms that improve the maturity of EERM in the long term.

After this necessary upfront investment, organizations doing this well should be able to achieve their aspiration of limiting ongoing capital expenditure to, at most, the same levels as annual EERM operating expenditure.

Smaller and nimbler organizations, however, may be more able and willing to move toward shared utilities models and adopt emerging technology, therefore demonstrating the inverse trend – higher levels of operating expenditure and only incremental capital expenditure.

Subcontractor risk

Risk management of fourth and fifth parties will gain increasing prominence and investment as organizations better understand the inherent risks and its significance as a potential source of reputation risk.

01

Economic and operating environment

Economic uncertainty continues to drive cost reduction and talent investment in EERM.

The story so far

Over the past four years, our annual EERM surveys have tracked the key drivers for engaging third parties and investments in third-party risk management. Our surveys repeatedly show that organizations increasingly use third parties to meet wider strategic objectives rather than just reduce costs. These include:

- Organizational agility, including flexibility and scalability.
- Product or service innovation, often by using the specialist knowledge and skills of third parties.

In 2015, investment in EERM almost exclusively focused on managing the downside risks, such as regulatory exposure or third-party incidents. There was less focus on exploiting upside risks that improve organizational performance through initiatives such as:

- Reducing costs by means of efficiencies in third-party management.
- Unlocking new revenue streams through better monitoring of third parties.

By 2018, our survey respondents – including board members and executive leadership – had developed a much stronger understanding of the risks and opportunities that third-party risk management offered. This meant they were more confident that their investments in EERM would show tangible benefits.

Recent economic global uncertainty, however, meant they have been less able to make significant capital investments in transformation initiatives to bring about a holistic and integrated approach to third-party risk management.

Economic uncertainty continues to drive cost reduction and talent investment in EERM.

2019 findings

Organizations are operating in an increasingly complex and challenging economic and business environment with tougher regulatory regimes and disruptive market shifts.

We also identified a concern among many respondents that the governments of some countries were encouraging insular and non-cooperative behavior that could negatively impact global businesses.

Our current survey reveals this complex and challenging environment is having a significant impact on investments in EERM: Organizations are revisiting their operating models to pursue efficiency and reduce costs.

Investment drivers

This year's most common drivers for investing in EERM are:

- **Cost reduction**
  (62 percent of respondents, up from 48 percent last year)
- **Reducing third-party incidents**
  (50 percent, up from 34 percent last year)
- **Regulatory scrutiny**
  (49 percent, up from 43 percent last year)
- **Internal compliance requirements**
  (45 percent, up from 41 percent last year).

Third-party incidents

Third-party incidents continue to cause disruption with varying impact. The majority (83 percent) of organizations experienced a third-party incident in the past three years. Of these, just 11 percent experienced a severe impact on customer service, financial position, reputation or regulatory compliance, but over a third (35 percent) experienced a moderate organizational impact.

Identified areas for EERM improvement

Despite a focus on cost reduction, just over half (53 percent) of respondents want a more coordinated and consistent approach to EERM across organizational functions. This is the top area for action.

The need to improve processes, technologies, and real-time management information for EERM (49 percent) is second.

The availability of managed services and utility models has reduced concerns about acquiring the more basic EERM skills, and about the overall capacity to deliver. Organizations instead want to invest in EERM leadership talent to coordinate and to lead initiatives.

Fig 1.1 Investment drivers for EERM

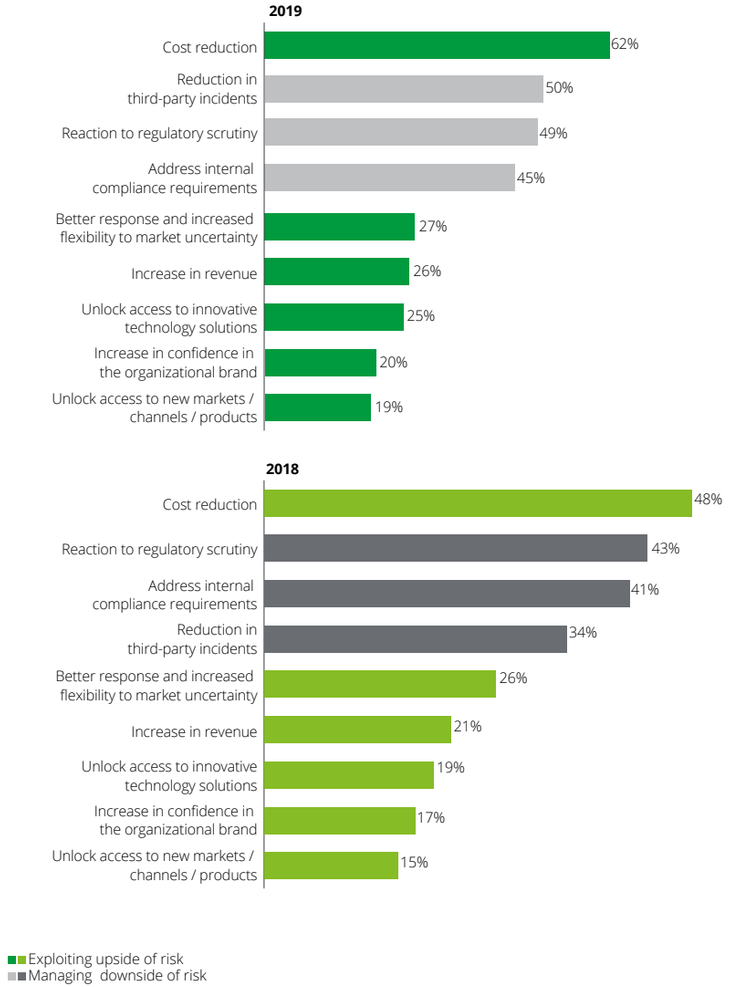


Fig 1.2 Impact of third-party incidents experienced in the last three years

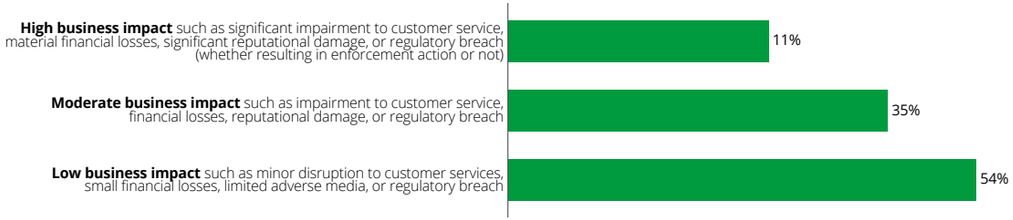
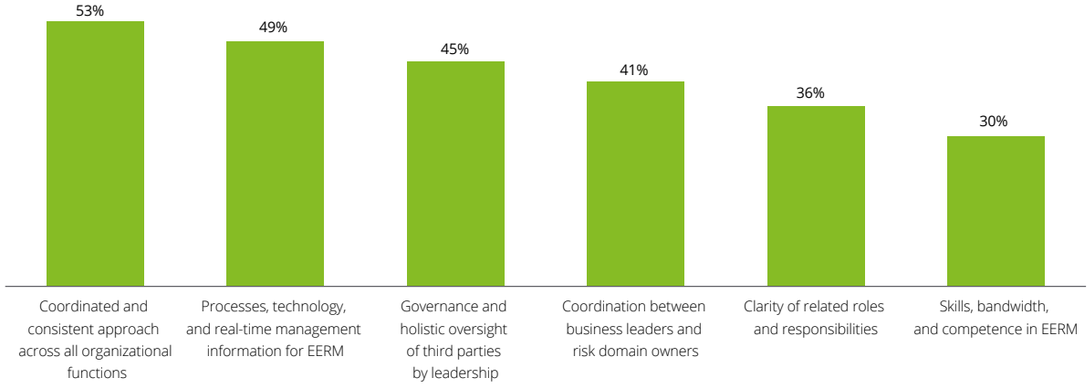


Fig 1.3 Areas where improvement is required to increase organizational confidence in EERM



Deloitte point of view

Organizations have been focusing on reducing costs through better third-party management for several years. We are starting to see more and more organizations taking a two-pronged approach to this:

- By establishing programs to recover overpayments or revenue leakages.
- Through investment in a strategic EERM solution and achieving efficiencies through mechanisms such as shared services.

The shortage of EERM leadership talent is an old problem too. But this concern has been further highlighted by the recognition that initiatives to create efficiencies and improve internal coordination can only be successful if led by people with leadership skills and EERM experience. We believe the consequences of negative actions by third parties will continue to grow more severe – damaging organizational reputation, earnings, and shareholder value. This will remain a compelling driver for organizations to invest in improving third-party risk management processes and frameworks.

At the same time, regulatory enforcement, mirrored by internal scrutiny and compliance requirements, will continually be a more proactive and continuous process.

More robust third-party management will be driven by radically more severe actions by regulators in a range of sectors – financial services, life sciences and Health Care, chemicals, food and retail – and legislation and regulations with a global reach and impact, such as the US Foreign Corrupt Practices Act.

Industry highlights

Cost reduction, reduction in third-party incidents followed by regulatory scrutiny and internal compliance requirements, present the most powerful motives for investment in EERM across most industries. But, there are exceptions to this, and particular priorities in different sectors.

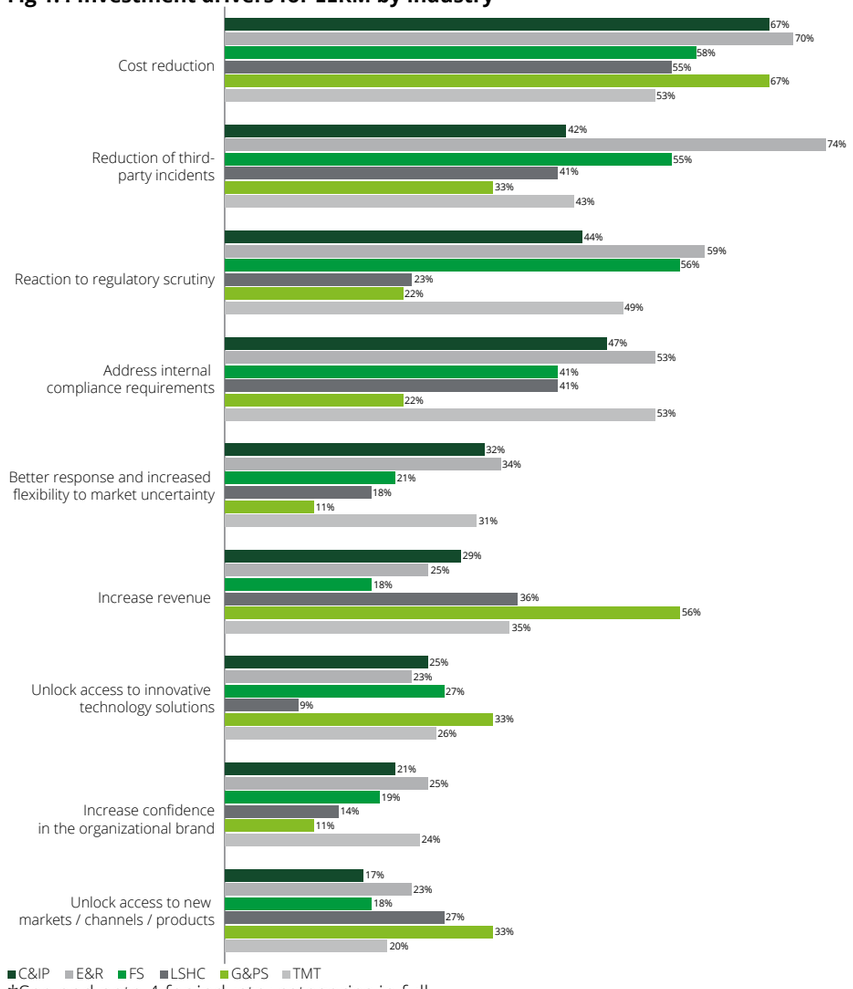
- Addressing internal compliance requirements is a higher concern (47 percent) compared to regulatory scrutiny (at 44 percent) in consumer & industrial products.
- Reducing the number of third-party incidents is the most common driver for investment in EERM in energy & resources (74 percent of respondents). This was far above the next highest industry, financial services, at 55 percent.
- A third (33 percent) of organizations in government & public services want to invest in EERM to unlock access to innovative technology solutions. The majority of organizations citing this within the sector were higher education institutions, probably because of their desire for technological innovation to enable initiatives such as distance learning. Finding tech solutions was also common in financial services (27 percent) and technology, media & telecoms (26 percent).
- Government & public services organizations were also by far the most likely to recognize the need for a greater coordination and consistency of approach across organizational functions, at 90 percent.

Organizations in life sciences & health care more commonly suffered high (19 percent) and moderate (46 percent) business impact from third-party incidents. Consumer & industrial products businesses are next: 17 percent of respondents saw third-party incidents with a high business impact, and a further 31 percent experienced a moderate impact. Followed by financial services at 10 percent high and 36 percent moderate.

In all sectors, a large number of organizations recognized the need for improvement in processes, technology, and real-time management information for EERM.

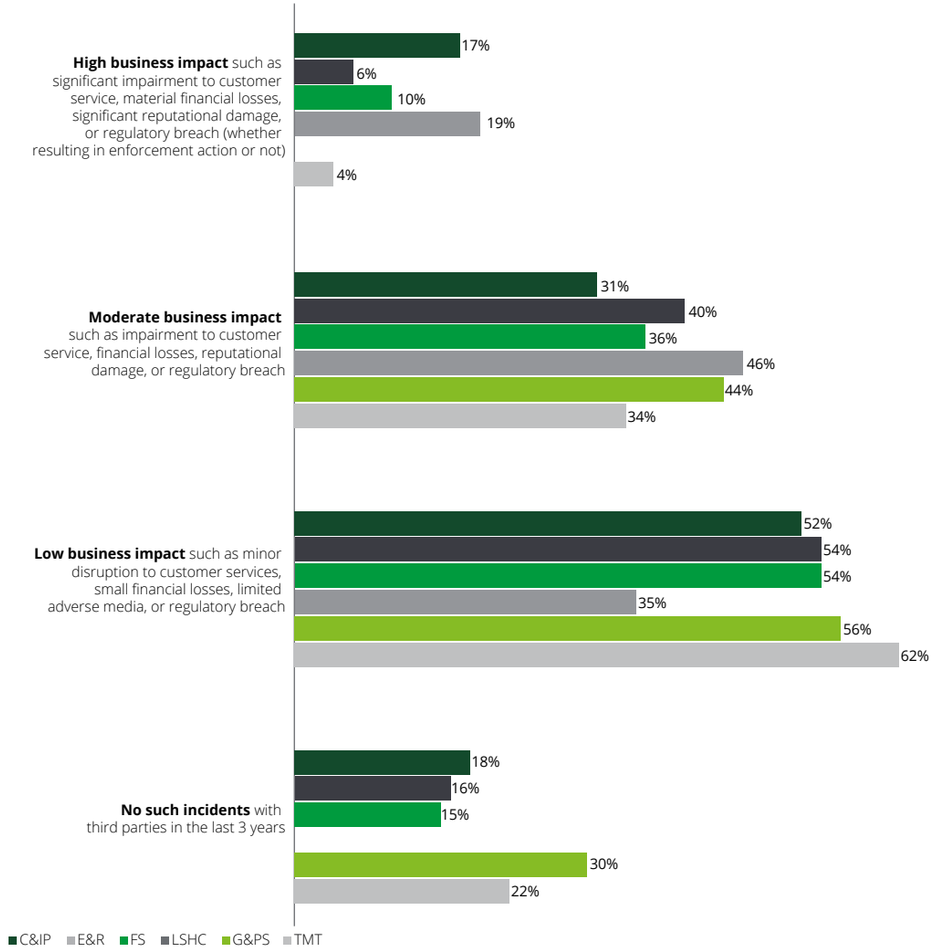
Life sciences & health care (60 percent), and government & public services (50 percent), particularly believe in the need for better engagement between business unit leaders and risk domain owners.

