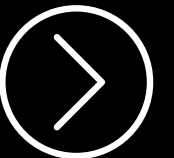


**Focusing on the climb ahead**

Third-party governance and risk management

Extended enterprise risk management global survey 2018





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts

# Foreword

Welcome to our 2018 global survey on Extended Enterprise Risk Management (EERM). This year we had just under one thousand responses, a significant increase and more than double we received last year. Survey responses reflect the views of senior leaders from a variety of organizations in 15 countries<sup>1</sup> across the Americas, Europe Middle East and Africa (EMEA), and Asia Pacific. A record number of participants this year is reflective of the ever increasing profile and investment third-party risk management is getting within organizations.

This third annual survey follows last year's survey entitled "Overcoming the threats and uncertainty" which revealed how EERM in many organizations had continued to benefit from greater executive awareness. However significant changes in the external environment (such as the Brexit result in the UK and the US presidential election) had slowed down progress in implementing holistic, integrated frameworks and risk management mechanisms. After this stagnation during 2016 in addressing EERM maturity, 2017 seems to have allowed organizations to tackle the topic with a renewed focus and investment.

Our prior surveys focused on understanding the nature and magnitude of the EERM challenge in large global organizations. Using this as a backdrop, the current survey aims to capture improvements in maturity of EERM frameworks with a specific focus on the business case and investments in EERM. The survey results also reflect an emerging shift to include more centralized oversight and management for EERM across the more decentralized or federated structures to enable increased risk-awareness and consistency. A more centralized approach to EERM also enables the aggregation of information at an 'organization-wide' level to not only have a cross-risk view of third-party relationships, but also to address issues around concentration risk. In addition to reporting other leadership initiatives and concerns, this report sets out our predictions for 2018/2019 and related points of view.

As in our previous surveys, survey respondents are typically responsible for governance and risk management of the extended enterprise in their organizations, including Chief Finance Officers (CFOs), Heads of Procurement/Vendor Management, Chief Risk Officers (CROs), Heads of Internal Audit, and those leading the Compliance and Information Technology (IT) Risk functions. The respondents represented all the major industry segments<sup>2</sup>. The majority of these organizations had annual revenues in excess of US\$1 billion. Additional insight was also obtained from subsidiaries of group organizations operating with higher degrees of decentralization and others with lower annual revenues.

I hope this report will continue to enhance your understanding of what has changed and what lies ahead as you exploit the many opportunities that EERM can yield for your organization.



**Kristian Park**  
**EMEA Leader, Extended Enterprise Risk Management**  
 Global Risk Advisory



**Jan Corstens**  
**Global Leader, Extended Enterprise Risk Management**  
 Global Risk Advisory



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts

# Revealing untapped opportunities in extending your enterprise

As companies continue to adopt, enhance, and grow their business ecosystems, EERM is increasingly becoming an astute management enabler and value driver rather than a compliance requirement.

Business ecosystems are the new norm and extending the physical and virtual boundaries of organizations to garner competitive advantage through collaboration with third-parties is an imperative. Leading organizations are investing in EERM to power growth, innovation and business performance in a risk-intelligent way to proactively address brand and reputation risk, especially important amid prevalent threats of high profile business failure, illegal third-party actions, or regulatory action with punitive fines.

Our current survey reveals that organizations are taking an earlier, more strategic view of risk drivers to create value and surface new opportunities. Seven out of ten respondents believe that business and macro-economic uncertainties have increased the risks inherent in managing the extended enterprise, at least by some extent, if not significantly. However, their overall levels of EERM maturity continue to improve at a much slower pace, which we believe to reflect awareness of the inherent complexity and challenges of an efficient EERM program.

Despite the slower pace, I'm encouraged to see an increased emphasis on utilizing risk to power performance and drive differentiation as rationale for investment in EERM, with nearly one in two respondents driven by overall cost reduction and efficiency objectives—truly, a significant shift from the near exclusive focus on the downside of risk, as reported in our last survey.

This burgeoning confidence reaffirms our belief that risk management is and can be a vital performance lever going forward.

Deloitte's Risk Advisory professionals around the world 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](http://www.deloitte.com/risk).



**Sam Balaji**  
**Global Business Leader**  
 Financial Advisory | Risk Advisory



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors

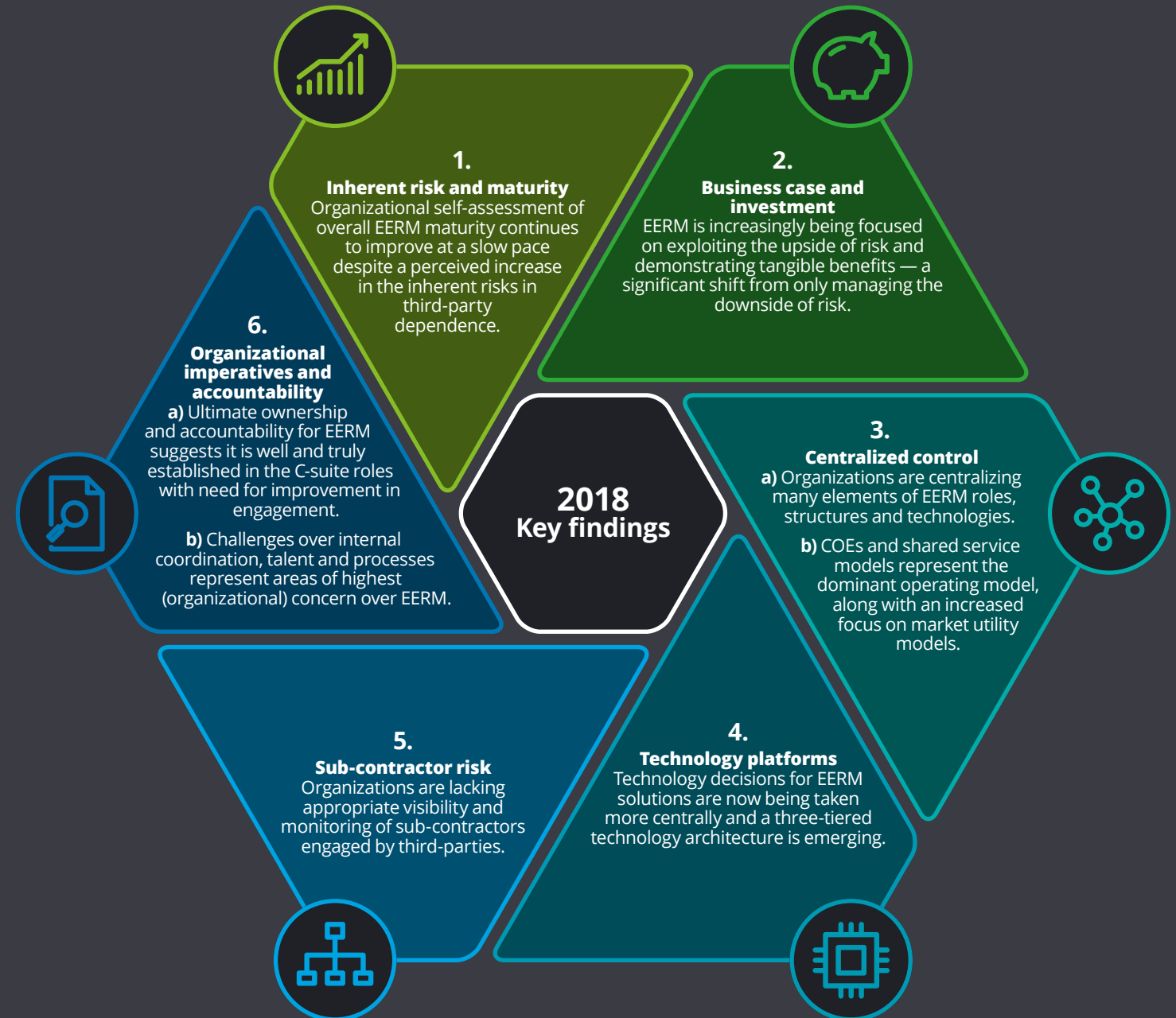


Contacts

# Executive summary

A record number of participants in our 2018 survey supports the ever increasing profile and investment that EERM now has within organizations.

Our survey has identified six key areas of focus for most organizations.





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts



# Executive summary

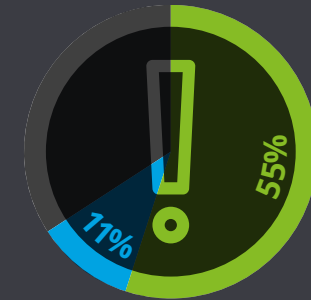
## Inherent risk and maturity

After the slowdown in 2016 to address EERM maturity, 2017 seems to have allowed organizations to tackle the topic with a renewed focus and investment. This has taken place amid an increase in the inherent risk of dependence on third-parties. This increased perception of inherent risk has been caused by continuing uncertainty in the business and macro-economic environment; concerns around emerging regulation and regulatory scrutiny; and threats of third-party related incidents/disruption. However in a year where many organizations stated that they were going to significantly move the dial in EERM maturity, the aggregate results suggests there is still work to do for many organizations to become fully integrated or optimized in their EERM capabilities (please refer to page 22 for the Deloitte EERM maturity model used in this report).

That said, the Asia Pacific region has seen some increase in respondents moving along the maturity scale to reach integrated or optimized status. This is comparatively higher than in EMEA which has had very little movement. Similarly, in industries where EERM has more recently come under increased regulatory scrutiny (e.g. Life Sciences & Health care (LSHC), Consumer & Industrial Products (C&IP), and Public Sector (PS)), we have seen significant progress in a similar upward movement along the EERM maturity scale.