Fig 1.4 Investment drivers for EERM by industry



*See end note 4 for industry categories in full

Fig 1.5 Impact of third party incidents experienced in the last three years by industry



Geography highlights

Investments in EERM were most likely to be driven by cost reduction and value preservation strategies in EMEA, followed by the Americas and Asia Pacific:

- **Cost reduction:** EMEA 63 percent, Americas 60 percent, Asia Pacific 57 percent
- **Reduction in third-party incidents:** EMEA 54 percent, Americas 46 percent, Asia Pacific 40 percent
- **Reaction to regulatory scrutiny**: EMEA 52 percent, Americas 50 percent, Asia Pacific 38 percent
- **Addressing internal compliance requirements:** EMEA 47 percent, Americas 46 percent, Asia Pacific 38 percent.

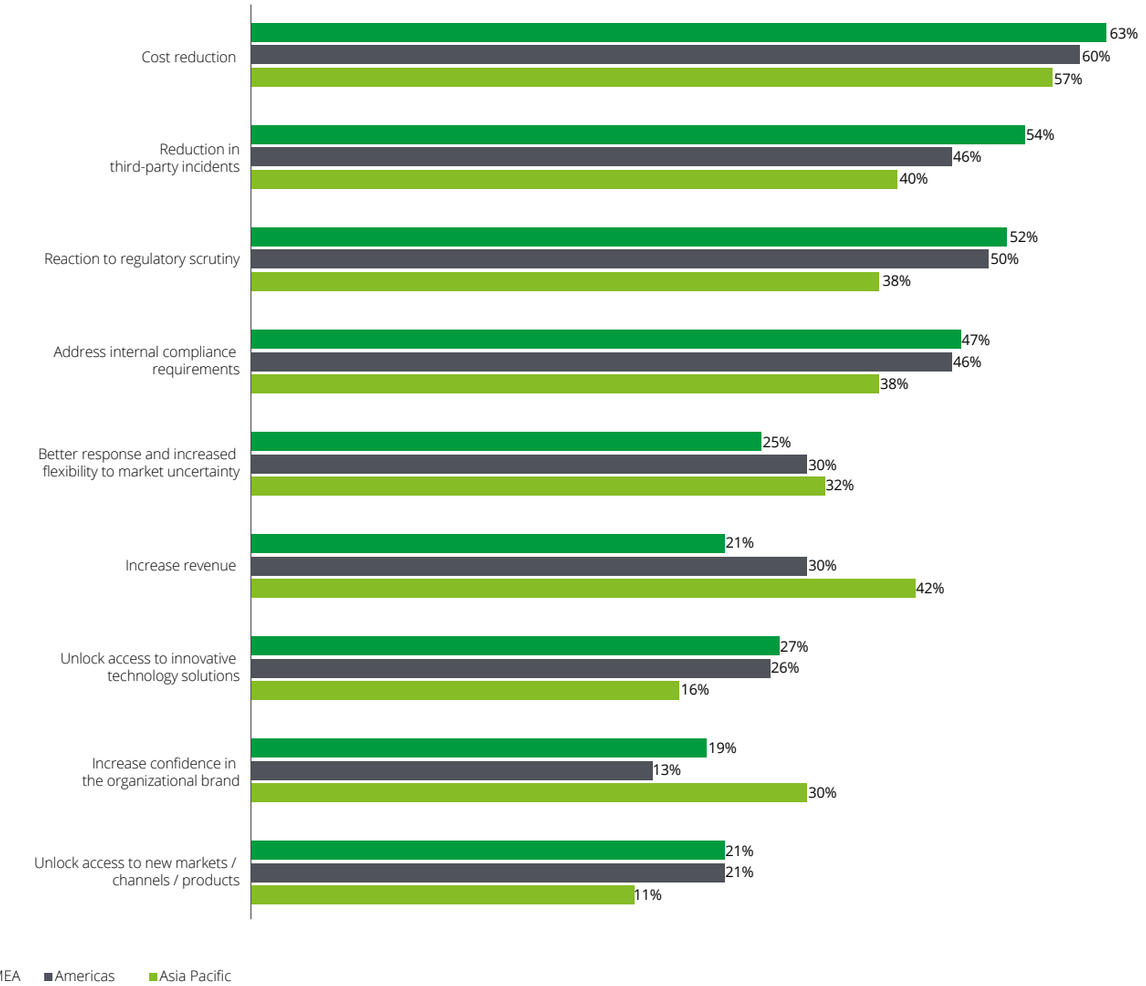
These statistics probably reflect the relative levels of uncertainty in these regional business environments. The top-ranked drivers also potentially reflect a history of greater regulatory enforcement activity in EMEA and Americas, compared to Asia Pacific countries.

Value creation drivers, other than cost reduction, were marginally stronger in Asia Pacific territories. For instance:

- Increase revenue (for example by identifying under-reported revenue streams): 42 percent in Asia Pacific, but only 30 percent in the Americas and 21 percent in EMEA.
- Better response and increased flexibility to market uncertainty: 32 percent of respondents in Asia Pacific as against 30 percent in the Americas and 25 percent in EMEA.

All regions had a similar occurrence of third-party incidents, although Asia Pacific had a marginally higher proportion of incidents with high business impact – 14 percent, as against 11 percent in EMEA and 9 percent in the Americas.

Fig 1.6 Investment drivers by region



02

Investment

Piecemeal investment has impaired EERM maturity, neglected certain risks, and adversely affected core basic tasks.

The story so far

Developments in EERM maturity have not kept pace with increasingly critical levels of dependence on third parties since our first survey in 2015. Only one in five organizations had integrated or optimized their approach between 2015 and 2018.

Organizations have reset their expectations about a realistic time frame to integrate and optimize the related risk management mechanisms to reach the desired state. They have gradually realized it is at least a two- or three-year journey, rather than a six-month or one-year project, as first thought.

In reality, the optimum state of EERM remains a moving target. Many organizations are still playing catch-up with rising expectations of how innovative third-party and related services could be. Concepts of good practice, technology solutions, utilities, and managed services are becoming more sophisticated. Consequently, respondents are re-evaluating their earlier self-assessments of maturity.

Some respondents over the years have reported a somewhat sporadic approach to EERM in their organizations, focusing annual investment mainly on the largest regulatory issues of the year. In 2018, for example, that was data privacy. Organizations need to be careful not to neglect wider risks and keep pace with advancements in capability.

Piecemeal investment has impaired EERM maturity, neglected certain risks, and adversely affected core basic tasks.

2019 findings

There has been strong evidence over the years that such a piecemeal approach to investing in EERM has impaired the speed at which organizations have been able to mature. In the latest survey, only 21 percent of respondents consider themselves "integrated" or "optimized" – only up from 20 percent last year. Just over half (51 percent, and only up from 50 percent last year) consider themselves in the "managed" category.

This year, we asked respondents about their investment in EERM. More than 70 percent believe they are spending less than the ideal amount, or are not sure whether they are. And seven in ten believe they engage fewer employees than necessary for EERM, or are not sure.

Although underinvestment is a common perception across most organizations, annual operating expenditure on EERM varies significantly. Half (50 percent) spend more than US$1 million on their annual EERM operating costs, but the top 11 percent spend more than US$10 million each and employ over 100 full-time equivalent (FTE) staff.

This year's survey also captured detail on investment in specific risk domains.

Investment is skewed toward information security (68 percent of respondents), data privacy (62 percent) and cyber risk (58 percent).

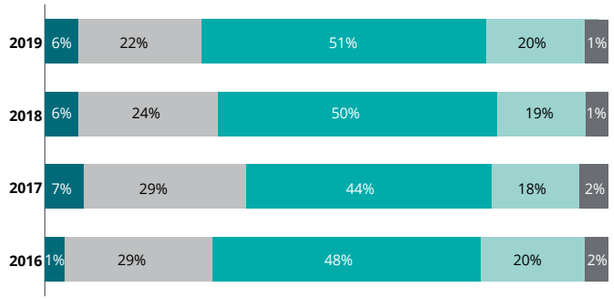
And many organizations underinvest in other domains such as labor rights (18 percent) and geopolitical and concentration risk (both at 12 percent).

In most organizations, investment in two areas is underemphasized:

- **Exit planning and termination activities** related to critical third parties. Exit plans for critical third parties are assessed less than annually for more than 60 percent of the respondents.
- **Managing concentration risk**. Concentration risks are assessed less than annually for almost half of the respondents. Concentration risk tends to be reviewed reactively via reporting as opposed to proactively as part of the EERM process.

A new insight is respondents realize this piecemeal approach has weakened organizational abilities to do basic core tasks well. The most common factors making it hard to tailor the monitoring effort to the level of risk involved are understanding the nature of third-party relationships (50 percent) and understanding related contractual terms (43 percent).

Fig 2.1 Change in level of maturity in EERM (2016–19)



1. **Initial:** None or very few of above elements addressed
2. **Defined:** Some of the above elements addressed with limited effort with regard to the above elements
3. **Managed:** Consideration given to addressing all the above elements with room for improvement
4. **Integrated:** Most of the above elements addressed and evolved
5. **Optimized:** Best in class organization – all of the above elements addressed and evolved

Fig 2.2 Most organizations believe that they are under-investing in EERM

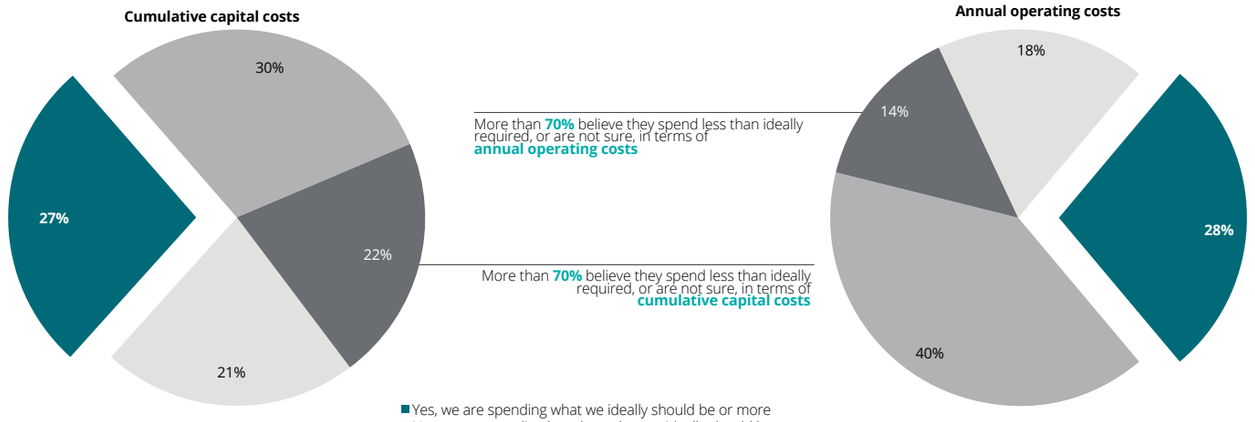
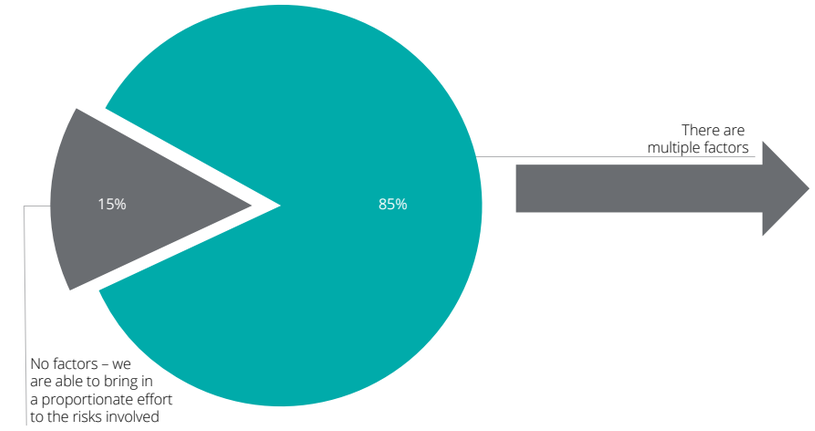


Fig 2.3 Top factors challenging third-party risks to be addressed with proportionate effort



Deloitte point of view

Our earlier EERM surveys highlighted that third-party risk has historically been siloed by risk domains and determined by multiple stakeholders driving specific activities. Examples are disruption risks from a supply chain perspective and information security risks related to IT services provided by third parties.

By 2016, more progressive organizations had begun to adopt a more holistic approach, covering all types of third-party and all areas of risk. Although these organizations made good progress in covering a broader range of third parties under a more holistic set of risk domains, the lack of adequate budgets has once again focused attention on investing heavily in specific risk domains that have been the subject of legislation. Examples in 2018 are:

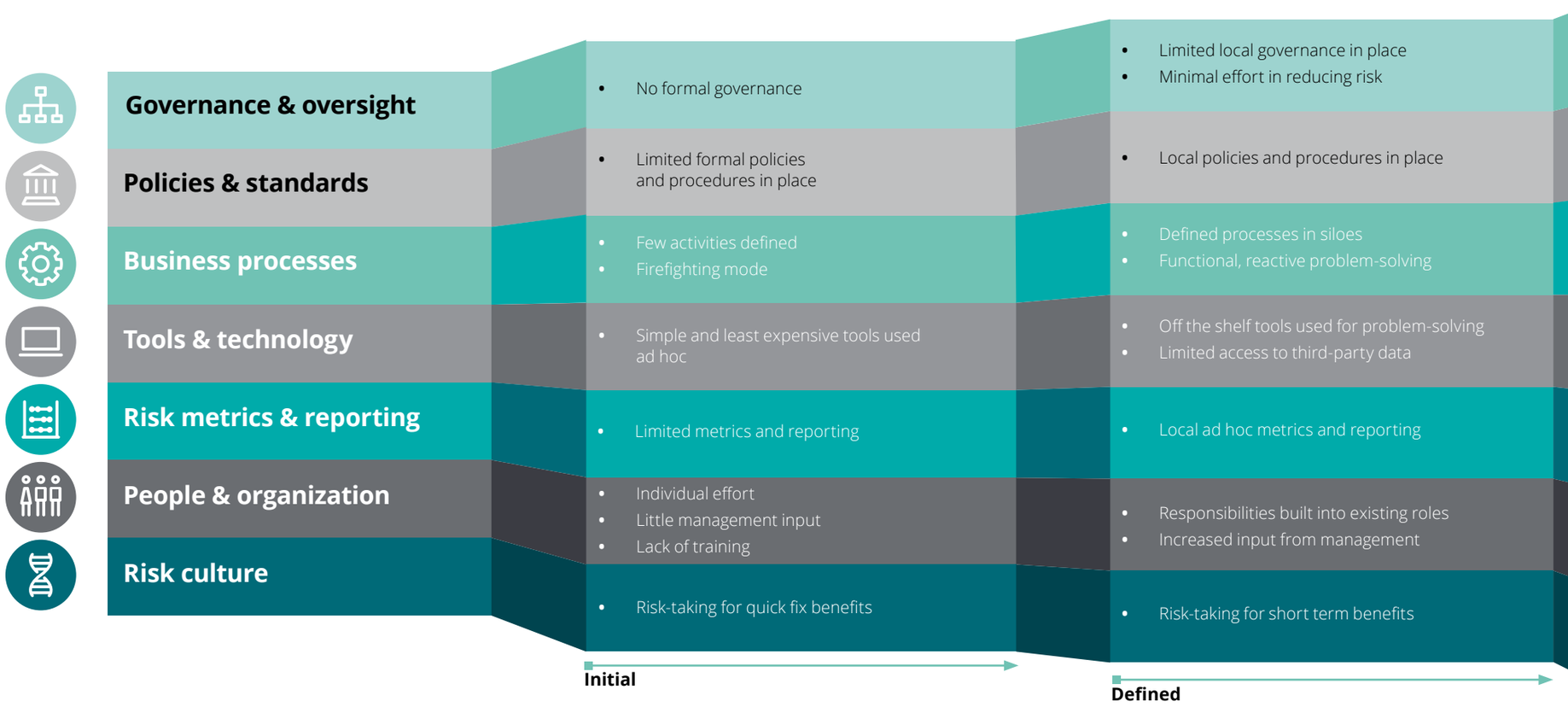
- Privacy concerns driven by the Global Data Protection Regulation (GDPR) in Europe and similar legislation elsewhere
- Cybersecurity fears following disruptive cyberattacks across the globe.

These limited piecemeal investments in EERM have impaired growth in organizational maturity and made it harder to take a strategic approach to investment. Critically, not being "brilliant at the basics" potentially undermines an organization's efforts to realize the benefits from more cutting-edge initiatives. As a result, the benefits realized are a small fraction of the potential.

Organizations should reinvigorate their focus on bringing third-party risk management together by streamlining processes and frameworks, while regularly exploring opportunities that make them more integrated, efficient, and effective.

Organizations should also consider allocating a higher proportion of annual EERM operating expenditure (opex) to pre-screening and exit planning and termination activities – perhaps about 10 percent to each of these. This would supplement the focus on selection – due diligence and contracting at 20 to 30 percent of the budget, and ongoing monitoring at 50 percent or a little above. This mix of spending would help organizations evolve their approach from detective to more preventive mechanisms.

Deloitte EERM Maturity Model



Industry highlights

The survey revealed similar EERM maturity levels across industries, with the exception of life science & health care and government & public services. Life science & health care organizations are more optimistic about their maturity compared to others: 28 percent rate their EERM as "integrated" or "optimized". Government & public service organizations are less positive than other organizations – only 10 percent deem themselves "integrated" or "optimized".

The perception of underinvestment in both capital expenditure (capex) and operating costs (opex) in EERM is common across sectors. Financial services, however, have the largest proportion of respondents who regard their organizational investments as adequate in capex (31 percent) and opex (34 percent). Government & public services organizations are at the other end of the scale, only 11 percent view their EERM investments as adequate (the same for capex and opex).

Certain risk domains – information security, data privacy, cyber risk and non-regulatory compliance – receive investment priority compared to others across all sectors. However, certain industries tend to focus on some risk domains neglecting others.

For example:

- Government & public services (78 percent respondents), energy & resources (68 percent), and financial services organizations (58 percent) focused particularly on fighting financial crime, including money laundering, bribery, and sanctions.
- Government & public services surpasses other sectors in its ongoing commitment to managing reputational risk (56 percent) and physical security (67 percent).
- Financial services, and energy & resources, place particular importance on managing resilience and business continuity, at 46 percent in both cases.
- Energy & resources puts a strong priority on addressing contract risk (59 percent of respondents), health and safety risk (66 percent), and subcontractor risk (55 percent).
- Financial services are reacting to the increasing concern from regulators, 23 percent focused on concentration risk.
- The technology, media & telecoms industry has the greatest interest in intellectual property risk (36 percent) – far more than other sectors.

Fig 2.4 Organizational self-assessment of EERM maturity by industry segment

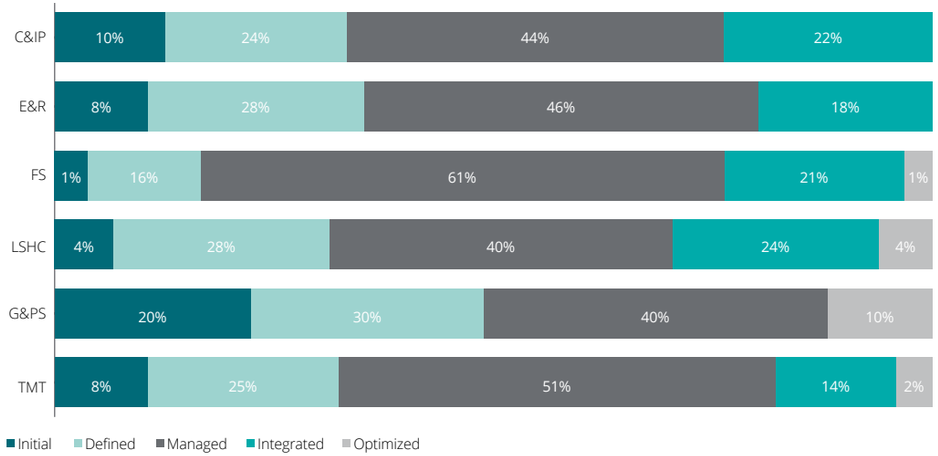
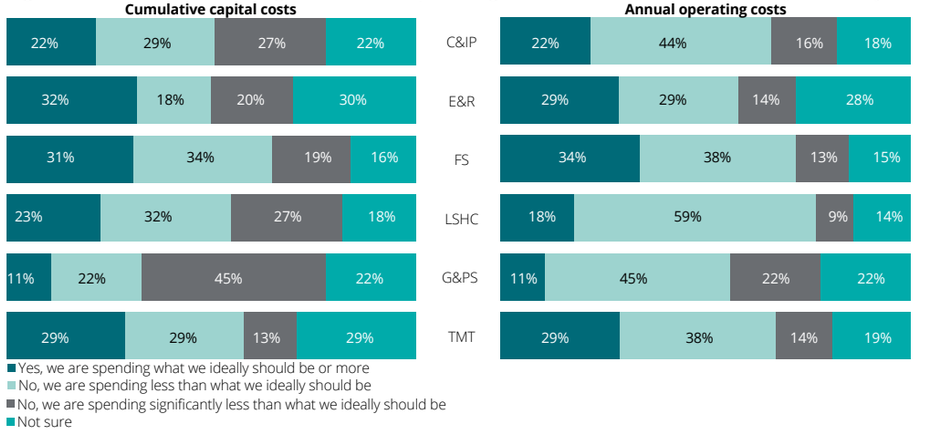
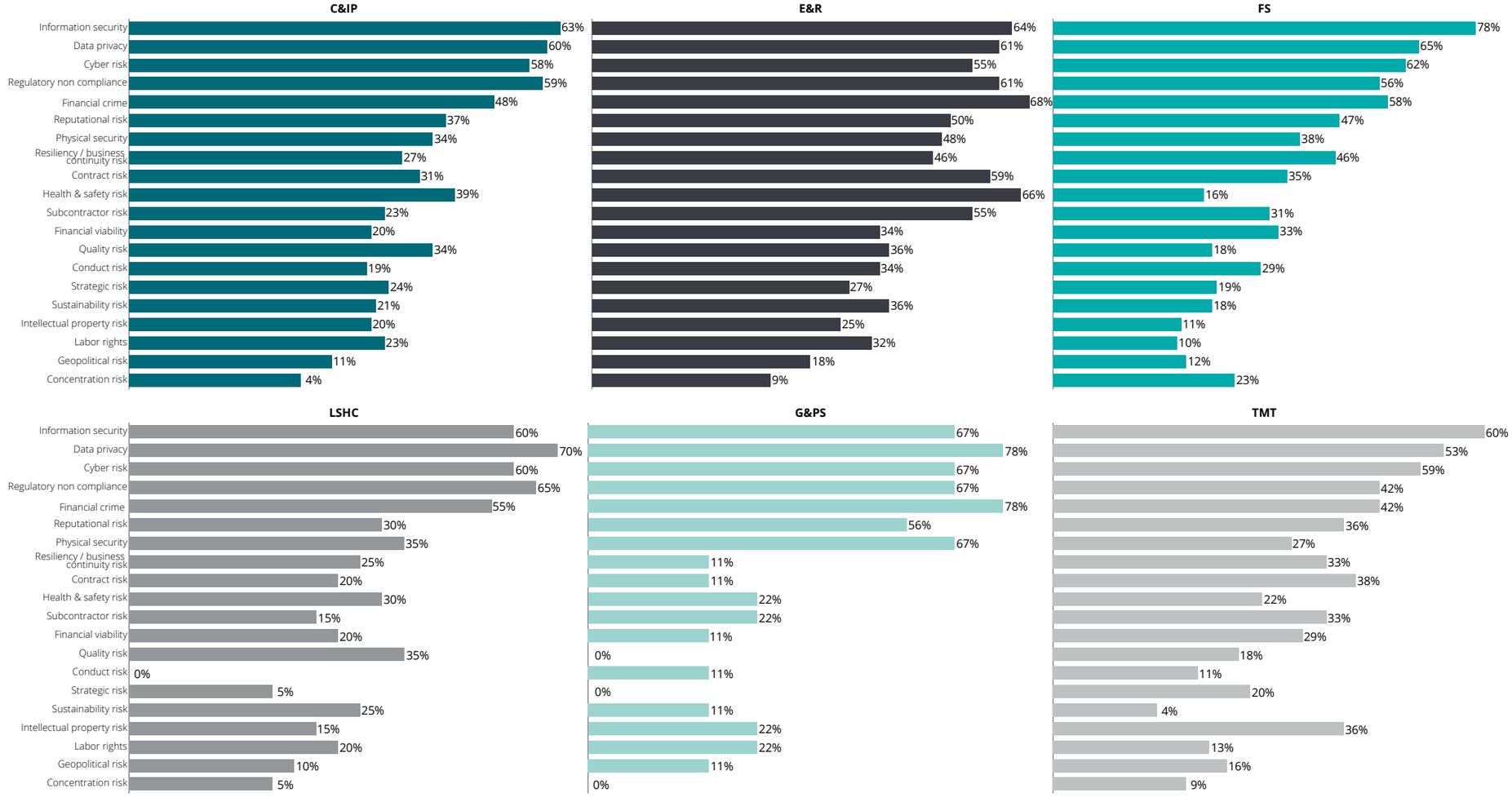


Fig 2.5 Belief in whether organization is spending what it should be in EERM by industry



*See end note 4 for industry categories in full

Fig 2.6 Investment in specific risk domains of EERM by industry



Geography highlights

There are no extreme geographical variations between the number of third parties engaged by organizations.

The number of FTEs broadly align to the level of annual investment across all regions, although this may change with greater adoption of managed services.

Organizations in the Americas are most likely to spend above US$1 million on EERM related activities, followed by EMEA and Asia Pacific:

- 65 percent of respondents from the Americas spend above US$1 million, including 25 percent who spend more than US$5 million annually on opex.
- 48 percent of respondents from EMEA spend over US$1 million, including 17 percent spending over US$5 million.
- In Asia Pacific only 38 percent spend above US$1 million, and only 10 percent above US$5 million.

Respondents from Asia Pacific were the least likely to believe they are spending what they should be or more on EERM capex (19 percent) and opex (23 percent). The vast majority believe their organizations are underinvesting. This is only slightly better in the Americas (21 percent for capex and 23 percent for opex) and EMEA (30 percent for both capex and opex).

Across the world, the risk domains given priority were broadly the same: data privacy, information security, and cybersecurity.

One interesting difference, however, was the proportion of EERM budget spent at each stage of the third-party relationship life cycle. Ongoing monitoring is typically the longest phase in this life cycle and typically accounts for the highest proportion of spending.

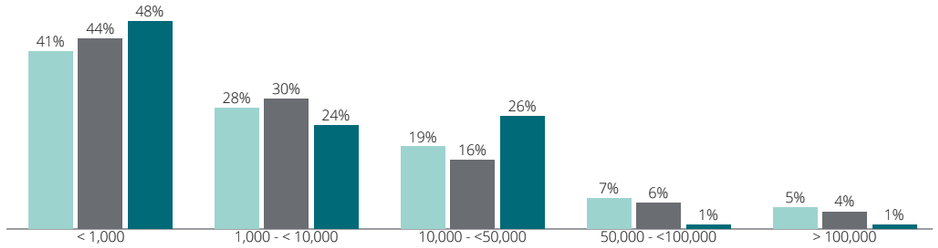
Respondents from Asia Pacific reported the lowest proportional spend of their budget on pre-screening, due diligence, and termination. For instance, as many as 60 percent of Asia Pacific respondents spent less than 5 percent of their annual budget on pre-screening activities, compared to 41 percent in the Americas and 37 percent in EMEA. More mature organizations typically spend around 10 percent.

The story is similar for termination activities and exit planning, although underinvestment here is a more uniform across regions. Nearly two-thirds (64 percent) of respondents in Asia Pacific spend less than 5 percent of their annual operating budget on this, with slightly smaller proportions for the Americas (59 percent) and EMEA (55 percent).

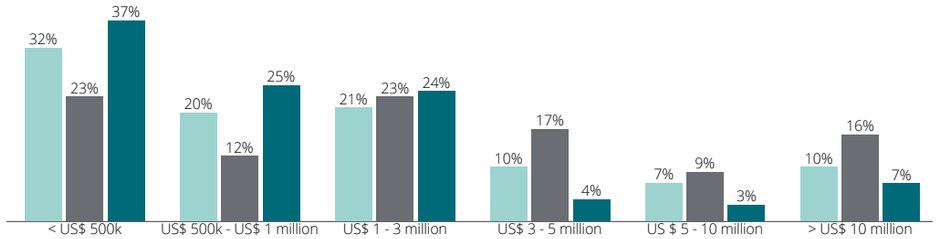
In contrast, organizations further up the maturity curve spend at least 10 percent of their budget on termination and exit planning. Respondents also indicated that spending on this is particularly high for critical third-party contracts, where termination or exit would require significant effort.

Fig 2.7 Financial and talent investment in EERM by region

Number of third parties engaged by your organization:



Level of investment in EERM that your organization should ideally be making in terms of annual operating costs



Number of Full-time equivalent staff (FTEs) that should be ideally involved in EERM in your organization

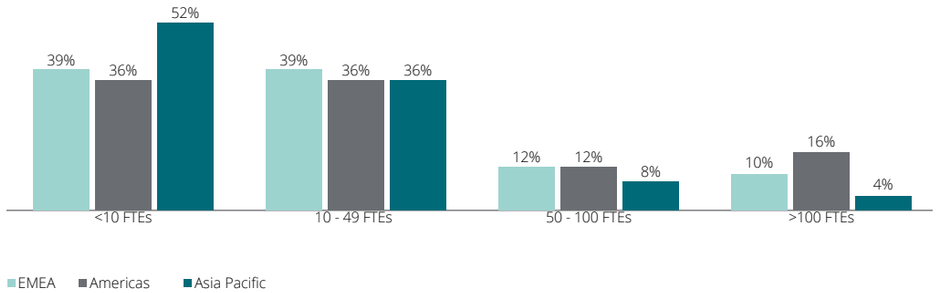


Fig 2.8 Whether respondent organizations believe they spend what they should in EERM by region