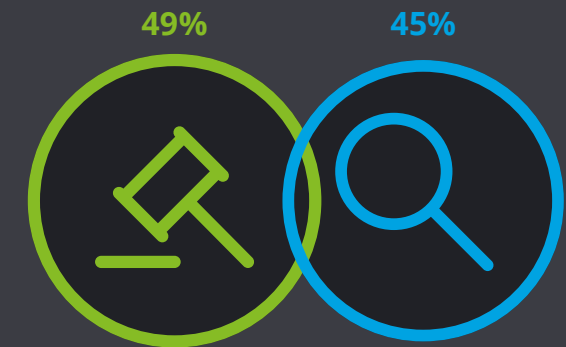
**Seven out of ten** respondents believe that risks inherent in managing their extended enterprise have increased at least by some extent if not significantly. However, organizational self-assessment of their overall levels of EERM maturity continues to improve at a slow pace.

**55 percent** of respondents perceived “some” increase in risks inherent in EERM while another **11 percent** perceived a “significant” increase in such risks.



**42 percent** of respondents reported “some” increase in their level of dependence on third-parties in the last year, with a further **11 percent** reporting a “significant” increase in such dependence (**10 percent** a year earlier).

Impact of changing regulation is considered to be the greatest contributory factor to the increased perception of inherent risks (**49 percent** of respondents) followed by heightened levels of regulatory scrutiny (**45 percent** of respondents).

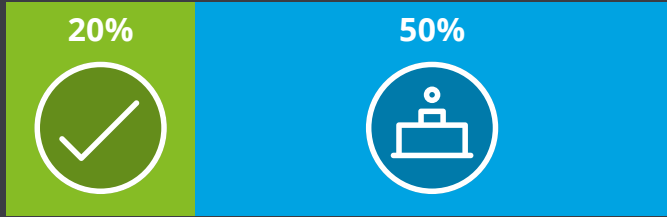






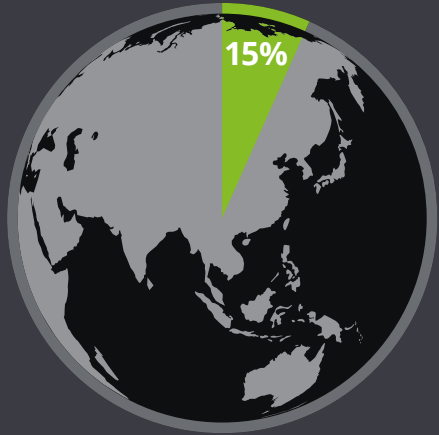
- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts

However, overall only **20 percent** of respondents have integrated or optimized their EERM mechanisms (same as last year – see paragraph below) with another **50 percent**, currently in managed status, aspiring to do so within the next 1-3 years.



In some cases, respondents, particularly from the Northern Americas region as well as from the Financial Services (FS) and Energy and Resources (E&R) industries have lowered their earlier self-assessments of maturity. This seems to reflect their deeper appreciation of the situation and a stronger understanding of third-party related issues than in the past. It should also be noted that as newer good practices continue to emerge, the goalposts are shifting too; hence in reality those that stand still are actually moving backwards on the maturity curve.

Asia Pacific have seen some increase in EERM maturity with **15 percent** of respondent organizations now having integrated their EERM systems as against **11 percent** last year. However regions, such as EMEA, have seen little increase (unchanged at **19 percent** since last year).



**53 percent** of respondents now believe that their journey to achieve the desired state of EERM maturity is two to three years or more, as against most respondents in earlier surveys being overly optimistic in believing that this can be achieved in six months to a year.



This significant increase in organizations integrating their EERM processes and technology during 2017 is also true in industries such as LSHC (**eight percent** last year to **24 percent** in the current survey), C&IP (**11 percent** to **19 percent**), and PS (**20 percent** to **35 percent**).





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts



## Executive summary

### Business case and investment

The business case for investment in EERM is increasingly being focused on **exploiting the upside of risk**—a significant shift from the almost-exclusive focus earlier on managing the downside, with increasing confidence to demonstrate tangible benefits.

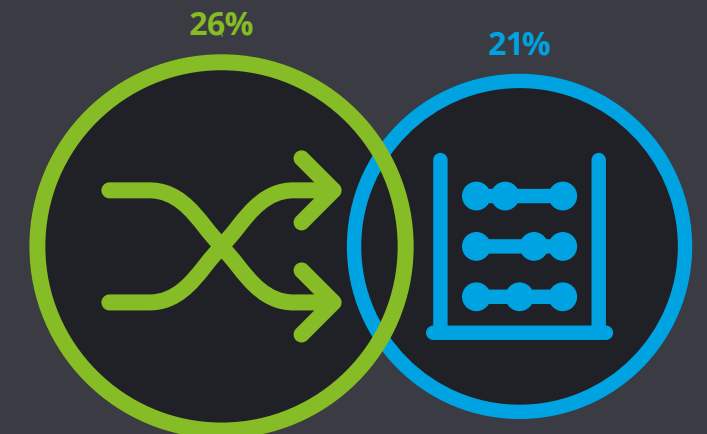
In order to achieve their desired stage of maturity in EERM, organizations have invested an average of US\$0.5 – 1.5 million per annum either in full time equivalents (FTEs) or in designing programs on a centralized basis (please refer to endnote 3 on page 66). Where EERM is considered integrated or optimized the average centralized operating costs are around US\$3 million for a majority of organizations, managed typically by more than 50 FTEs. Those with a significant amount of third-parties (50,000 or more) spent upwards of US\$5 million centrally with more than 100 FTEs, while smaller organizations with serious aspirations to move to higher maturity levels still typically invested US\$100,000 – 500,000.

The drivers for the focus on EERM continued to be regulatory requirements (e.g. General Data Protection Regulations), addressing internal compliance standards or concern around third-party related incidents, but the need for positive cost reduction across the business was equally powerful—a trend that we have not seen in prior surveys. It is also heartening to see that the business case for investment in EERM is increasingly being driven by other factors that exploit the upside of risk, such as enhancing organizational responsiveness and flexibility, innovation, brand confidence, and increasing revenues—a significant shift from the almost-exclusive focus earlier on managing the downside (such as regulatory exposure or third-party related incidents). The majority of respondents had some or significant confidence in their ability to demonstrate tangible benefits from such investment.

As many as **48 percent** of respondents were driven by overall cost reduction objectives in investing in EERM, which they felt could be achieved by bringing in efficiencies through the use of third-parties or by preventing over-payments.



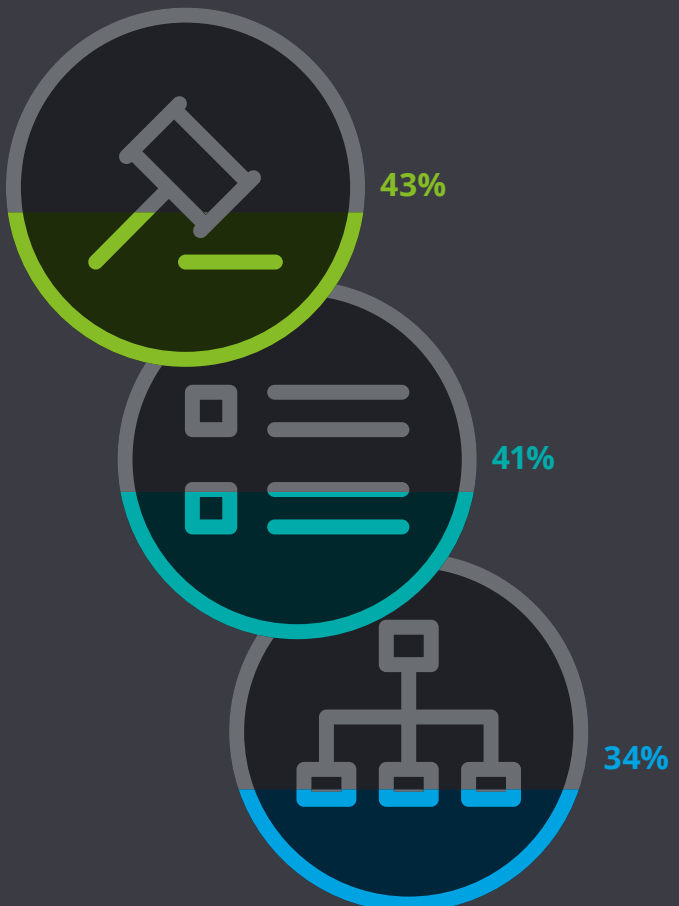
At the same time, **26 percent** of respondents felt that they could achieve greater flexibility to address market uncertainty and **21 percent** considered investment in EERM a revenue-generating opportunity, for instance by identifying under-reported revenue streams.





- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts

Reduction of regulatory exposure (**43 percent** of respondents); addressing internal compliance requirements (**41 percent** of respondents); and reducing the number of third-party related incidents (**34 percent** of respondents) were the strongest business case drivers focused on managing the downside of extended enterprise risk.