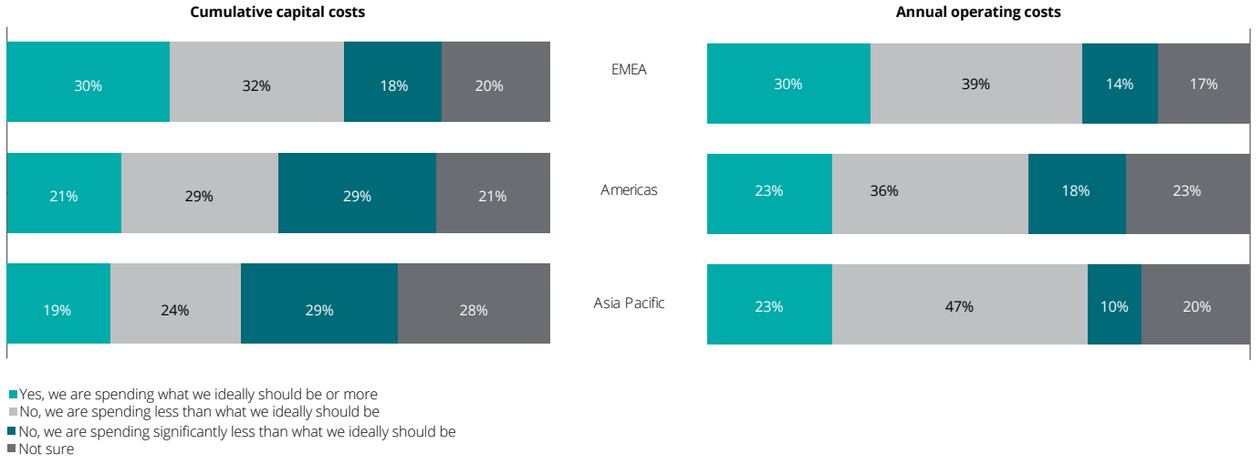
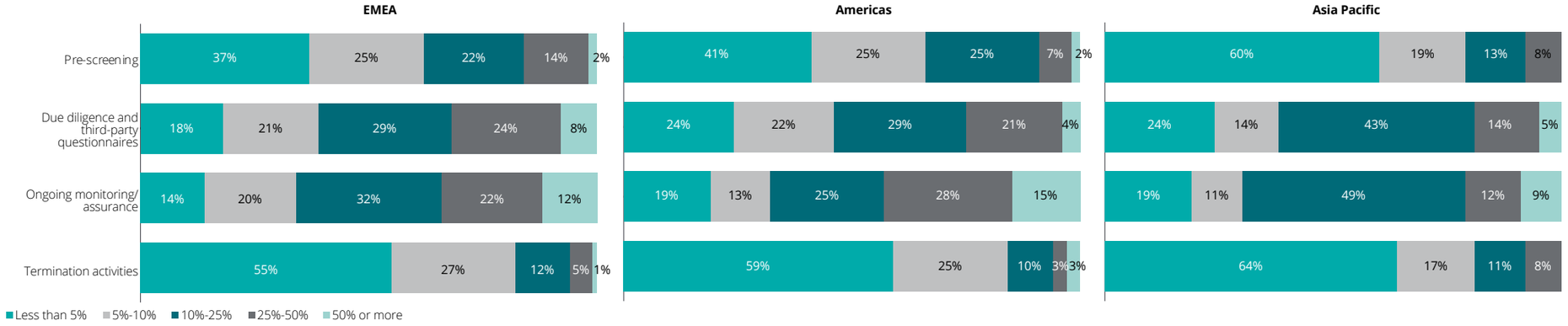
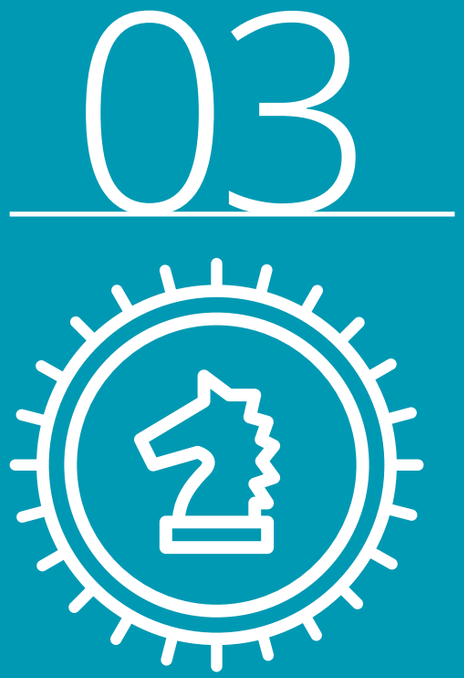


Fig 2.9 Split of annual EERM operating expenditure across each stage of the third-party life cycle by region





Leadership

Leadership wants better engagement, better coordination, and smarter use of data.

The story so far

Since 2016, our annual EERM surveys have captured how boards and executive leadership (C-suite) have enhanced their understanding of third-party risks, enabling them to strike a better balance between their responsibilities for risk oversight, growth, performance, and strategy.

This is an important change: Third-party risk management was viewed as an operational rather than a board or top leadership issue for decades. Even a few years ago, this rethinking around the position of EERM started to present a transformational opportunity for the more progressive organizations.

Between 2016 and 2018, we saw significant growth in the number of organizations moving ultimate accountability for EERM to the board and C-suite. Third-party risk now consistently features on the board agenda – with varying levels of urgency – in progressive organizations and in those from highly regulated sectors.

Nonetheless, our 2018 survey revealed room for improvement in the level of engagement on EERM between board members and risk domain owners. Survey respondents believed that lower levels of engagement and understanding by risk domain owners harmed coordination. Better coordination between leaders and teams for risk domains, business units, and functions such as procurement, legal, and internal audit, is a top EERM priority for organizations.

Leadership wants better engagement, better coordination, and smarter use of data.

2019 findings

This year's survey shows that boards and senior leadership continue to retain ultimate responsibility for EERM in more than three quarters of respondent organizations. Specifically responsibility rests with the:

- **Head of risk** in 24 percent of cases;
- **CEO** in 17 percent;
- **Board** in 19 percent;.
- **CPO** in 10 percent; and the
- **CFO** in 8 percent.

Boards and senior leadership want to fulfill their roles more responsively and be more engaged with issues specific to particular risk domains and the internal specialists dealing with them. This "inside-out" approach supplements their historical "outside-in" perspective.

Over a third (37 percent) of survey respondents believe better in-house coordination between leaders and teams for risk domains, business units, and functions such as procurement, legal, and internal audit, is a top EERM priority for organizations.

Only 16 percent, however, believe in-house coordination is strong in their organizations, with another 49 percent judging it moderate. The remaining 35 percent consider it low, nearly absent, or don't know.

This inside-out thinking is also reflected in organizational initiatives to exploit data on third parties more smartly. Boards and senior leaders want to move away from periodic color-coded ("RAG") dashboards to succinct real-time actionable intelligence with alerts and analysis of trends.

- 56 percent of respondents are using or planning to use **cloud-based platforms** for EERM
- 45 percent are focused on **robotic process automation (RPA)**
- 36 percent are using or planning to use **visualization techniques** to make this intelligence much more actionable.

Fig 3.1 Boards and executive leadership continue to retain ultimate responsibility for EERM

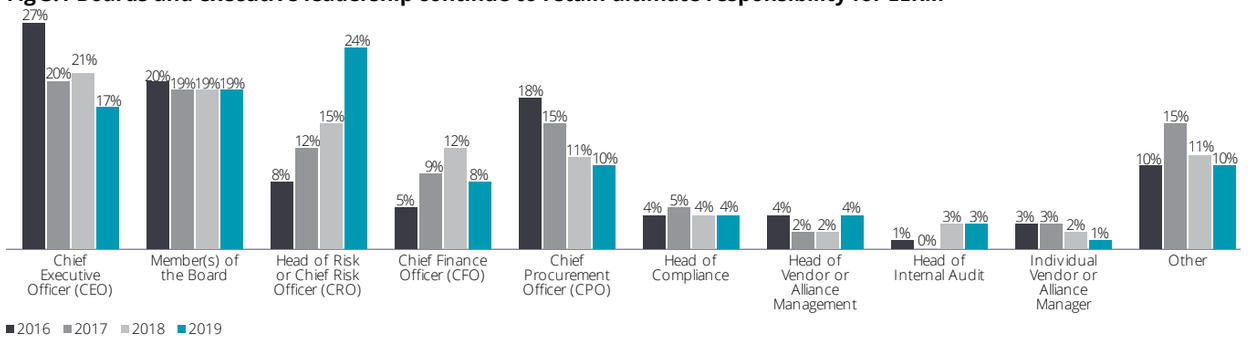


Fig 3.2 Level of engagement and coordination between key EERM stakeholders such as risk domain owners, procurement, legal, and business leaders

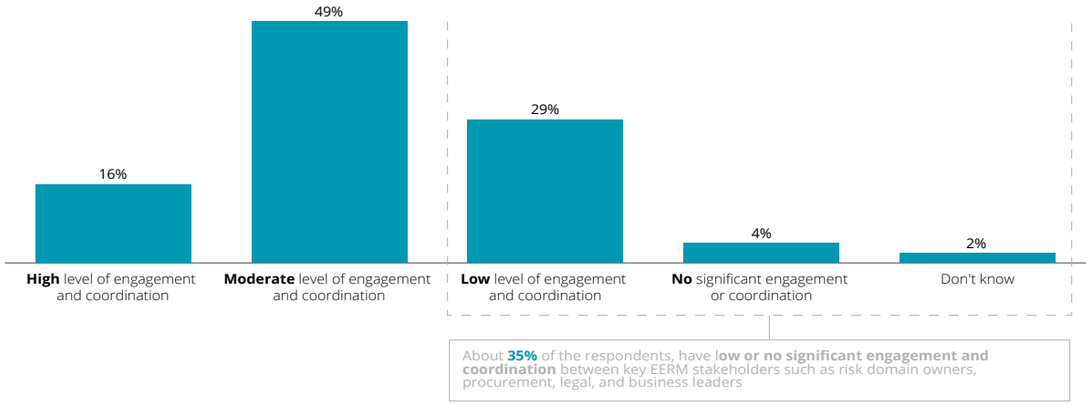
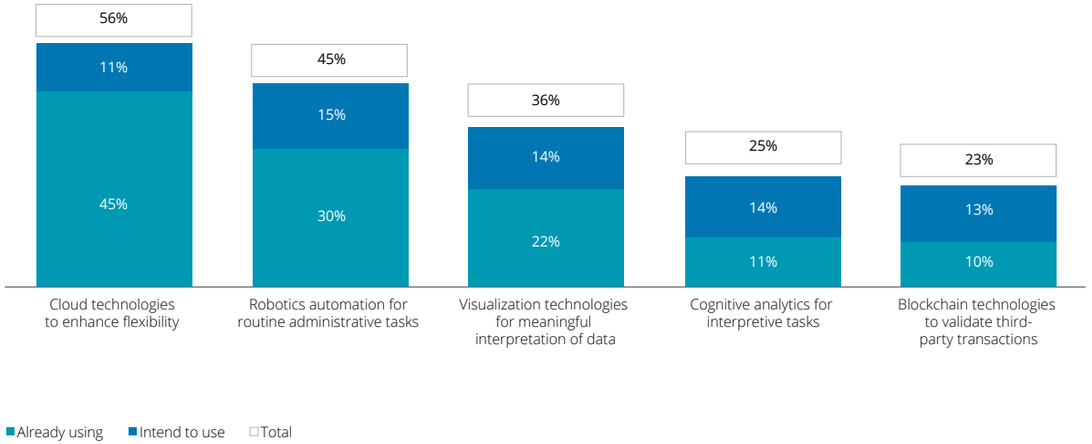


Fig 3.3 Emerging technologies being explored for EERM



Deloitte point of view

Board and C-suite ownership and oversight of EERM has been critical in enabling organizations to start realizing the opportunities and managing the risks from third parties efficiently and effectively.

Teams responsible for managing third-party risks should take advantage of this senior-level interest by challenging budgetary constraints and pushing for investment to address challenges.

Senior ownership can also facilitate cooperation across the organization and resolve conflicting priorities to drive coordinated strategic investments. This could help replace the piecemeal investment approach discussed in section two.

2018 has seen boards desire greater innovation in EERM. This includes the emergence of boardroom reporting and dashboards to make information on third parties digestible and meaningful. The timely implementation and seamless integration of vigilance mechanisms on third parties would enable teams to more efficiently identify imminent risks and performance issues. This could prevent threats from becoming reality.

A more coordinated approach within the organization can also bring together the different perspectives and skill sets that those involved in EERM bring to the business. This would ensure that risk management resources are deployed effectively to address the most significant areas of concern and opportunity.

Industry highlights

Across all industries, ultimate responsibility for EERM tends to lie with the board and C-suite. There are, though, some interesting differences. CROs most commonly have ultimate responsibility in industries most mature in EERM – consumer & industrial products, financial services, and life sciences & health care organizations.

In energy & resources and telecoms, media & technology, it most commonly sits with the board, and in government & public services with the CEO or CFO. Chief procurement officers (CPOs) are more likely to have responsibility in organizations where third-party relationships relate to the supply chain.

Energy & resources organizations were most likely to believe their organizations had good engagement and coordination. Financial services and technology, media & telecoms (16 percent of respondents for each industry) followed. At the other end of the scale, none of the respondents from government & public services felt so.

The most commonly explored emerging technology is cloud technologies, followed by RPA, in most sectors. Further interesting findings include:

- Consumer & industrial products companies are the highest adopters of **cloud technologies**. Nearly two-third (65 percent) were exploring or planning to explore such technologies. This is followed by life sciences & health care (55 percent), energy & resources (53 percent), financial services (52 percent), technology, media & telecoms (49 percent), and government & public services (44 percent).
- Consumer & industrial products companies are also the greatest adopters of **RPA**. More than half (52 percent) are exploring or planning to explore such technologies. This is followed by life sciences & health care (50 percent), technology, media & telecoms, and government & public services (44 percent each), financial services (41 percent) and energy & resources (40 percent).
- **Visualization technologies** are most popular in life sciences & health care (55 percent), followed by consumer & industrial products (39 percent), technology, media & telecoms (37 percent), energy & resources (33 percent), financial services (32 percent) and government & public services (22 percent).

Fig 3.4 Level of engagement and coordination between key EERM stakeholders and business leaders by industry

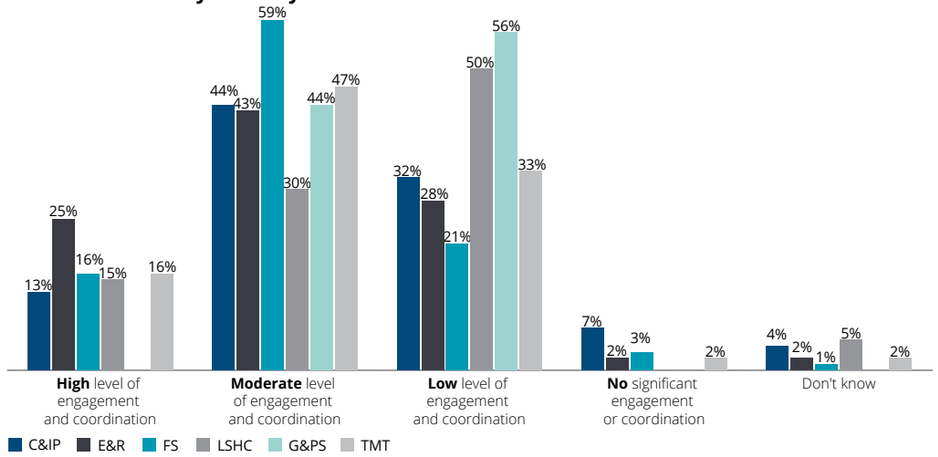


Fig 3.5 Ultimate responsibility for EERM by industry

	C&IP	E&R	FS	LSHC	G&PS	TMT
Most common	CRO	Board	CRO	CRO/Board	CEO/CFO	Board
Second most common	CEO	CPO	Board	CEO	Board/CRO	CEO
Third most common	Board	CEO	CEO	CPO	Compliance	CRO

*See end note 4 for industry categories in full

Fig 3.6 Emerging technologies being explored by industry

Geography highlights

The need for boards and executive leadership to improve engagement and coordination with risk domain owners, procurement, and legal teams is highest in the Americas, where only 11 percent of respondents rated their current level of engagement as high. The number was only marginally better in Asia Pacific (16 percent) and EMEA (17 percent).

Asia Pacific is leading the way in exploring or planning to explore technologies for EERM in the cloud (65 percent) and RPA (58 percent).

This may be because it is making capital investments in EERM relatively later, when these newer technologies have been at more advanced stages of adoption.

In contrast, Americas and EMEA counterparts are now upgrading their earlier investments in EERM to take advantage of the additional functionality available in moving to the cloud or embracing RPA.

The corresponding rates of adoption of cloud or RPA technologies in EMEA are 56 percent and 43 percent respectively while the same in the Americas are 43 percent and 42 percent respectively.

A similar trend can be seen for all forms of emerging technology except cognitive analytics where the Americas narrowly lead on adoption (27 percent of respondents), followed by EMEA (26 percent) and Asia Pacific (23 percent).

Fig 3.7 Level of engagement and coordination between key EERM and business leaders by region

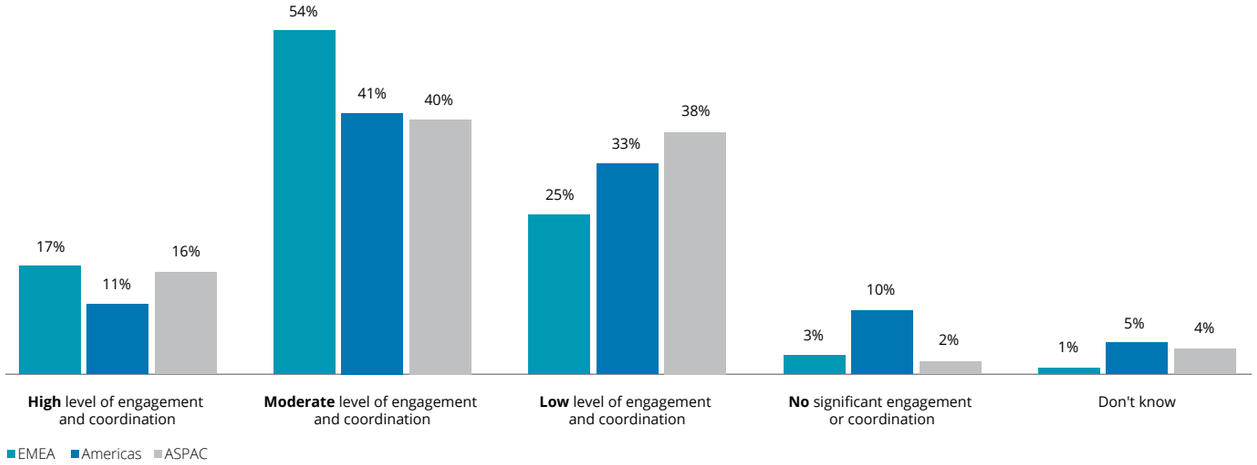
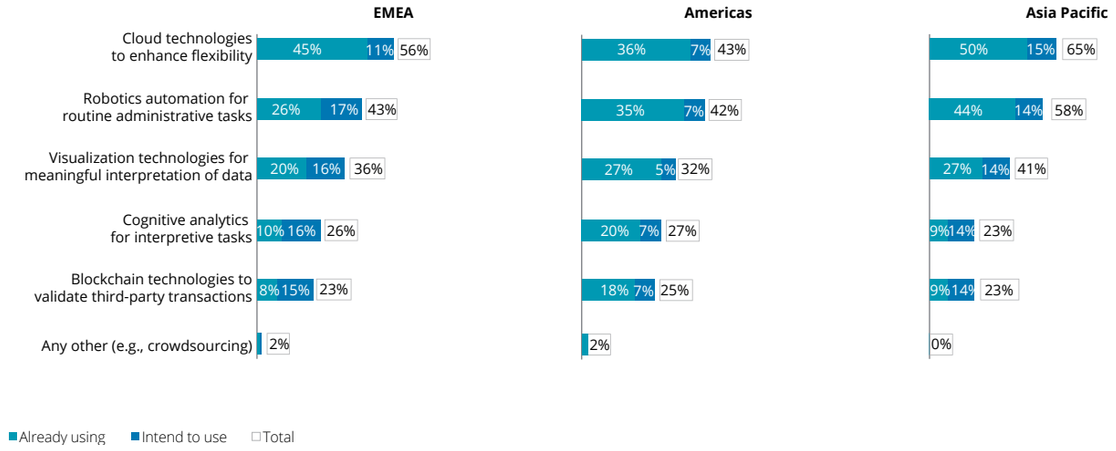


Fig 3.8 Emerging technologies being explored for EERM by region



04

Operating model

Federated structures are the dominant operating model for EERM, underpinned by shared services and centers of excellence.

The story so far

Our surveys between 2015 and 2018 identified various changes in operating models for third-party risk management.

In 2016, organizations were in the process of deciding between centralized in-house models and external service-provider based models, though for third-party monitoring only.

By mid-2016, this had emerged as a much broader debate between decentralization and centralization of key elements in governance and risk management. Some decentralization was required to make operating units agile to changing market and customer requirements yet, the EERM function itself needed to be more centralized to enable consistency.

2017 and 2018 saw centralized elements in roles, technologies, and processes become more common but within decentralized structures. As a result, centers of excellence (CoEs) and shared services centers (SSC) started to emerge as the most common operating models, with an increasing desire to explore market utility models and managed services models provided by third parties.

Federated structures are the dominant operating model for EERM, underpinned by shared services and centers of excellence.

2019 findings

Our current survey shows that federated structures for EERM, underpinned by a CoE or SSC, now exist in two-thirds of organizations (69 percent). These structures are accelerating the shift to sustainable operating models for EERM. Only 11 percent of organizations remain highly centralized (down from 17 percent last year). Most of the remaining 89 percent that are not yet highly centralized are introducing federated structures for EERM (69 percent of respondents).

Emerging federated structures for EERM are increasingly underpinned by:

- **CoEs: 53 percent** of organizations already have them. and a further 21 percent intend to establish them
- **SSCs: 38 percent** of organizations use them and a further 20 percent aspire to.

Our 2019 survey reconfirmed the growing popularity of managed services and shared assessments and utilities, as a common feature across diverse operating units that otherwise act with varying degrees of autonomy. These operating units could be a business or geographic unit or functional area.

For the first time, our 2019 survey captured uptake on three different types of managed services model:

1. **Managed services to acquire risk intelligence**, including utility models that facilitate the shared exchange of such data. 18 percent of organizations use these and a further 21 percent plan to. This is the most popular managed services solution.
2. **Managed services deploying on-premise staff**. 18 percent of organizations use these and a further 13 percent intend to.
3. **Managed services solutions deploying EERM technology** as a service. 11 percent use these and a further 14 percent plan to.

Investments in managed services and shared assessments and utilities, drive efficiency by reducing the need to increase headcount and drastically reduce capital expenditure.

Nearly three quarters (73 percent) of respondents expect that cumulative capital costs should not exceed annual operating costs of EERM, once they adopt these sustainable solutions. A further 14 percent do not go so far, but believe that capex should come down to about twice that of annual operating costs, with 10 percent putting the ratio at three times. This would mark a sharp decline from respondents' estimate last year that cumulative EERM capex is typically three to five times their annual operating cost.

Our current survey revealed another new collaborative trend: co-ownership of budgets – albeit underpinned by a fundamentally stronger element of centralized control. Core business leadership and procurement increasingly control budget for EERM.

- **CEO/board/executive leaders: 24 percent**
- **Procurement: 27 percent**
- **Business units: 28 percent**
- **Geographic leadership: 4 percent.**

Fig 4.1 Federated structures for EERM are emerging as the norm

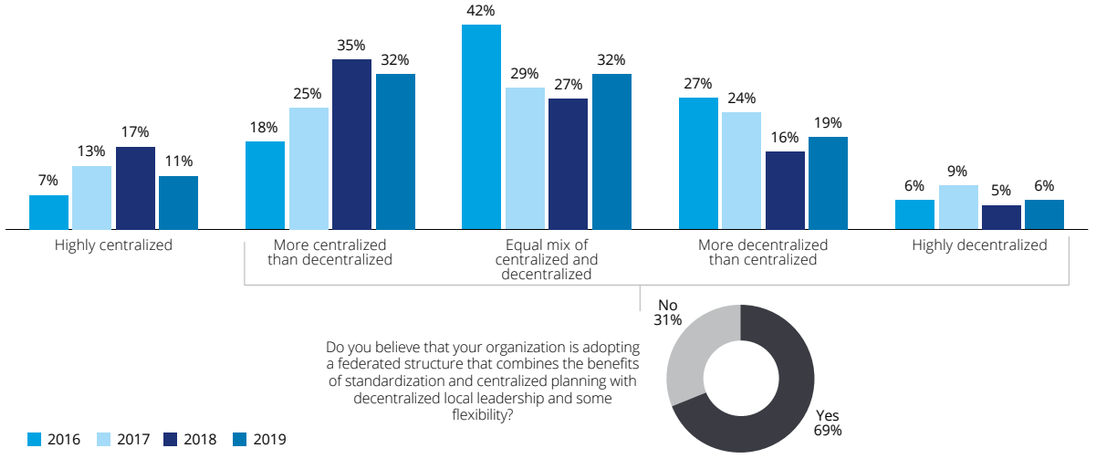


Fig 4.2 Use of CoEs, SSCs, managed services, and utilities

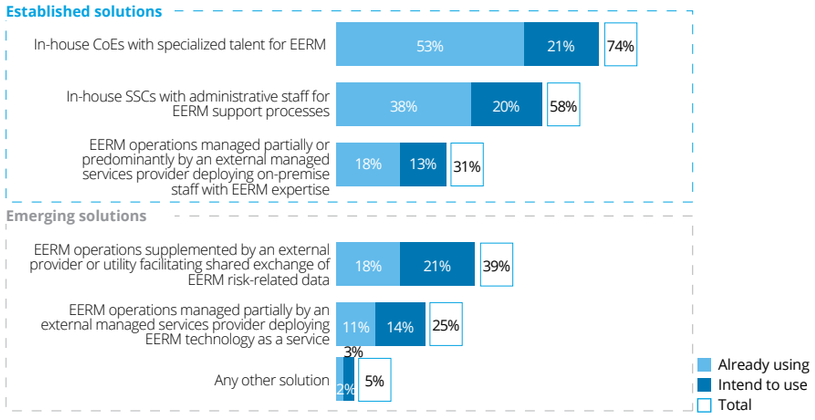
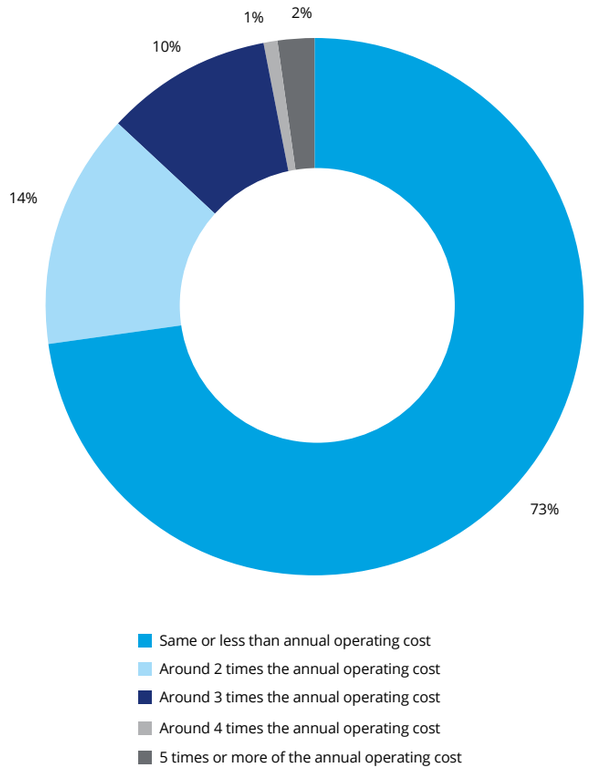


Fig 4.3 Level of investment in EERM capex



Deloitte point of view

The growing trend towards a more centralized yet collaborative approach to EERM is a pragmatic way to proceed. It could generate considerable value, including:

- Financial benefits
- Efficiency gains
- Improvements in quality
- Consistency of rigor through controlled agility.

CoEs and SSCs can unlock this value through a more joined-up approach across the more autonomous operating units within the organization.

The emerging trend of co-ownership of EERM budgets recognizes the diversity of operating unit environments and the needs of local stakeholders. Organizations are retaining centralized control over EERM budgets but with much stronger engagement and collaboration with business unit leaders. Unit leaders might be drawn in, for example, to include activities specific to their departments. This creates a good balance between consistency and flexibility.

Boards and executive leadership have started investing in emerging technologies to provide online real-time insights on EERM. These technologies better equip boards and executives to make decisions about third-party issues and are an integral component of sustainable operating models. The more centralized yet collaborative approach makes it easier to implement such overarching initiatives in EERM.

Considering a managed services solution is the logical next step in establishing common EERM delivery.

The urge must be resisted for more autonomous business units to structure and select their own managed services solution to support the third-party risk management activities they consider most important and relevant. Otherwise, it will lead to inefficiency and inconsistency in EERM across the organization.

It might be appropriate for some organizations to set up certain hubs that cater to specific needs of operating units or even time zones. But, these should be appropriately resourced with staff who have the necessary skills to retain consistency of method and quality, and are not appropriate for all organizations.

Industry highlights

All industries demonstrate a balance between centralized control over EERM budgets and a spirit of increasing collaboration and joint ownership.

The technology, media & telecoms sector had the smallest proportion of organizations considered highly centralized (9 percent), followed by financial services (10 percent), and government & public services (11 percent). Life sciences & health care organizations (15 percent) were most likely to consider their organization highly centralized, just followed by energy & resources (14 percent).

Government & public services organizations were the most likely to think they were adopting a federated structure (88 percent). Next came consumer & industrial products (72 percent) and life sciences & health care (71 percent).

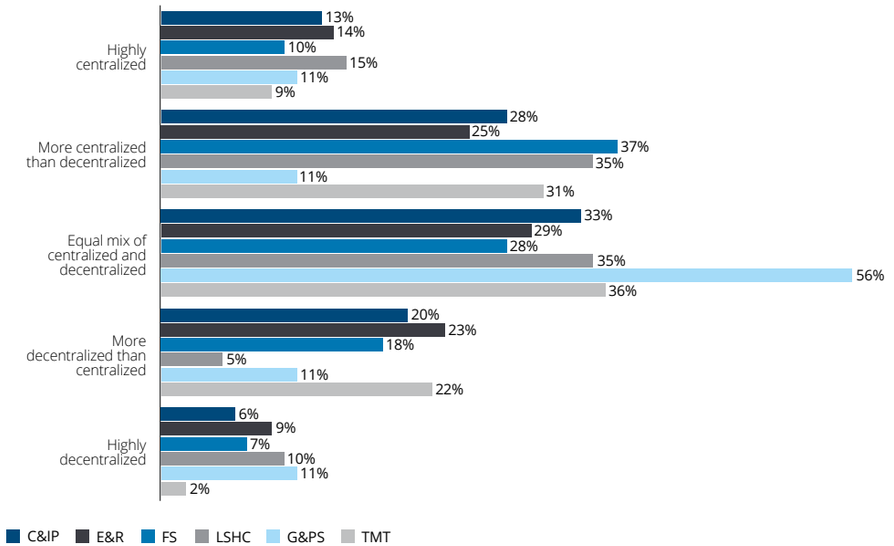
Life sciences & health care had the highest adoption of CoEs: 95 percent of organizations had created them, or intend to. Next came government & public services (78 percent) and financial services and consumer & industrial products (73 percent in both cases).

Life sciences & health care organizations were also the most likely to adopt internal shared service centers: 70 percent had done this or intend to. Consumer & industrial products (62 percent) followed, and then government & public services (56 percent), and energy & resources (55 percent).

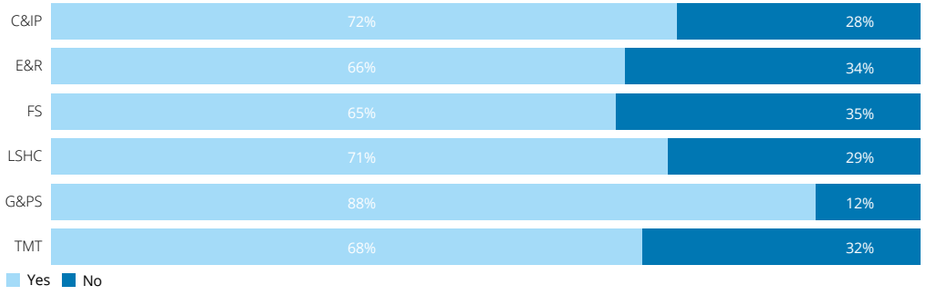
Consideration of managed services solutions is growing across all sectors. The more traditional form of managed services solutions that deploy on-premise staff was most popular in life sciences & health care, with 50 percent of respondents already adopting or planning to adopt such solutions. In government & public services, this was 44 percent, and consumer & industrial products 35 percent.