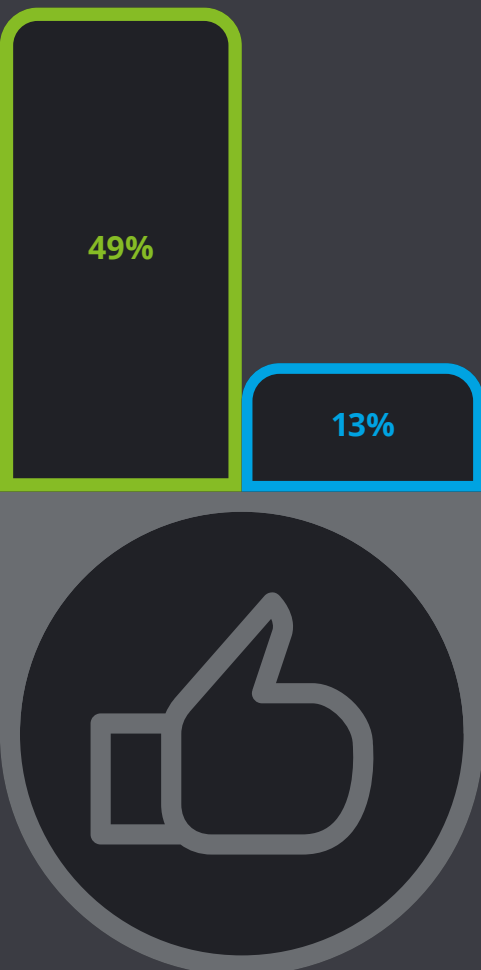
Organizations that are *integrated* or *optimized* in managing their extended enterprise are now typically investing over **US\$3 million** annually on EERM initiatives, managed by more than 50 FTEs.



Organizations that engage 50,000 or more third-parties in their extended enterprise are now typically investing over **US\$5 million** annually on EERM initiatives, managed by more than 100 FTEs.



**49 percent** of organizations felt “somewhat confident” that they could demonstrate tangible benefits from EERM investments, while another **13 percent** were “extremely confident”.







Home

Foreword

Executive summary

01 Inherent risk and maturity

02 Business case and investment

03 Centralized control

04 Technology platforms

05 Sub-contractor risk

06 Organizational imperatives and accountability

About the authors

Contacts



## Executive summary

Centralized oversight and management

Many organizations, regardless of their broader organizational structure (decentralized vs. centralized), are centralizing many elements of the EERM role, structures and technologies. For instance, **Centers of Excellence (CoEs) and shared service models have emerged as the dominant operating model** with an increasing desire to explore market utility models.

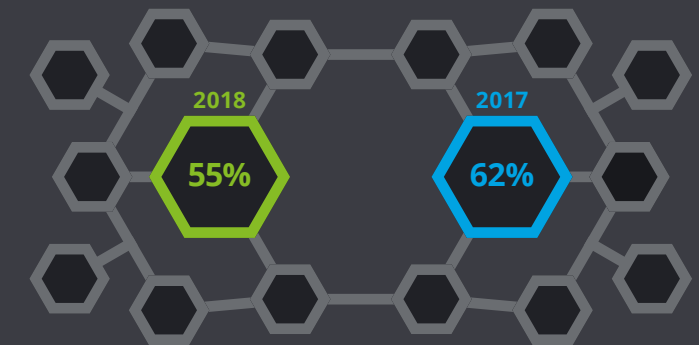
In 2016 we released our whitepaper on how to manage EERM in decentralized organizations, a theme of which suggested an element of central oversight and management could help accelerate risk awareness and efficiency. The 2018 survey results show that more and more organizations are adopting this technique with the more decentralized or highly federated<sup>4</sup> EERM models being replaced with some component of central oversight, where centralized elements in roles/structures and enabling technologies/processes are becoming more common-place.

Furthermore, most respondents told us that an internal utility for EERM, which was either a CoE or shared service center in some form (whether operated fully by in-house teams or with some coordination with outsourced service providers), was where the centralized operations sat, with just **four percent** in a fully outsourced managed services environment as an external utility for EERM.

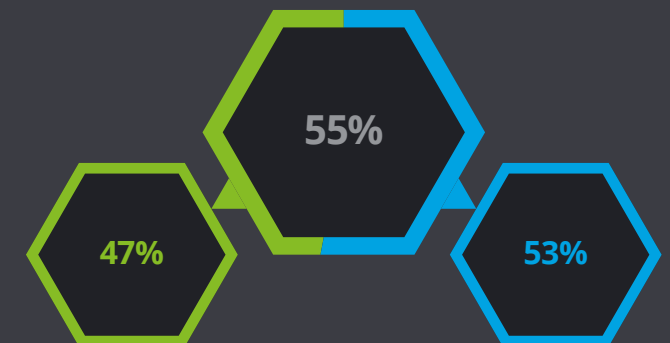
Qualitative comments provided by respondents seem to suggest that most of these internal utilities are managed by procurement teams in organizations where supply-chain or “buy-side” has the majority of third-parties. On the other hand, in organizations where third-parties are distributed more equitably across the sales and distribution network or “sell side,” this management responsibility appears to be progressively shifting to central risk management teams.

At the same time, **34 percent** of respondents suggested they either used market utility models<sup>5</sup> in some form or intend to do so in the future to supplement specific aspects of EERM activity. Consistent with last year, half of respondents were unaware of managed service/utility options available to them, which is understandable, given that such opportunities are relatively new and are still evolving.

**55 percent** of organizations are now equally or more decentralized than centralized (down from **62 percent** last year). This reflects that organizations are starting to scale back on decentralization in the overall organization.



Out of these 55 percent, only **47 percent** have EERM frameworks that are equally or more decentralized than centralized. The remaining **53 percent** of respondents thus form the current majority with more centralized EERM programs.

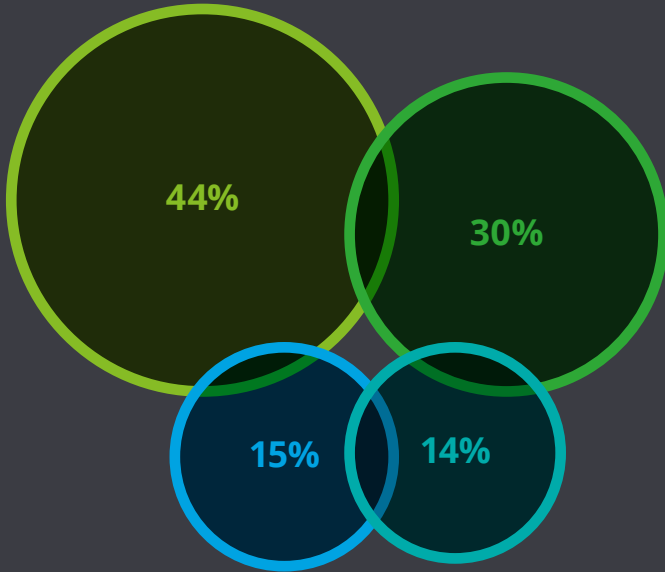




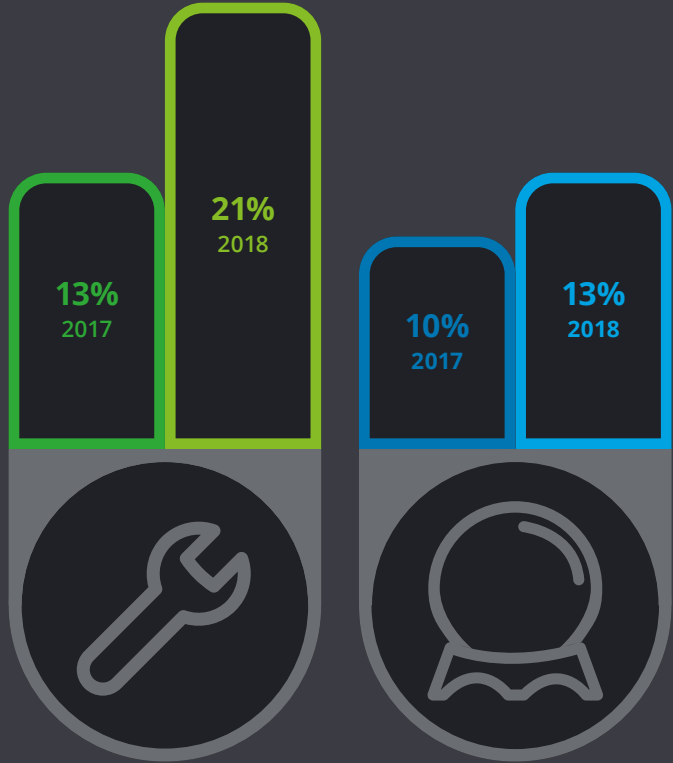
- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts

**44 percent** of respondents have now invested in a centralized in-house CoE for EERM while another **30 percent** utilize a central shared services organization (whether fully insourced or with some elements outsourced).

A further **15 percent** have established federated structures and **14 percent** operate as a "hub-and-spoke" model<sup>6</sup> where centralized elements of EERM are becoming more common-place.

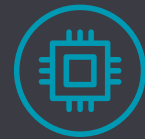


**21 percent** of respondents are already utilizing market utilities for specific aspects of EERM (up from **13 percent** last year) with another **13 percent** intending to do so in the near future (up from **10 percent** last year). Consistent with last year, half of respondents were unaware of managed service/utility options available to them.