Life sciences & health care organizations were also most likely to adopt managed services solutions to acquire risk intelligence, including utility models facilitating shared exchange of data (55 percent of respondents). Other sectors most likely to adopt these were technology, media & telecoms (51 percent), consumer & industrial products, and energy & resources (41 percent each).

Fig 4.4 EERM structures adopted by industry

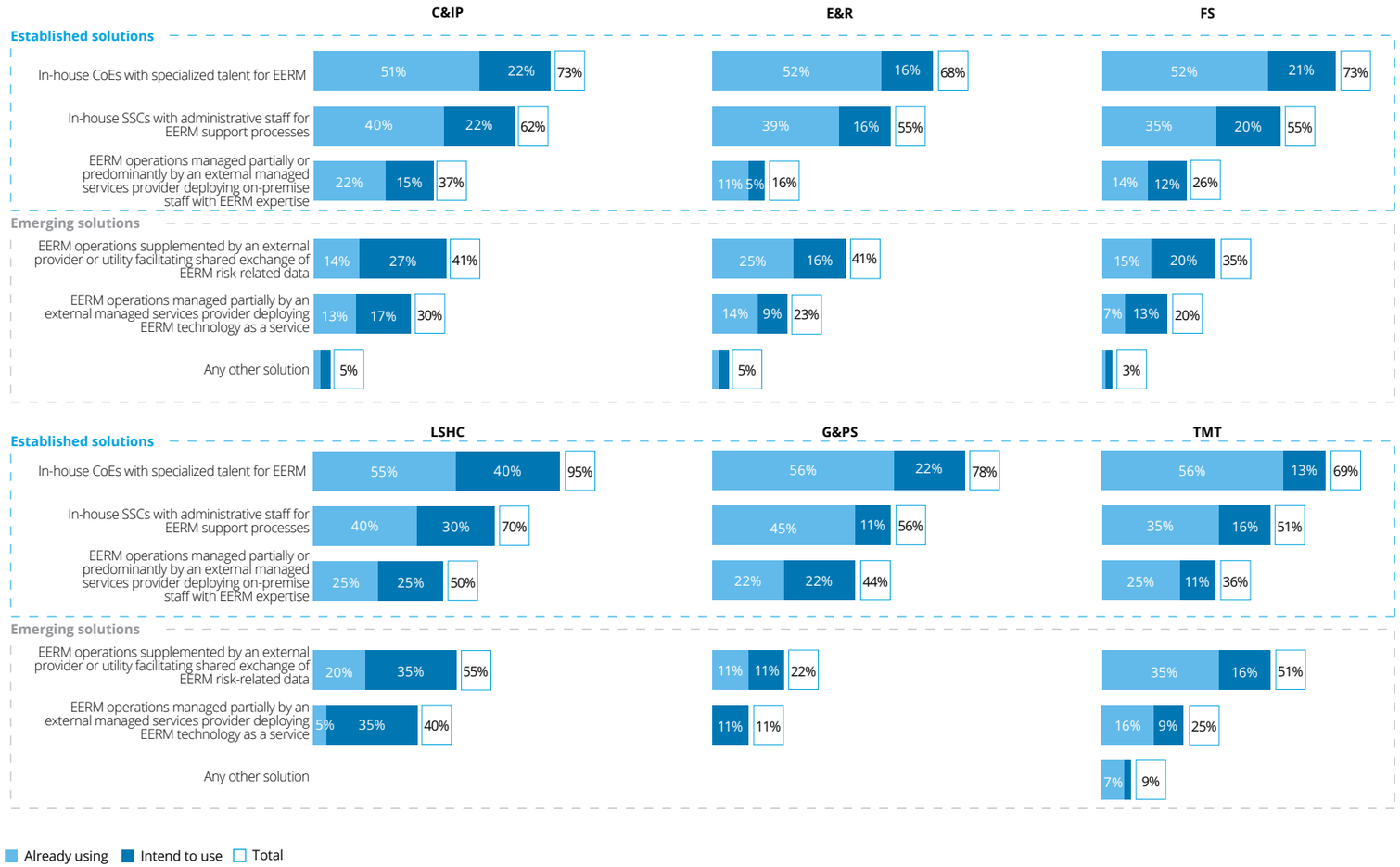


Do you believe that your organization is adopting a federated structure that combines the benefits of standardization and centralized planning with decentralized local leadership and some flexibility?



*See end note 4 for industry categories in full

Fig 4.5 Models used or intend to be used to support federated structures by industry



Geography highlights

The overwhelming majority of organizations across all three regions had some element of decentralization, reducing those that were highly centralized to a small minority. Only 12 percent of organizations in EMEA were highly centralized, followed by 10 percent in the Americas, and 9 percent in Asia Pacific.

More than three quarters (76 percent) of organizations in Asia Pacific were adopting a federated structure to bring in the benefits of centralized control in EERM. This was slightly lower in EMEA (69 percent) and the Americas (60 percent).

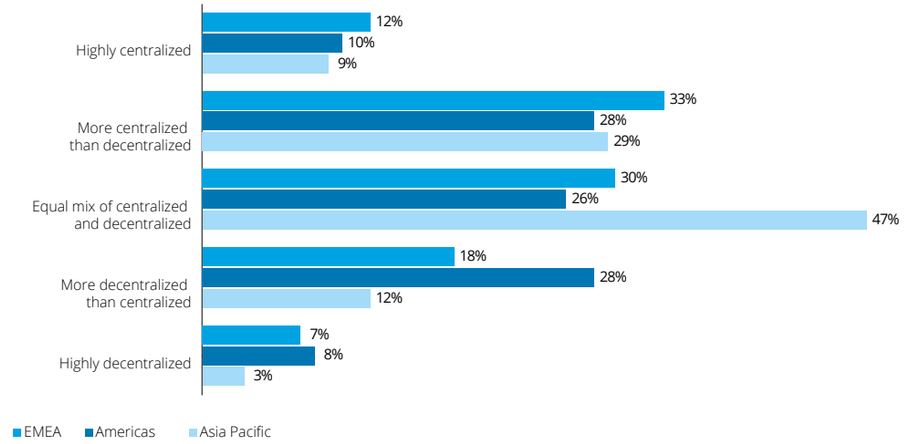
Asia Pacific also leads in the intended adoption of CoEs and SSCs, although rates of actual take-up are similar across the world. This is likely to be because of the predominance of or ease of access to SSCs in the region over EMEA and the Americas.

Perhaps for the same reason, the managed services model characterized by on-site deployment of staff is more common in Asia Pacific too. Nearly half (46 percent) of respondents had adopted this model, with a further 22 percent intending to. This once again reveals untapped opportunities for respondents in the Americas and EMEA.

Asia Pacific is also at the forefront in managed services that involve shared exchange of third-party risk data or deployment of technology as a service.

The Americas most commonly give control of EERM budgets to core leadership (60 percent) and procurement teams (30 percent). It is followed by EMEA (58 percent for core leadership and 30 percent for procurement teams). In Asia Pacific, core leadership teams controlled EERM budgets in only 43 percent of cases, and procurement teams in 15 percent of cases. In this region the risk management department was most likely to control budgets.

Fig 4.6 EERM structures adopted by region



Do you believe that your organization is adopting a federated structure that combines the benefits of standardization and centralized planning with decentralized local leadership and some flexibility?

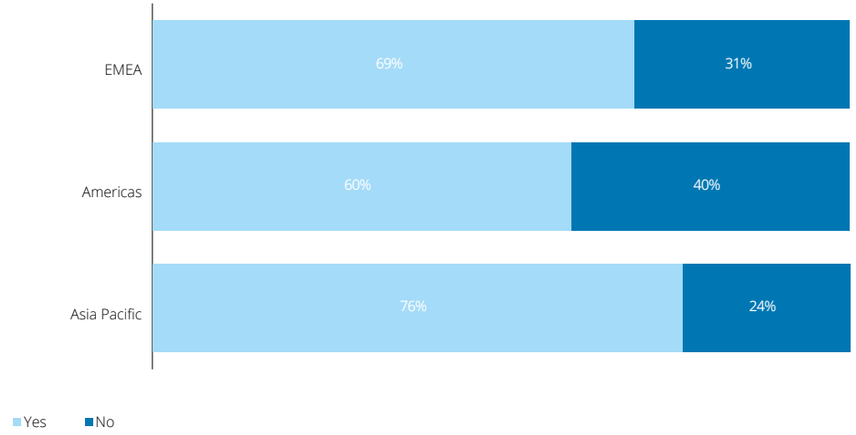


Fig 4.7 Supporting models for federated structures by region

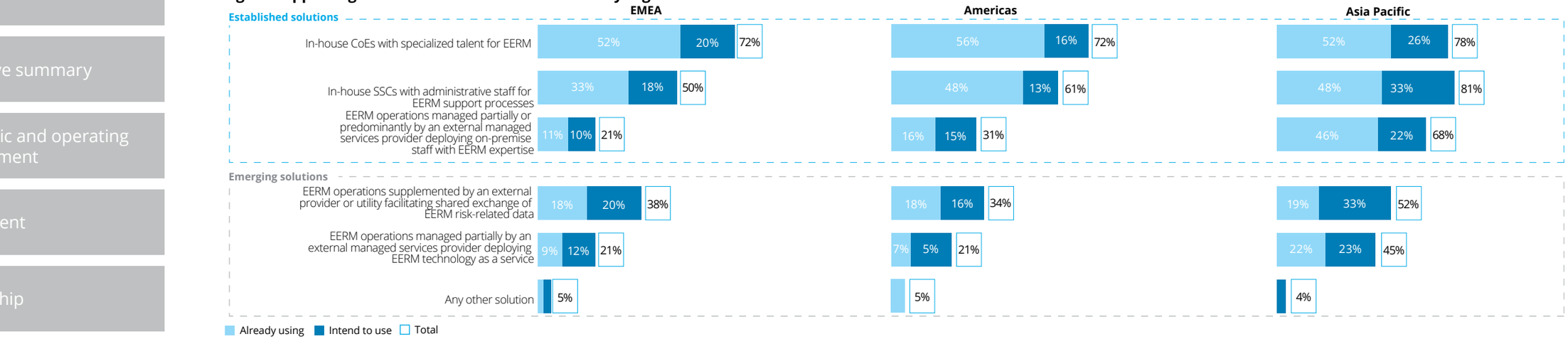
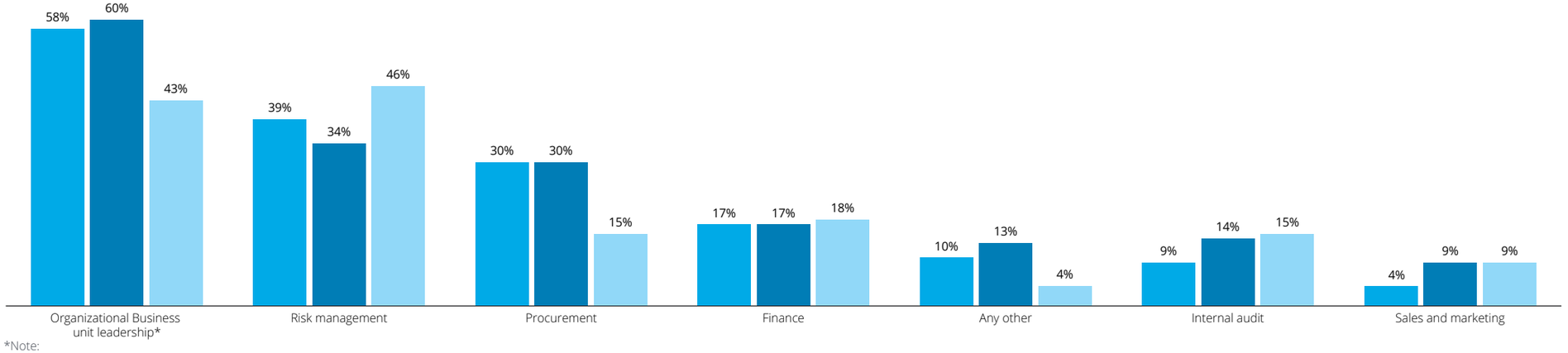
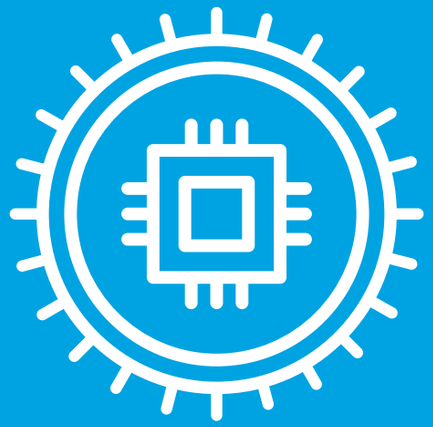


Fig 4.8 Budget ownership for EERM by region



*Note:
Organizational/business unit leadership comprises CEO/executive leadership/board, business unit, and geography leadership
Total in excess of 100% in this chart indicates multiple ownership of EERM budgets, typically between leadership and other functions, echoing the spirit of a federated structure

05



Technology

Organizations are streamlining and simplifying EERM technology across diverse operating units.

The story so far

Our EERM survey revealed a disorganized approach to the use of technology for end-to-end EERM processes in 2016.

By the following year, the vast majority (90 percent) of respondents raised issues concerning tools and technologies used for EERM. There was concern about the lack of a single unifying technology to manage third-party risks holistically and disparity of third-party management processes used across organizations. This was making it difficult to integrate and optimize EERM.

By 2018, however, two emerging trends started reducing this concern.

First, as discussed earlier in this report, the stage was being set for a more coordinated approach to investment in technology, through the:

- Introduction of centralized ownership and management: and the
- Growing popularity of CoEs and SSCs.

Second, a three-tier technology architecture (see diagram right) had emerged. A single technology solution for EERM was still to emerge.

Organizations are streamlining and simplifying EERM technology across diverse operating units.

2019 findings

Our 2019 survey confirms our prediction that a tiered approach for streamlined and standardized technology investments in EERM will continue. Very few organizations want to develop their own complex bespoke solutions. This supports the adoption of sustainable operating models, as discussed in the earlier section of this report.

Tier One

Our current survey reveals a much stronger position for the major ERP and procurement platforms within the first tier. Respondents say these help to establish a common foundation and operational discipline to support the emerging federated structures. More than half (59 percent) of organizations leverage their ERP or procurement platforms as the core foundational component for EERM. Common solutions include:

- SAP (30 percent of respondents).
- Oracle (17 percent).
- SAP Ariba (15 percent).
- Microsoft Dynamics (8 percent).

Tier Two

Three quarters (75 percent) of respondents adopt risk management solutions for EERM. There was debate among respondents around the choice of:

- **EERM-specific risk management packages**. Nearly two in ten (18 percent) organizations use EERM-specific risk management packages. These are sometimes referred to as "best of need" solutions. Or,
- **Generic integrated risk management solutions** used for third-party management requirements. More than half (57 percent) of organizations use generic integrated risk management solutions for EERM use. These streamline organizational technology architecture in the organization, and are sometimes referred to as "best of breed" solutions. Solutions include RSA Archer (13 percent of respondents), IBM OpenPages (8 percent), Thomson Reuters (6 percent), ServiceNow, and MetricStream (4 percent of respondents in each case).

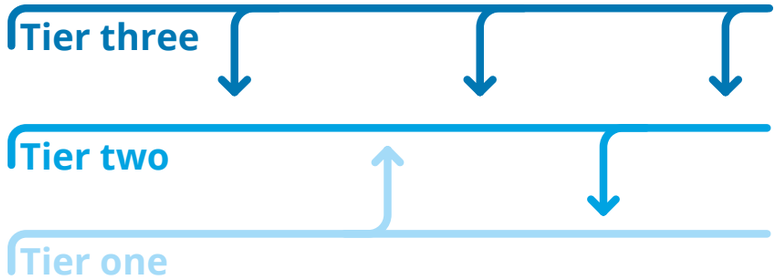
Tier Three

Domain-specific risk intelligence solutions are now commonplace as the third tier. The solutions available continue to grow in specific risk domains such as:

- Financial viability: 30 percent of respondents.
- Financial crime: 28 percent.
- Contract management: 18 percent.
- Sustainability: 11 percent.
- Cyber threats: 9 percent.

Organizations seek to acquire risk intelligence in other risk domains without investing in resources and headcount in-house, for example, using managed services or utilities.

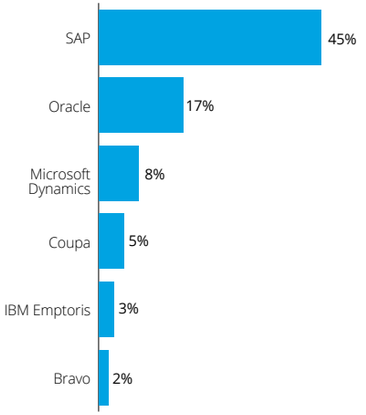
The evolving tiered architecture for EERM tools and technologies



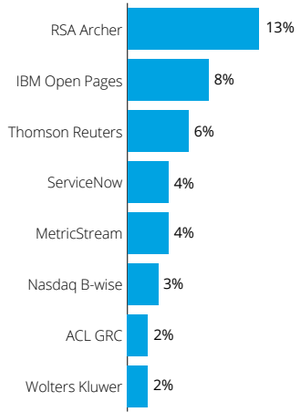
- **Tier one:** Enterprise Resource Planning (ERP) or procurement platforms that establish a common foundation and operational discipline for EERM.
- **Tier two:** Either EERM-specific risk management packages tailored to an organization's third-party management requirements, or generic governance, risk management and compliance (GRC), or controls management platforms that include EERM capability.
- **Tier three:** Niche packages for specific EERM processes or risks providing feeds from specialized risk domains such as financial viability, financial crime, contract management, and cyber threats.

Fig 5.1 Use of EERM technology solutions

(a) ERP and P2P systems or other backbone infrastructure: **59%**



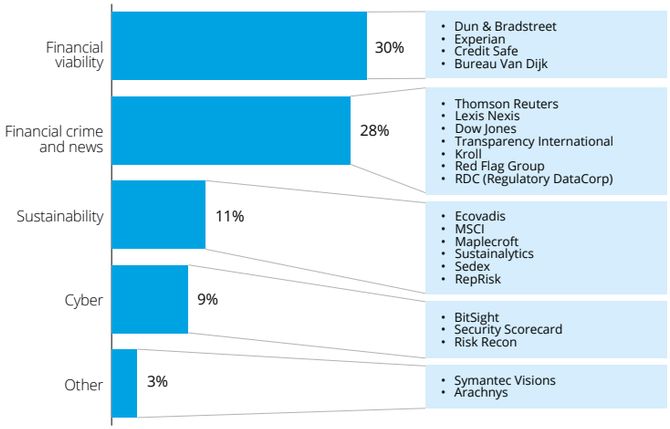
(b) GRC and controls management solutions: **57%**



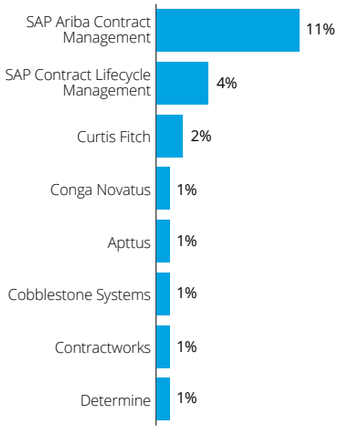
(c) EERM-specific risk management platforms or utilities: **18%**

No dominant platforms were revealed by the survey.

(d) Domain-specific feeder systems providing risk intelligence around EERM:



(e) Contract management and analytics: **18%**



Deloitte point of view

There is a strong desire for standardization and streamlining in EERM technology across diverse business and operating units. Smartly coordinated investments in EERM technology across the three tiers can drive efficiency, reduce costs, improve service levels, increase return on equity, and enable a shift to sustainable operating models.

We anticipate seeing more EERM capex invested in transformation initiatives and related design and implementation in 2019 and 2020. Many organizations should achieve their aspiration of limiting ongoing capex to the same levels as their annual EERM opex once these initiatives are implemented successfully.

There is also likely to be a convergence between third-party risk management tools and broader third-party management tools that will enable better holistic and integrated management of performance, contract, and commercial issues in conjunction with the risk generated by these issues.

The debate between standardized governance, risk management and compliance (GRC) solutions, and EERM-specific solutions is likely to continue. There will be increasing unhappiness over the fitness for purpose of standardized functionality provided by GRC solutions, even though these solutions promote easier integration within the organization.

Our survey results suggest that the current trend is an increasing adoption of "best of need" systems by many organizations, primarily to address the functionality relevant to the management of third parties. These systems will sometimes complement existing GRC solutions.

This belief is supported by a 2019 survey on GRC technology by think tank, the Open Compliance and Ethics Group (OCEG). It identified that a standardized GRC technology architecture can no longer support multipurpose user needs effectively. These needs include third-party risk management and domain-specific compliance requirements, such as cyber risk management, through a use-case approach. This has sapped satisfaction levels: In 2018 only 21 percent of users claimed good or excellent organizational alignment based on a single GRC solution with multiple use cases – a fall from 28 percent in 2016.

We also expect the evaluation criteria for EERM technology solutions to evolve beyond "cheaper, faster, better" to include:

- Support in emerging markets.
- Ability to embrace robotics and cognitive automation.
- Seamless integration with the shared utilities and managed services platforms of the future.

06

Subcontractor and affiliate risk

Organizations have poor oversight of the risks posed by third parties' subcontractors and affiliates.

The story so far

Our 2018 EERM survey recognized the realization of the significant risks associated with outsourcing. In many cases, third parties contract out some of the processes subcontracted to them – creating fourth parties. This chain can go on, creating fifth parties, sixth parties, and so on.

This expansion of subcontracting chains has led to a rise in disruptive incidents caused by organizations that appear, at first sight, to have little to do with the prime organization at the other end of the chain. A sixth party, for example, can harm the operations of the original organization connected to it through a chain comprising the third, fourth, fifth, and sixth parties. This has attracted the attention of various regulators, which are holding organizations accountable for lack of oversight of their supply chain relationships.

For some years now, organizations have also failed to address adequately how they manage relationships with affiliates.

In 2018, many of these organizations were starting to establish oversight structures for their IT and business service delivery units, whether in-house, outsourced, or provided by an affiliate entity (or a combination thereof). These structures are typically known as global business services (GBS) and are sometimes encased within separate legal entities managing complex combinations of third-party, in-house (shared services), and affiliate teams. These GBS units are creating a multi-tiered challenge to EERM, with some risks similar to those of subcontractors, and some unknown.

Organizations have poor oversight of the risks posed by third parties' subcontractors and affiliates.

2019 findings

Our current survey indicates that organizations are not adequately addressing subcontractor and affiliate risks, despite commitment to embrace sustainable operating models and enabling technology.

Subcontractor risk

Subcontractor risk – also referred to as fourth and fifth party risk – is still not attracting the appropriate level of attention from EERM leadership.

Only 2 percent of respondents (the same as last year) identify and monitor all subcontractors engaged by their third parties. A further 8 percent (down from 10 percent last year) do so for their most critical relationships. The remaining 90 percent lack the required ongoing focus:

- 11 percent assess this only when taking on a new third party (up from 8 percent last year)
- 44 percent rely on third parties to do so (the same as last year)
- 18 percent do this on an ad hoc basis (the same as last year)
- 17 percent do not identify, assess, or monitor third parties at all (the same as last year).

Affiliate risk

Organizations also continue to lack clarity in their approach to monitoring and managing risks related to affiliates. Nearly a third (32 percent) of organizations applied the same rigor in evaluating and monitoring such risks as they do with third parties. However, nearly half (46 percent) reported varying standards, including some degree of ambiguity or an ad hoc approach. Generally, initial due diligence processes and ongoing monitoring related to affiliates appear significantly lighter-touch than those applied to other third parties. The remaining 22 percent of organizations did not have any significant affiliate relationships.

Fig 6.1 Monitoring of subcontractors engaged by third parties

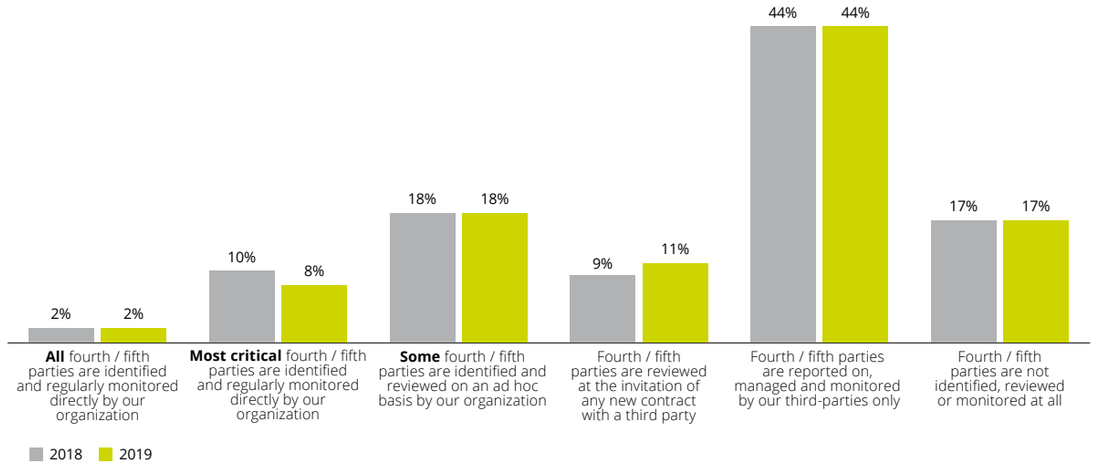
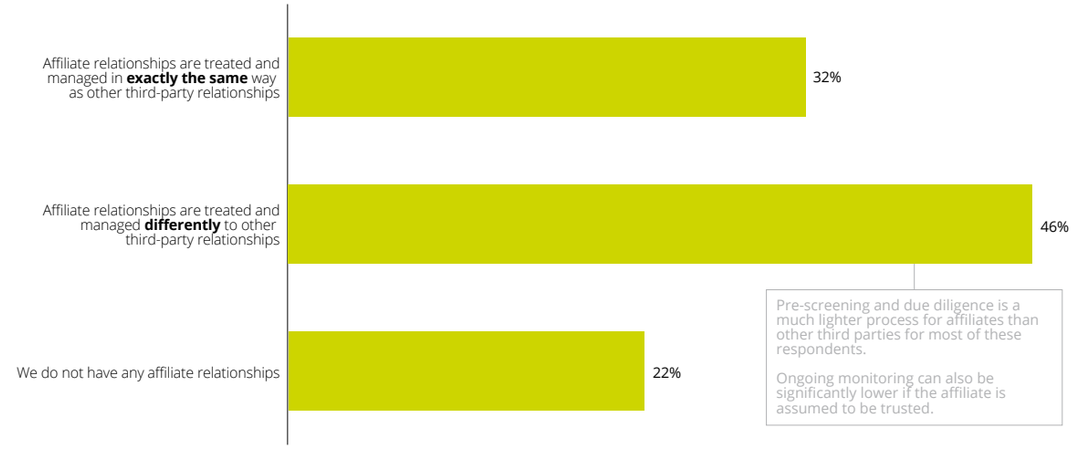


Fig 6.2 Approaches to managing affiliates



Deloitte point of view – subcontractor risk

The lack of appropriate oversight over subcontractors is making it difficult for organizations to determine their strategy and approach to the management of subcontractor risk. The risks typically reside in deeper layers of the third-party ecosystem, so this lack of oversight impairs their ability to apply the appropriate discipline and rigor to managing risks.

This issue is particularly relevant to regulated industries such as financial services, where systemic concentration risks are a significant cause for concern. However, recent legislation and regulation extend this concern to other industries as well, because they include requirements to manage relationships with fourth and fifth parties. These developments include the UK's Modern Slavery Act and the EU's GDPR. Concentration risks may also be embedded within some of these multiple tiers of the extended enterprise, requiring ongoing assessment.

Leading organizations are starting to address these blind spots through "illumination" initiatives to discover and understand these "networks within networks". Once they grasp who their critical subcontractors are, the next step is to understand what assurance their third party is obtaining about these fourth parties. This assurance must be supported by evidence.

We understand that some organizations go further, to form combined inspection teams with their third parties to undertake assurance activities on fourth parties. In addition, some organizations also request the option to complete additional assurance activities themselves. This would typically need to be enabled by the third-party's contract with the fourth party.

More commonly, leading organizations are adopting a less invasive approach by using risk intelligence tools to understand critical fourth party control environments including financial solvency. In some cases, these organizations insist on the ability to veto subcontractors to their third-party, if they believe they pose too much risk.

Deloitte point of view – affiliate risk

As affiliates are typically part of the same group, organizations are likely to have a higher level of risk-intelligence, for instance around the existence of common (group-wide) risk policies and reviews carried out by group internal audit teams. Additionally, there is no need to separately assess certain risks such as financial viability that impact the entire group.

For this reason, a lighter touch for managing affiliates than external providers may sometimes be acceptable if it is proportionate to the risk involved. This must, however, be grounded in appropriate and ongoing assessment of conformity and compliance. The approach to making this assessment must be clearly defined and consistent, not varying and ad hoc.

At the same time, GBS structures (as a newer variant of subsidiary or affiliate relationships) are gaining increasing popularity in organizations. These are trying to integrate governance mechanisms and good practices across all third parties as well as internal shared service delivery teams. The scope of these structures, and the legal entities in which they sit, vary across organizations. This adds further complexity and creates multi-layered challenges for third-party risk management.

In most cases, these GBS entities are not directly within the scope of the relevant industry regulation, because regulation is generally administered by legal entities. Because of this, where risks have manifested in actual harm, organizational reputation of the primary organization using them has been damaged, business continuity has been interrupted, and these organizations have attracted substantial penalties and regulatory enforcement action due to the subsidiaries or affiliates that serve them.

Industry highlights

Organizations in government & public services most commonly fail to identify, assess or monitor their risks from subcontractors, at 44 percent of respondents. A further 44 percent chose to rely on their third parties to do this.

The next sector to most commonly fail to identify, assess or monitor its risks from subcontractors was life sciences & health care, at 30 percent. A further 50 percent relied on third parties to do this.

Only 7 percent of respondents from energy & resources, and 15 percent from financial services, did not identify, assess or monitor subcontractor risks. However, the proportion of those that relied on their third parties' EERM procedures was the same or very similar to the proportion in government & public services (44 percent for energy & resources, and 45 percent for financial services).

Life sciences & health care, and government & public services, organizations were also least likely to take the risks posed by their affiliates as seriously as risks posed by subcontractors.

70 percent of government & public services organizations, and 67 percent of life sciences & health care organizations, applied a less rigorous approach. This was grounded in an assumption, rather than confirmed facts based on formal assessment, that these entities could be trusted more than their external counterparts. Consequently, organizations believed their affiliates required a lower level of due diligence, pre-screening and monitoring.

Technology, media & telecoms organizations were most likely to be consistent in managing affiliates and other third parties alike. 38 percent said they followed this approach, with another 31 percent stating that they did not have any significant affiliate relationships. This left 31 percent of respondents opting for the lighter approach.