-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  02 Business case and investment
-  03 Centralized control
-  04 Technology platforms
-  05 Sub-contractor risk
-  06 Organizational imperatives and accountability
-  About the authors
-  Contacts



# Executive summary

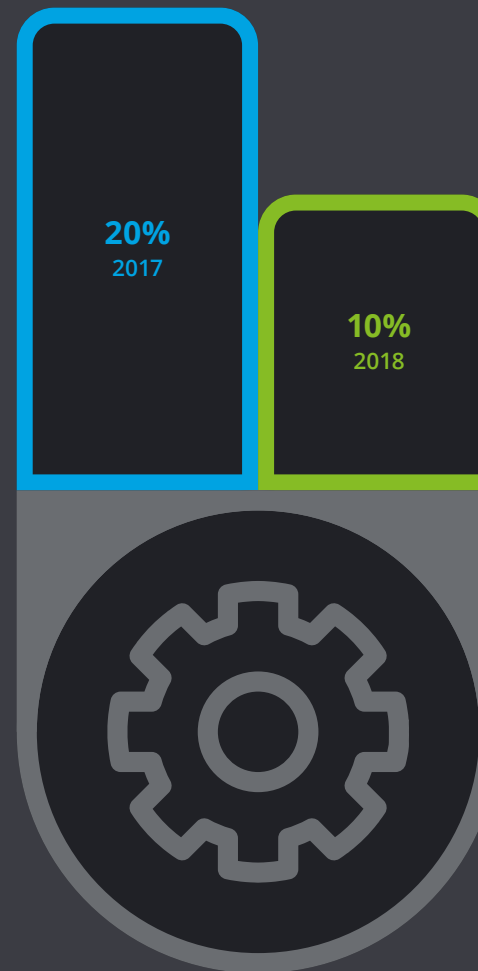
## Technology platforms

In keeping with the trend of increased centralized oversight of EERM activities, **technology decisions are now being taken more centrally** and a standard tiered technology architecture is emerging.

The 2018 survey suggests that a three-tier technology architecture will increasingly form a common setup for organizations around EERM and typically comprises of (i) ERP systems or other backbone applications for procurement; (ii) generic GRC software or EERM-specific risk management packages tailored to the organization and (iii) other niche packages for specific EERM processes or risks with feeds from specialized risk domains.

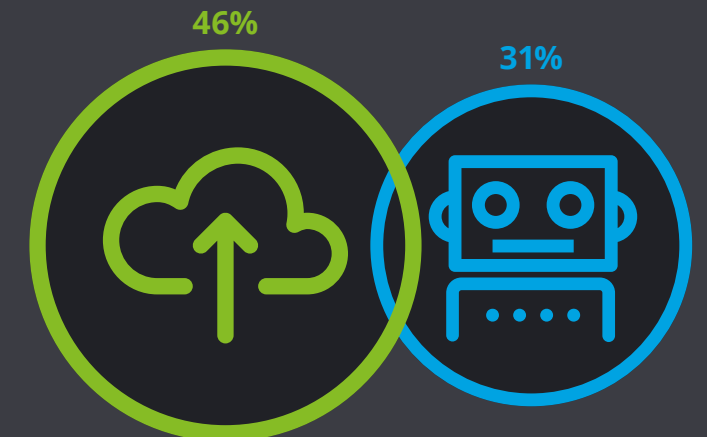
Aligned to this trend, qualitative responses from the survey indicate that organizations are no longer keen to invest in developing complex bespoke solutions for EERM, which, together with the use of its existing ERP platform in the past may have significantly lowered the confidence of stakeholders in the quality and reliability of the overall technical solution for EERM.

Less than **10 percent** of respondents are currently using bespoke systems for EERM, a sharp drop from just over **20 percent** last year (please also refer to our subsequent section on predictions for 2018/2019 on technology).



Standardization of technology architecture for EERM using a combination of ERP systems and other backbone applications for procurement packaged solutions is supported by an increasing intent by management to invest in emerging technologies for EERM. Cloud technologies that enable agile business operations with standardization represent the most popular emerging technology platform being investigated by survey respondents. Robotic Process Automation (RPA) features second on this list, offering the opportunity to automate routine tasks related to EERM.

**46 percent** of respondents are planning to utilize standardized cloud technologies for EERM while **31 percent** are considering using RPA for routine EERM tasks across the organization.





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts



# Executive summary

## Sub-contractor risk

Despite the continued investment and renewed focus on EERM, respondent organizations were found to be lacking appropriate visibility of instances where sub-contractors are engaged by their third-parties. This is making it difficult for organizations to determine their strategy and approach to the management of sub-contractor risk and to apply the appropriate amount of discipline and rigor. Recent regulation such as the Modern Slavery Act in the UK and Global Data Protection Regulations (GDPR) in Europe, which include requirements to manage layers of fourth/fifth parties, where they exist, makes this a matter of increased concern. Other global regulators such as the Federal Reserve (Fed) and Office of the Comptroller of the Currency (OCC) in the US, and the Hong Kong Monetary Authority, etc. also highlight the need for organizations to understand this area better.

Organizations **lack visibility of sub-contractors engaged by their third-parties** making it challenging to apply an appropriate strategy to monitor such fourth/fifth parties.

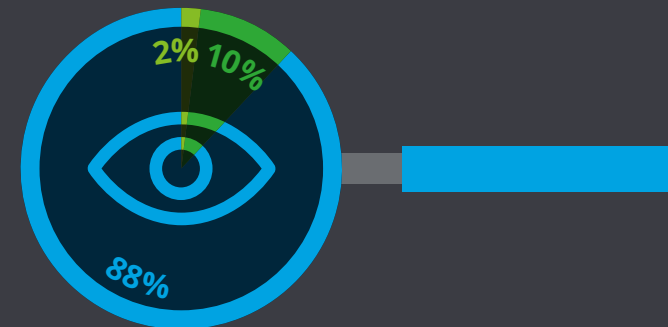
**57 percent** of survey respondents feel they do not have adequate knowledge and appropriate visibility of sub-contractors engaged by their third-parties and a further **21 percent** are unsure on their organization's level of understanding.



Only **18 percent** of organizations periodically review the concentration risk associated with their fourth/fifth parties quarterly or half-yearly; while the vast majority (**82 percent**) review this annually or even less frequently.



Only **two percent** of respondents regularly identify and monitor their sub-contractors (fourth/fifth parties) while another **10 percent** do so only for those subcontractors identified as critical. The other **88 percent** either rely on their third-parties to do so; have an unstructured/ad-hoc approach; do not do so at all; or do not even know their organizational policy and practices in this regard.





-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  02 Business case and investment
-  03 Centralized control
-  04 Technology platforms
-  05 Sub-contractor risk
-  06 Organizational imperatives and accountability
-  About the authors
-  Contacts



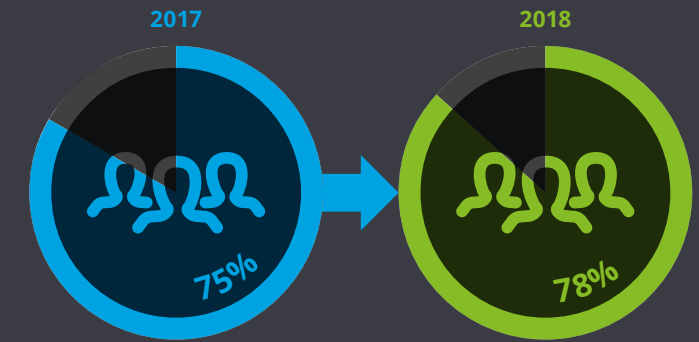
# Executive summary

## Organizational imperatives and accountability

Ownership and accountability for EERM suggests it is well and truly established in the C-suite with **78 percent** of organizations suggesting that either the Chief Executive Officer (CEO), CFO, Chief Procurement Officer (CPO), CRO, or a member of the Board is ultimately accountable for this topic. **33 percent** suggested the CEO or CFO was responsible for EERM. In some cases, there appears to be a small shift in ultimate accountability from CPOs and Vendor/Alliance Managers to Heads of Risk and CFOs under Board/CEO supervision, although this is not a trend where the organizational supply-chain forms the most significant component of the extended enterprise. In such organizations which still form the majority, the CoEs and shared services are also largely owned by procurement teams. Survey respondents however believe that there is room for improvement in the level of engagement on the EERM agenda by Board members and risk domain owners.

Ownership and accountability for EERM suggests **it is well and truly established in the C-suite** with some need for improvement in levels of engagement.

Either the CEO, CFO, CPO, CRO, or a member of the Board is ultimately accountable for EERM in **78 percent** of organizations, up from **75 percent** last year.



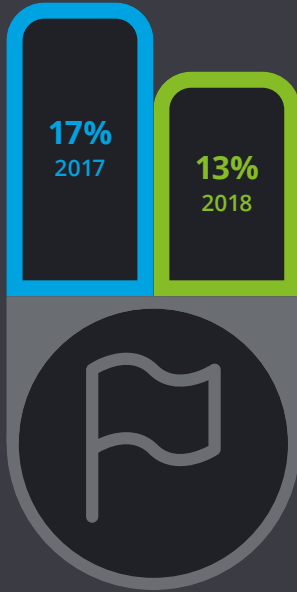
The CEO or CFO is now accountable for EERM in **33 percent** of organizations, up from **29 percent** last year.



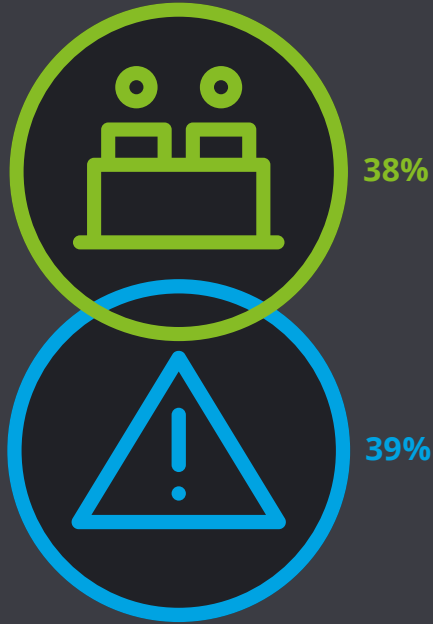


- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts

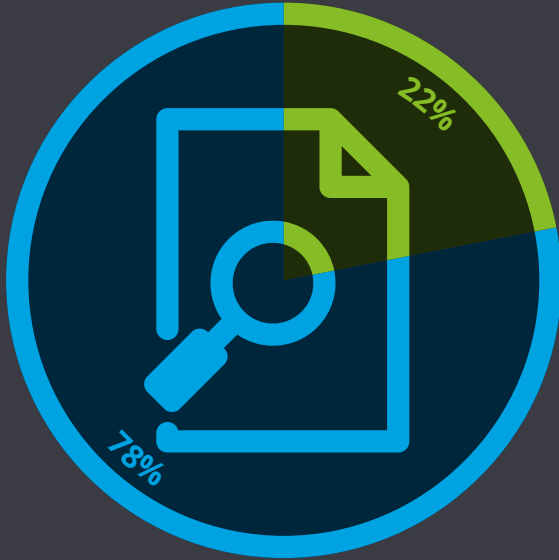
Ownership for EERM vested in CPOs and Vendor/Alliance Managers has reduced from **17 percent** last year to **13 percent** this year with a corresponding increase in such responsibility vested in the CFO and CRO by three percent in each case.



However, our survey results indicate that **38 percent** of Board members and **39 percent** of risk domain owners still have lower to insignificant levels of engagement on the EERM agenda.



Only **22 percent** of respondent organizations have Board-level reviews of EERM that include alignment with organizational strategy and risk appetite on a quarterly or half yearly basis, while the vast majority of organizations surveyed (**78 percent**) review this annually or even less frequently.







Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts

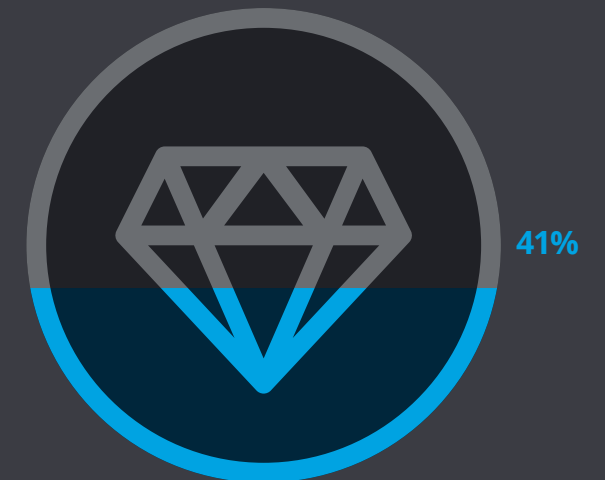
Our prior surveys had identified an “Execution Gap” in implementing EERM in organizations, reflecting the inability of people, process, and technology supporting EERM initiatives to achieve the intended results. With the emergence of a standardized three-tier technology architecture as described earlier in this executive summary, this execution gap around technology seems to have started to narrow down, although the gap remains as wide as in earlier years on the people and process front.

Internal coordination (specifically between risk domain owners, business unit leaders, functional heads, legal, and internal audit teams) is now the dominant concern of the majority of organizations, followed by the need to ensure ongoing relevance of skills, roles and responsibilities, being realistic about availability of staff bandwidth.

In summary, concerns over coordination, talent, and processes have now overshadowed the technology-related concerns expressed in earlier surveys.

Concerns over **internal coordination, talent, and processes** have now overshadowed the technology-related concerns expressed in earlier surveys.

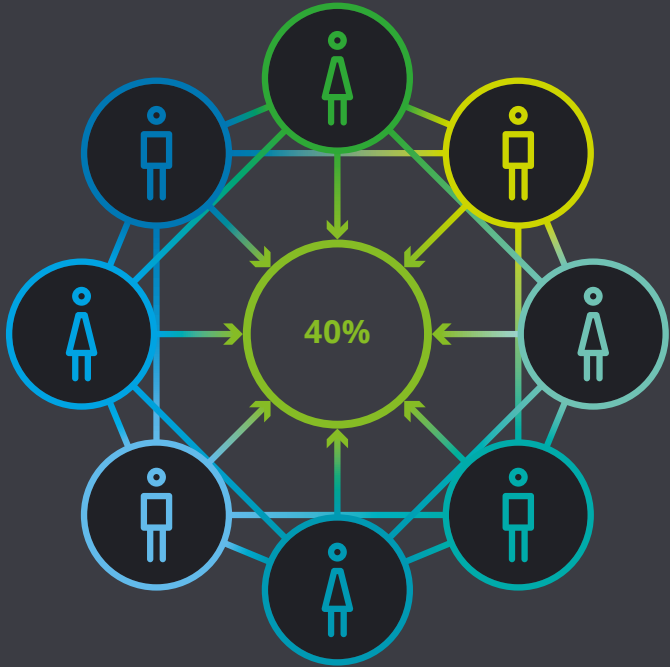
Skills, bandwidth, and competence of talent engaged in EERM-related activities appears to be the most significant concern for respondents (**45 percent**), followed by the clarity of roles and responsibilities and EERM processes (**41 percent** in either case).



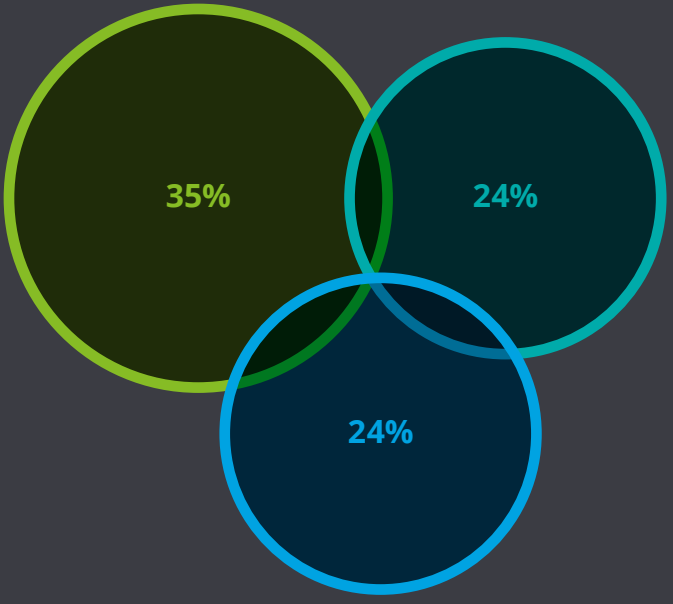


- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts

As many as **40 percent** of respondent organizations have prioritized the need to establish better coordination between risk domain owners, business unit leaders, functional heads, legal, and internal audit teams as their top organizational imperative related to EERM.



Strengthening due diligence activities prior to on boarding new third-parties is second on the list of top organizational imperatives related to EERM (**35 percent** of respondent organizations); followed by building stronger resilience to disruption caused by third-party related incidents (**24 percent**) and categorizing the most strategic third-parties to ensure a proportionate EERM approach (**24 percent**).





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts

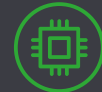


# Executive summary

## Predictions



We believe that the investments made in EERM in 2017 will begin to pay dividends in either 2018 or 2019—in line with respondents’ realistic assessment that it takes two to three years for organizations to be integrated or optimized in EERM.



Technology will continue to play a significant role in driving efficiency—although this may not be associated with big in house implementations but rather leveraging managed service technology platforms. As a first step in this direction, less than **10 percent** of respondents are currently using bespoke systems for EERM, a sharp drop from just over **20 percent** last year and a standardized three-tier technology architecture comprising (i) ERP and other backbone procurement system; (ii) GRC or EERM package; and (iii) other niche EERM solutions for specific needs have already become the norm.



We have already seen 2017 suggest that community models/market utilities will be adopted across a number of industries with FS leading the way since 2016 with the emergence of four key players. Expected industries to follow suit include LSHC (increase in actual utilization from **16 percent** to **24 percent** during 2017), CB (e.g. FMCG) (**11 percent** to **18 percent**), and TMT (**12 percent** to **27 percent**). E&R (**28 percent** to **33 percent**), while the leading industry segment in exploring market utilities, has some way to go to fully embrace the opportunities here through extensive usage (with only two percent of the latter **33 percent** using such models extensively but the vast majority represented by the other **31 percent** making only limited use). But already we have seen movement in this space at the back end of 2017.



The focus on people described in the section on organizational priorities above is driving a boom in the market for EERM talent. In turn, the current scarcity of this talent is driving competition and in turn may further assist in building the business case and trend for community models, utilities, and managed services.



We anticipate 2018 will see more design/ implementation of frameworks (Capex) through either continuing design work or further refining frameworks, but expect by 2020 that most EERM expenditure will be in the operational (Opex) space—where the use of community models will further drive costs down. Interestingly, survey respondents did not specifically distinguish between Capex and Opex in reporting their estimated annual spend centrally.



Recent regulation such as the Modern Slavery Act in the UK and Global Data Protection Regulations (GDPR) in Europe, which include requirements to manage layers of fourth/fifth parties (where applicable), is likely to make the need for additional investment in the management of fourth/fifth parties a matter requiring further attention.



Finally, EERM now has a more balanced outlook in establishing the business case for investment in EERM initiatives. On the one hand, it continues to mitigate the threats of “bad things happening” or the downside of risk, for instance the operational impact of critical third-party failures or the reputational impact of bribery and corruption by third-parties to large global organizations. On the other hand, however, such balanced business cases are enabling calculated risk-taking aligned to the realization of strategic opportunities such as innovation and positive cost-reduction across the entire organization to capture the upside opportunity. However the critical success factors for achieving this will be measured not only on how cost efficient or effective the frameworks are designed or operated, but primarily on how well risk is managed and mitigated with a continuous process of alignment with strategy and organizational risk appetite. Should organizations lose this strategic insight and reduce their annual investments in EERM, this is likely to be at the expense of reputation, regulatory scrutiny, and ultimately consumer backlash.