Fig 6.3 Monitoring of third-parties' subcontractors by industry

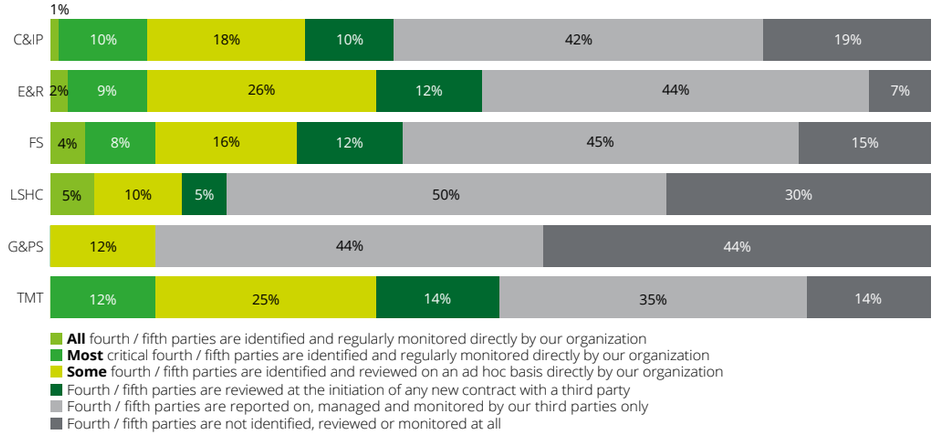
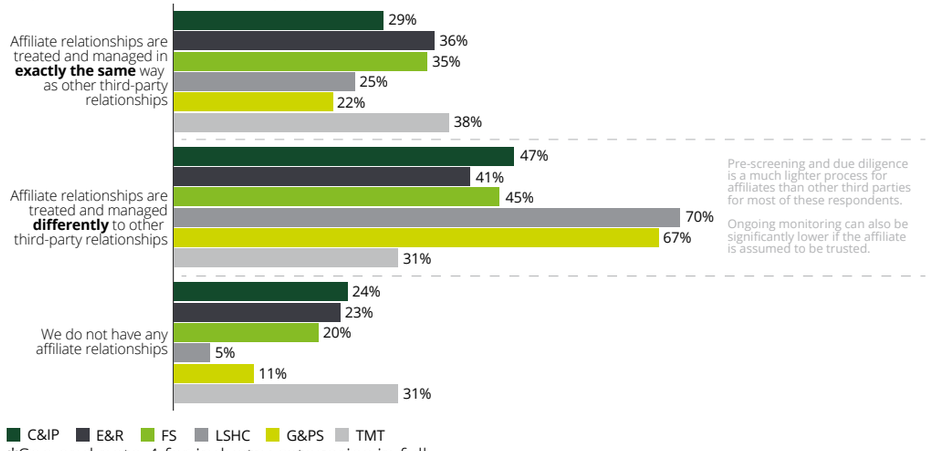


Fig 6.4 Approach to managing affiliates by industry



*See end note 4 for industry categories in full

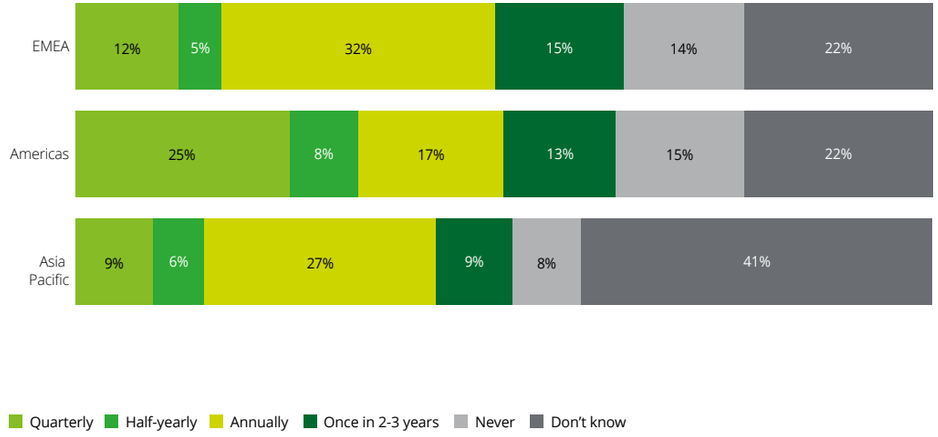
Geography highlights

There was little variation globally in the management of subcontractors and affiliates. Although in general, fewer respondents (67 percent) from the Americas had affiliate relationships, compared to 80 percent from both EMEA and Asia Pacific.

There was, however, more variation in the assessment of concentration risk (single points of failure/single geographic region) embedded in the various tiers of affiliate and other third-party relationships:

- 41 percent of Asia Pacific organizations did not know how concentration risk was being assessed, and 9 percent did not assess concentration risk at all
- 22 percent of Americas organizations did not know how it was being assessed, and 15 percent did not assess it
- 22 percent of EMEA organizations did not know how it was being assessed, and 14 percent did not assess it.

Fig 6.5 Review of concentration risk across multiple tiers of the extended enterprise by region



About the authors

Kristian Park
EMEA Leader, Extended Enterprise Risk Management
Global Leader, Third-party Risk Management
Global Risk Advisory
Deloitte LLP

Kristian Park leads the extended enterprise risk management team in the EMEA region, as well as Deloitte's global third-party risk management group. As a partner in Deloitte UK, Kristian works with his clients to develop governance frameworks to identify and manage all types of third-party risk. He looks at both process and technology solutions, performs inspections of third-party business partners on his clients' behalf, and assesses third-party compliance with contractual terms and conditions.

Kristian is also responsible for Deloitte UK's software asset management and software licensing teams, assisting clients in managing their software licensing obligations to generate efficiencies and savings. He has experience in a variety of industry sectors including life sciences, financial services, energy and resources, sport, technology, media, and consumer & industrial products.

Danny Griffiths
Director, Extended Enterprise Risk Management
Deloitte LLP

Danny Griffiths is a director in Deloitte's London based EERM team. He has 12 years of experience providing assurance and advisory services relating to third-party risk. Danny leads the third-party advisory proposition within Deloitte's UK EERM team, and specializes in supporting clients to develop third-party governance and risk management frameworks.

Danny also has significant experience leading compliance programs for large national and multinational organizations, assessing third-party compliance against contractual obligations. He has led inspections across a range of third parties including suppliers, outsourcers, marketing agencies, distributors, resellers, and licensees.

He has experience working in a broad range of industries including financial services, telecoms, media & technology, consumer, sports, energy and utilities, real estate, and public sector. He has led projects in multiple countries within EMEA, the Americas, and Asia Pacific, and regularly hosts roundtables and presents at forums on third-party risk.

Mark Bethell
Partner, Extended Enterprise Risk Management
Deloitte LLP

Mark Bethell is a partner in the UK EERM practice. Mark rejoined Deloitte in 2015 after spending four years at a global FTSE 5 company. While working there Mark led the design and implementation of a global third-party risk management framework. Mark's other roles while there included, membership of the internal audit leadership team with accountability for all internal audit work performed in relation to the extended enterprise (contractors, suppliers, and joint ventures).

Since returning to Deloitte, Mark has led a number of projects to help clients across many industries manage the risks associated with the extended enterprise. He has helped his clients to design, build, and implement third-party risk management frameworks and design and operate large-scale, global programs of third-party audits covering a variety of risk types. Mark specializes particularly in the implementation of EERM managed services for his clients and in the ongoing development of technologies to support automated risk screening and monitoring.

Dr Sanjoy Sen
Head of Research and Eminence
Extended Enterprise Risk Management
Deloitte LLP

Sanjoy Sen is the head of research and eminence for third-party risk management at Deloitte LLP.

He has a doctorate in business administration from Aston University in the UK based on his global research on the third-party ecosystem. He also holds the honorary title of visiting senior fellow in strategy and governance in the school of business and economics at Loughborough University. Since 2014, Sanjoy's work has been cited in various global academic and professional journals, newspapers, and conference papers.

Sanjoy has extensive experience advising boards, senior leadership, heads of risk, and internal audit on strategic governance and risk management of the extended enterprise, outsourcing, and shared services. He has worked across the UK, Gibraltar, India, and various countries in the Middle East.

He is a chartered accountant (FCA), cost and management accountant, and certified information systems auditor (CISA) with over 30 years of experience, including 17 years of partner-level experience at Deloitte and another big four firm.

Contacts

Global Extended Enterprise Risk Management contacts			
Global Leader	Jan Corstens	+32 2 800 24 39	jcorstens@deloitte.com
Asia Pacific Leader	Jimmy Wu	+88 6225459988	jimwu@deloitte.com.tw
EMEA	Kristian Park	+44 20 7303 4110	krpark@deloitte.co.uk
Americas	Dan Kinsella	+1 312 486 2937	dankinsella@deloitte.com
Country contacts			
EMEA			
Austria	Alexander Ruzicka	+43 153 7007 950	aruzicka@deloitte.at
Belgium	Jan Corstens	+32 2 800 24 39	jcorstens@deloitte.com
CIS	Sergey Kudryashov	+74 957 870 600	skudryashov@deloitte.ru
Denmark	Jesper Due Soerensen	+45 30 93 64 20	jessoerensen@deloitte.dk
Finland	Jouni Viljanen	+35 8207555312	jouni.viljanen@deloitte.fi
France	Gregory Abisror	+33 1 58 37 94 03	gabisror@deloitte.fr
France	Sonia Cabanis	+33 1 58 37 03 04	scabanis@deloitte.fr
Germany	Jan Minartz	+49 403 2080 4915	jminartz@deloitte.de
Greece	Alithia Diakatos	+30 2106 78 1176	adiakatos@deloitte.gr
Hungary	Zoltan Szollosi	+36 (1) 428 6701	zszollosi@deloitte.com
Ireland	Eileen Healy	+353 214 907 074	ehealy@deloitte.ie
Italy	Andrea Musazzi	+39 028 3322 610	amusazzi@deloitte.it
Luxembourg	Jan Corstens	+32 2 800 24 39	jcorstens@deloitte.com
Netherlands	Jina Calmaz	+31 8828 81871	jcalmaz@deloitte.nl
Poland	Mariusz Ustyjanczuk	+48 22 511 0939	mustyjanczuk@deloittece.com
Portugal	Joao Frade	+351 2104 27 558	jfrade@deloitte.pt
Slovenia	Polona Klep Cufer	+386 1 307 29 87	pcuferklep@deloittece.com
Southern Africa	Nombulelo Kambule	+2 711 806 5548	nkambule@deloitte.co.za
Spain	Oscar Martín	+34 914432660	omartinmoraleda@deloitte.es
Sweden	Charlotta Wikström	+ 46 73 397 11 19	cwikstroem@deloitte.se
Switzerland	Ronan Langford	+41 58 279 9135	rlangford@deloitte.ch
Turkey	Cuneyt Kirlar	+90 212 366 60 48	ckirlar@deloitte.com
United Arab Emirates	Tariq Ajmal	+971 2 408 2424	tajmal@deloitte.com
United Kingdom	Kristian Park	+44 20 7303 4110	krpark@deloitte.co.uk

Asia Pacific			
Australia	Elissa Hilliard	+61 2 9322 3014	ehilliard@deloitte.com.au
Australia	Tom Sykes	+61 3 9671 5686	tsykes@deloitte.com.au
China	Yvonne Wu	+86 21 614 115 70	yvwu@deloitte.com.cn
Hong Kong	Hugh Gozzard	+852 2852 5662	huggozzard@deloitte.com.hk
India	Vishal Chaturvedi	+91 22 6245 1010	vchaturvedi@deloitte.com
India	Munjal Kamdar	+91 22 6122 8470	mkamdar@deloitte.com
Japan	Niki Kazuhiko	+81 90 6020 8466	kazuhiko.niki@tohmatsu.co.jp
Japan	Bruce Kikunaga	+81 90834 77656	bruce.kikunaga@tohmatsu.co.jp
Korea	Min Youn Cho	+82 2 6676 1990	minycho@deloitte.com
New Zealand	Aloysius Teh	+64 4495 3934	ateh@deloitte.co.nz
Philippines	Luisito Amper	+63 2 581 9028	lamper@deloitte.com
Taiwan	Jimmy Wu	+34 9129 26985	jimwu@deloitte.com.tw
Singapore	Suci Ramadhany	+65 6800 2555	sramadhany@deloitte.com
Thailand	Weerapong Krisadawat	+66 2034 0145	wkrisadawat@deloitte.com
Vietnam	Philip Chong	+65 6216 3113	pchong@deloitte.com
Americas			
Argentina	Esteban Enderle	+54 11 43 2027	eenderle@deloitte.com
Brazil	Camila Araujo	+55 11 5186 6221	camilaaraujo@deloitte.com
Canada	Laura Joudrie	+1 416 775 7020	ljoudrie@deloitte.ca
Chile	Christian Duran	+56 22 72 98 286	chrduran@deloitte.com
LATCO	Esteban Enderle	+54 11 43 2027	eenderle@deloitte.com
Mexico	Ricardo Bravo	+52 55 508 06 159	ribravo@deloittemx.com
United States	Dan Kinsella	+1 312 486 2937	dankinsella@deloitte.com

Endnotes

1. We use the phrase “extended enterprise risk management” interchangeably with “third-party risk management” in this report given the increasing use of the term “extended enterprise” to represent the ecosystem of third parties used by an organization.

2. We have considered fully and partially completed survey responses – to the extent survey questions have been answered by these respondents – when analyzing data and preparing our report.

3. It is difficult to compare 2019 results with previous years’ surveys in some cases. This is because of the increased proportion of respondents from regions where levels of understanding and maturity in third-party risk is less developed than more mature territories.

4. Industries covered by the survey include consumer & industrial products (C&IP), energy & resources (E&R), government & public services (G&PS), life sciences & health care (LSHC), and telecoms, media & technology (TMT). Industries are referred to by acronyms in all graphics.

5. Figures set out in section 2 on investment relate to centralized spending on EERM as estimated by respondents. Some respondents have said that their organizations may be spending significantly higher amounts on EERM, given the decentralized nature of spend and activity.

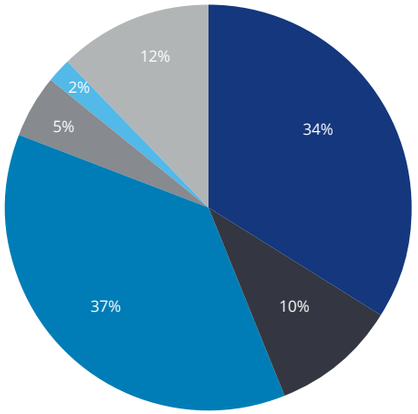
6. An affiliate organization, unlike a subsidiary, is one where the focal organization does not hold a majority stake. Control is exercised through indirect means such as a common parent organization. In some countries covered by our survey, the term “affiliates” has a broader connotation. It may include, for example, thirdparties covered by marketing agreements (for example in online retail), certain independent contractors, and so on.

Endnotes

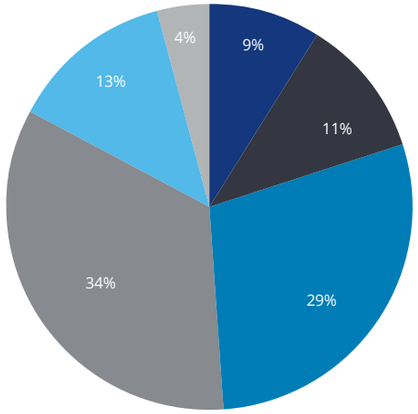
Survey respondent profiles

This year we received 1,055 responses from participants in 19 countries around the world, covering all the major industry segments. Respondents are typically responsible for governance and risk management of the extended enterprise in their organizations.

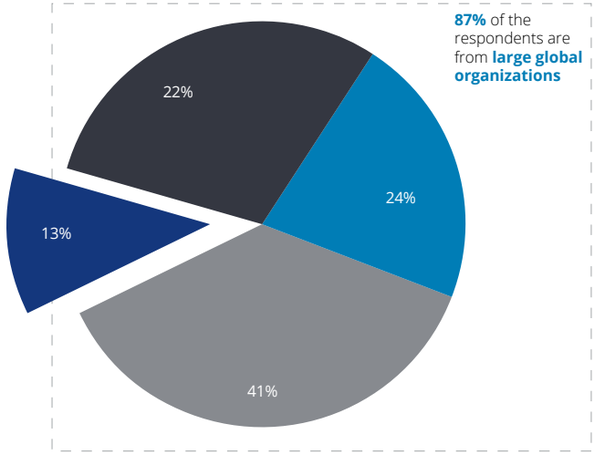
Primary industry of respondents



Respondent job titles or their nearest equivalent



Size and turnover of respondents



Deloitte.

Designed and produced by 368, London & Deloitte CoRe Creative Services, Rzeszow. J17667/263052