Home



Foreword



Executive summary



**01** Inherent risk and maturity



**02** Business case and investment



**03** Centralized control



**04** Technology platforms



**05** Sub-contractor risk



**06** Organizational imperatives and accountability



About the authors



Contacts

# 1. Inherent risk and maturity

Organizational self assessment of overall levels of EERM maturity continues to improve at a slower pace despite a perceived increase in the inherent risks in third-party dependence.





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts



1. Organizational self assessment of overall levels of EERM maturity continues to improve at a slower pace despite a perceived increase in the inherent risks in third-party dependence.

**53 percent** of respondents now believe that their journey to achieve the desired state of EERM maturity is two to three years or more, as against most respondents in earlier surveys being overly optimistic in believing that this can be achieved in six months to a year.



53%



**Key messages**

Our earlier surveys demonstrated how a renewed set of drivers, directly aligned to long-term value-creation (e.g., business agility, access to specialized skills and knowledge, innovation, and process improvement) in addition to cost-savings, were beginning to motivate organizations to increase dependence on third-parties forming the extended enterprise. The current survey indicates that this strategic dependence on third-parties continues to increase with **41 percent** of respondents reporting “some” increase in their level of dependence on third-parties in the last year (no change from our last survey) and a further **11 percent** reporting a “significant” increase in such dependence (**10 percent** in our last survey).

High or even critical levels of dependence on third-parties, together with the increasing frequency of significant third-party incidents<sup>7</sup> with various adverse consequences and regulatory intervention, had increased board-level awareness on EERM, making them consider investing in holistic and integrated programs to manage extended enterprise risks. Following a brief slowdown in 2016, organizations now seem to be returning back to tackle the topic with renewed focus and investment. This has taken place amid a perception by respondents that the inherent risk of dependence on third-parties has increased. This increased perception of inherent risk has been caused by continuing uncertainty in the business and macro-economic environment; concerns around emerging regulation and regulatory scrutiny; and threats of third-party related incidents/disruption. However in a year where many organizations stated that they were going to make

significant progress, the aggregate results suggests there is still work to do to move from managed to integrated or optimized in the maturity scale.

Even with the growing levels of high or critical levels of dependence on third-parties, only **20 percent** have integrated or optimized their EERM mechanisms (same proportion as last year), with another **50 percent**, currently in managed status, aspiring to achieve integrated or optimized status within the next one to three years.

Respondents recognize that these current levels of integration or optimization are far below aspirational levels. There are therefore aspirations to further integrate and optimize the related risk management mechanisms. **52 percent** of respondents now believe that their journey to achieve the desired state of EERM maturity is two to three years or more, as against most respondents in earlier surveys being overly optimistic in believing that this can be achieved in six months to a year.

It was interesting to note that some respondents had lowered their earlier self-assessments of maturity. This seems to reflect their deeper appreciation of the situation and a stronger understanding of third-party related issues than in the past.

As a result, many respondent organizations have indicated, through qualitative comments that they are still not managing the risks that third-parties present to them in a holistic and coordinated manner and this position has only slightly changed since last year.



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability

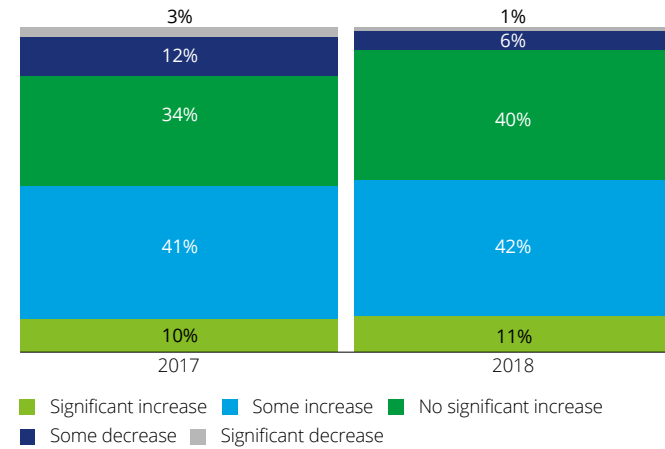


About the authors

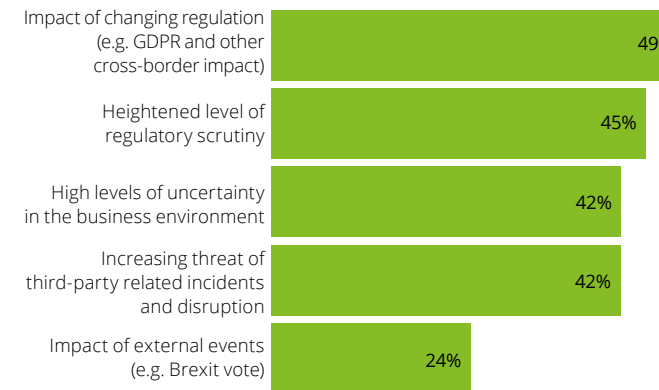


Contacts

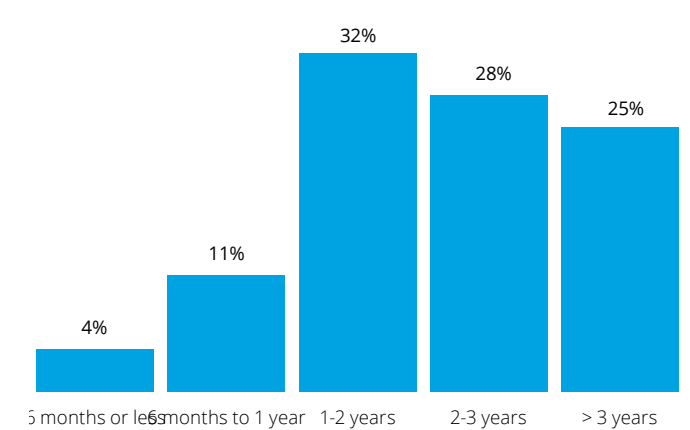
### Change in level of dependence on extended enterprise over the last year



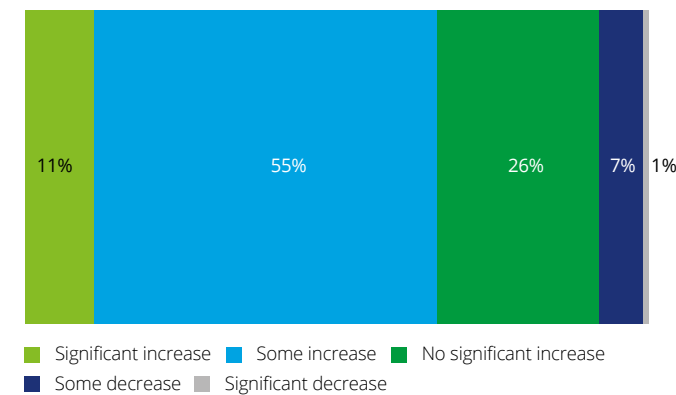
### Greatest contributory factors in the perception of heightened inherent risk related to the extended enterprise



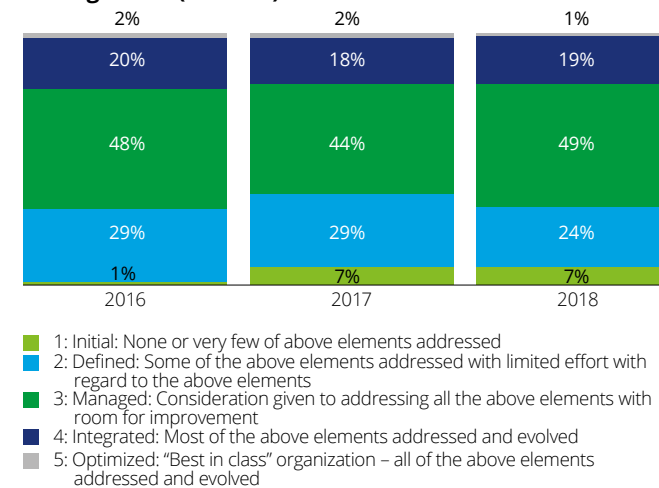
### Time taken by organizations to achieve the desired level of EERM optimization



### Change in the level of risk inherent in managing the extended enterprise over the last year



### Change in level of maturity in approaching third-party risk management (2016-18)



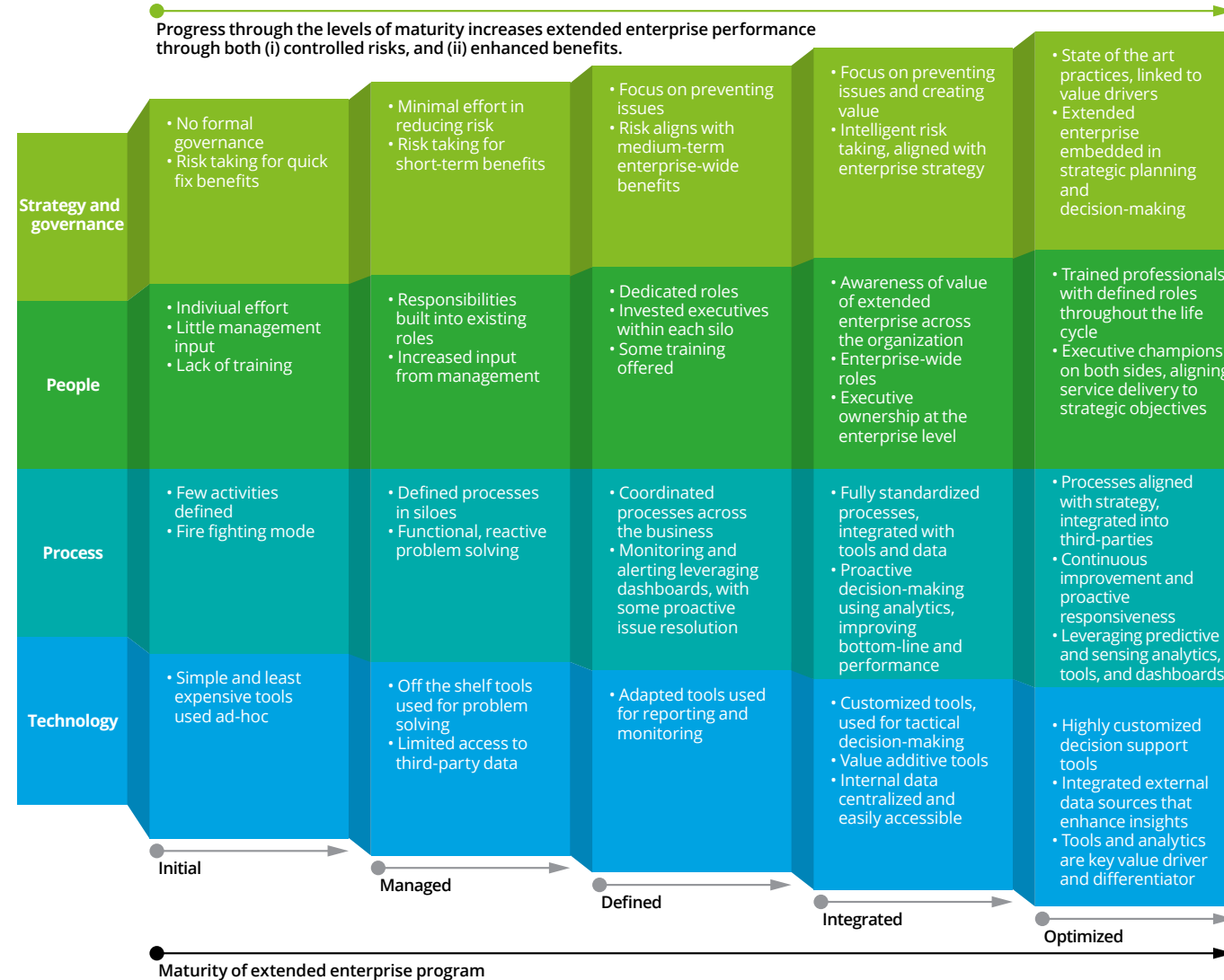




- 🏠 Home
- 💬 Foreword
- 📄 Executive summary
- 📈 01 Inherent risk and maturity
- 💰 02 Business case and investment
- 🔗 03 Centralized control
- 🔧 04 Technology platforms
- 🏢 05 Sub-contractor risk
- 📄 06 Organizational imperatives and accountability
- 👤 About the authors
- 👤 Contacts

**Deloitte EERM Maturity Model**

Progress through the levels of maturity increases extended enterprise performance through both (i) controlled risks, and (ii) enhanced benefits.



**Deloitte point of view**

Due to changes in the business and macro-economic environment (including regulatory pressure), each organization will need to establish what it considers to be its desired optimum state for EERM, making it a moving target, and many organizations are continuing “catch-up” with the emerging set of strategic opportunities and related risks that third-parties continue to present.

This includes:

- A broader set of support services delivered innovatively in a rapidly-changing external environment.
- A growing number of alliance and joint venture partners and an increasing proportion of third-parties in newer areas beyond the traditional focus on the direct supply chain (suppliers and vendors).
- The increasing use of new technology (such as the cloud and cloud-based applications) that facilitate collaboration and enable businesses to enhance their virtual boundaries will further accelerate this trend.

It should also be noted that as good practice continues to evolve, the related goalposts are shifting too; hence in reality those that stand still are actually sliding backwards on the maturity curve.



Home

Foreword

Executive summary

**01** Inherent risk and maturity

02 Business case and investment

03 Centralized control

04 Technology platforms

05 Sub-contractor risk

06 Organizational imperatives and accountability

About the authors

Contacts



### Industry highlights

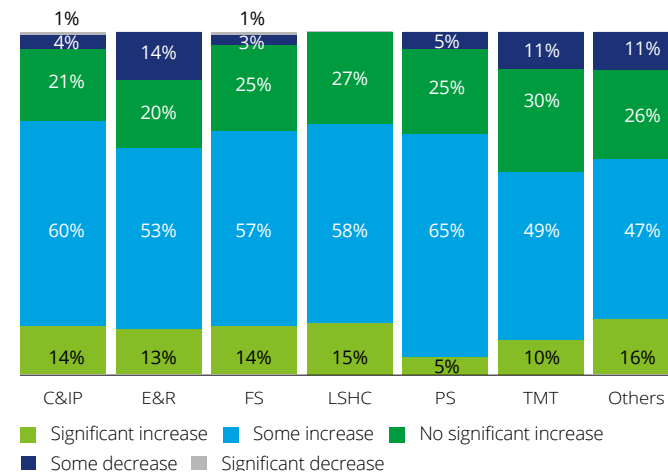
- Respondents from all industry segments, without exception, have reported the heightened perception of risks inherent in third-parties with the highest perceived increase (some or significant) reported by **74 percent** of C&IP respondents, **73 percent** of LSHC respondents and **71 percent** of FS respondents.

- However, this heightened perception of inherent risks does not appear to have deterred organizations from continuing to increase their levels of dependence on third-parties. The most notable increases in the level of dependence on the extended enterprise have taken place in the FS industry segment with **59 percent** of respondents reporting some or significant increase over the last year, followed by LSHC (**58 percent**), C&IP (**55 percent**), TMT (**52 percent**), and E&R (**52 percent**). Even in the industry segment with the lowest increase in the level of dependence on third-parties, i.e. PS, more than **45 percent** respondents said that they continued to increase their third-party dependence.

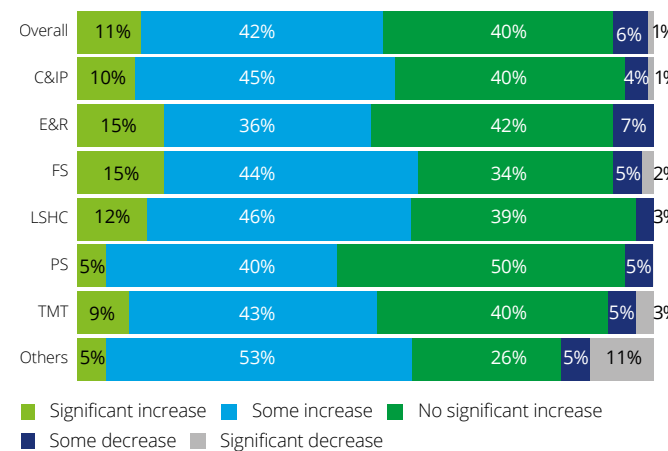
Against this backdrop, the industry segments that made the biggest improvement in integrating or optimizing their EERM processes and technology were LSHC (**eight percent** integrated/optimized last year to **24 percent** in the current survey), C&IP (**11 percent** to **19 percent**), and PS (**20 percent** to **35 percent**).

- PS has the largest majority of organizations that believe they have the longest journey to achieve desired state in EERM with **75 percent** of respondents believing this to be at least two to three years or more, followed by FS (**57 percent** of respondents) and LSHC (**54 percent**). TMT is the last one on this list; however even in this industry segment, as many as **49 percent** of respondents believe this journey is at least two to three years or more.

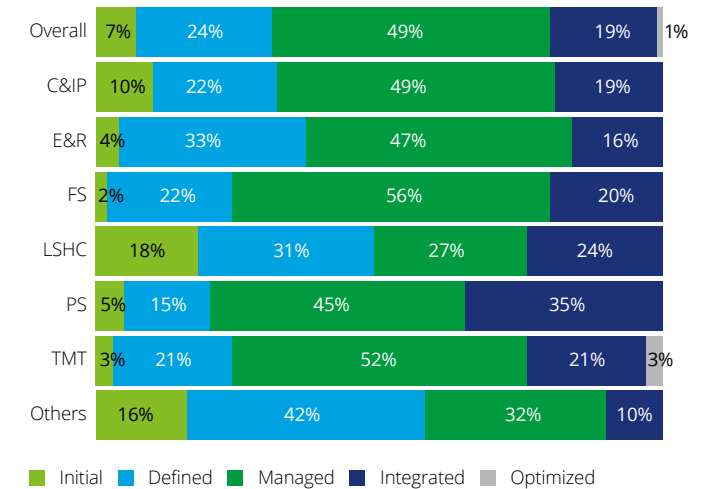
### Change in level of risk inherent in managing the extended enterprise by industry



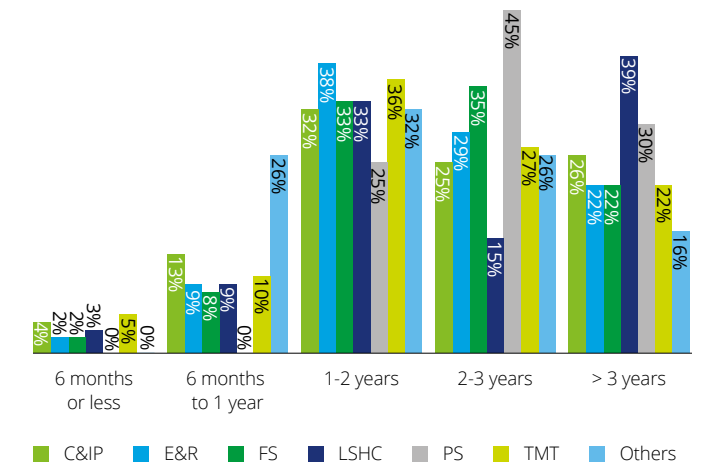
### Change in level of dependence on extended enterprise over the last year by industry



### Level of maturity in EERM by industry



### Time taken by organizations to achieve the desired level of EERM optimization by industry





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts

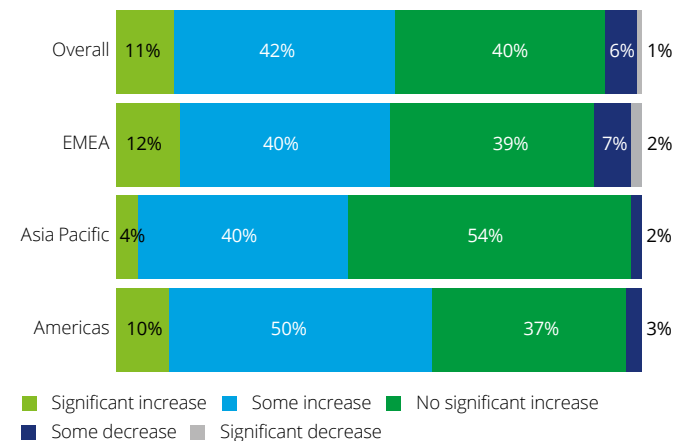


### Geography highlights

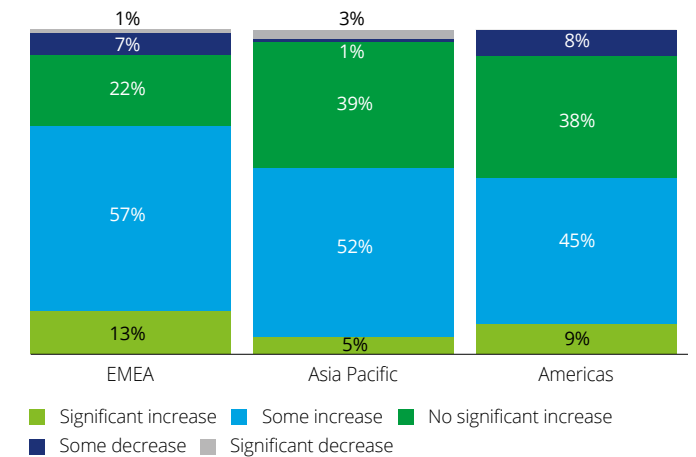
- The Americas region has traditionally had the highest level of dependence on third-parties followed by EMEA and Asia Pacific respectively. Increase in the level of such dependence over the last year in these regions has taken place in the same relative proportion with **60 percent** respondents in Americas reporting some or substantial increase, compared to EMEA with **52 percent** and Asia Pacific with **44 percent**.
- Even with the highest levels of dependence on the extended enterprise in the Americas, the perception of inherent risks increasing is relatively the lowest, albeit with **54 percent** of respondents from that region perceiving some or substantial increase in risks related to third-parties (as against **70 percent** in EMEA and **57 percent** in Asia Pacific).
- The proportion of respondents with integrated and optimized EERM mechanisms is also the highest in the Americas (**29 percent**) followed by EMEA (**19 percent**) and Asia Pacific (**15 percent**).
- Asia Pacific have seen some increase in EERM maturity with **15 percent** of respondent organizations now having integrated their EERM systems as against **11 percent** last year. However the EMEA region have seen little increase (unchanged at **19 percent** since last year).

- The Americas region has comparatively the (a) highest level of dependence on third-parties; (b) the lowest perception of inherent risk among respondents; and (c) the highest proportion of organizations with integrated or optimized levels of EERM maturity. As a result, this region is likely to see even more dependence being placed on the extended enterprise with a stronger business case for investment in EERM initiatives going forward. On the other hand, the impact of macro-economic factors and uncertainty in EMEA, such as the outcome of the Brexit vote results have clearly increased the perception of inherent risks and slowed down investment in EERM initiatives, thus slowing down the increasing level of dependence. Organizations from the Asia Pacific region continue to catch-up with their other global counterparts in extending the enterprise, given their propensity to traditionally be more of outsourcing providers rather than clients or customers<sup>8</sup>.

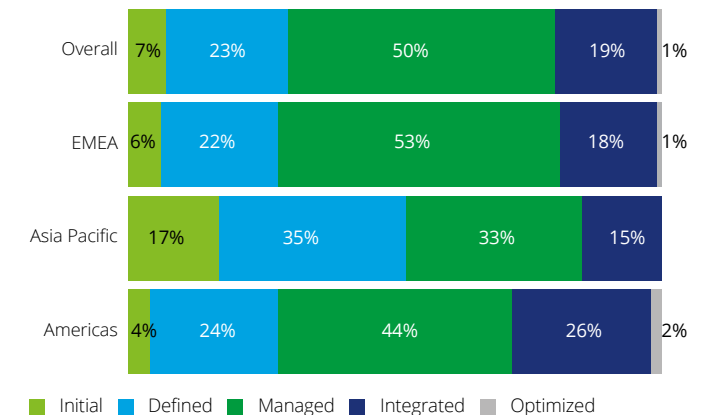
Level of dependence on extended enterprise in the last year by region



Change in inherent risk levels related to third-party dependence over the last year by region



Current level of maturity in EERM by region





 Home

 Foreword

 Executive summary

 01 Inherent risk and maturity

 **02 Business case and investment**

 03 Centralized control

 04 Technology platforms

 05 Sub-contractor risk

 06 Organizational imperatives and accountability

 About the authors

 Contacts

# 2. Business case and investment

The business case for investment in EERM is increasingly being focused on exploiting the upside of risk—a significant shift from the focus in prior surveys on managing the downside, with increasing confidence to demonstrate tangible benefits.



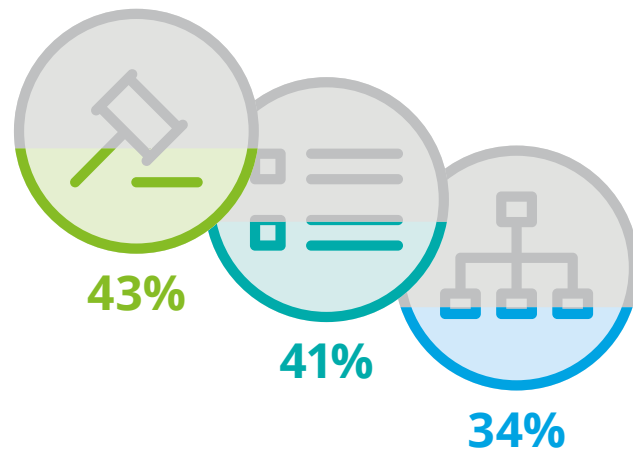


-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  **02 Business case and investment**
-  03 Centralized control
-  04 Technology platforms
-  05 Sub-contractor risk
-  06 Organizational imperatives and accountability
-  About the authors
-  Contacts



2. The business case for investment in EERM is increasingly being focused on exploiting the upside of risk—a significant shift from the focus in prior surveys on managing the downside, with increasing confidence to demonstrate tangible benefits.

Reduction of regulatory exposure (**43 percent** of respondents); addressing internal compliance requirements (**41 percent** of respondents); and reducing the number of third-party related incidents (**34 percent** of respondents) were the strongest business case drivers focused on managing the downside of extended enterprise risk.



**Key messages**

Comments made by a number of participants in our earlier surveys had identified a common angst in their inability to objectively establish the business case for investment in EERM in their organizations, given their lack of knowledge and understanding of key business drivers influencing similar articulations of business case in their peer group of organizations. Participants had also indicated that they lacked the availability of relevant data around total investment in EERM, both in monetary terms as well as in terms of headcount of full-time staff involved in EERM-related activities. Our 2018 survey aimed to address these knowledge gaps, as well as capture the level of confidence of respondents in being able to achieve tangible benefits as compared to their articulated business case.

Survey results indicate that the drivers for the focus on EERM continued to be regulatory requirements, for example GDPR in Europe (**43 percent** of respondents); addressing internal compliance standards (**41 percent** of respondents); or concern around third-party related incidents (**34 percent** of respondents); but the need for positive cost reduction across the business was equally (if not more) powerful (**48 percent** of respondents) in organizations which they felt this could be achieved by bringing in efficiencies through the use of third-parties or by preventing over-payments. This represents an emerging trend that we have not seen in prior surveys.

It is also heartening to see that business case for investment in EERM is increasingly being driven by other factors that exploit the upside of risk, such as enhancing organizational responsiveness and flexibility, innovation, brand confidence, and increasing revenues.

**26 percent** of respondents felt that they could achieve greater flexibility to address market uncertainty and **20 percent** considered investment in EERM a revenue-generating opportunity, for instance by identifying under-reported revenue streams. This represents another significant shift from the almost-exclusive focus earlier on managing the downside (such as regulatory exposure or third-party related incidents).

The majority of respondents (**62 percent**) had some or significant confidence in their ability to demonstrate at least some tangible benefits, if not significant returns from such investment, supported by the use of performance measures (see examples set out in the table on page 26).

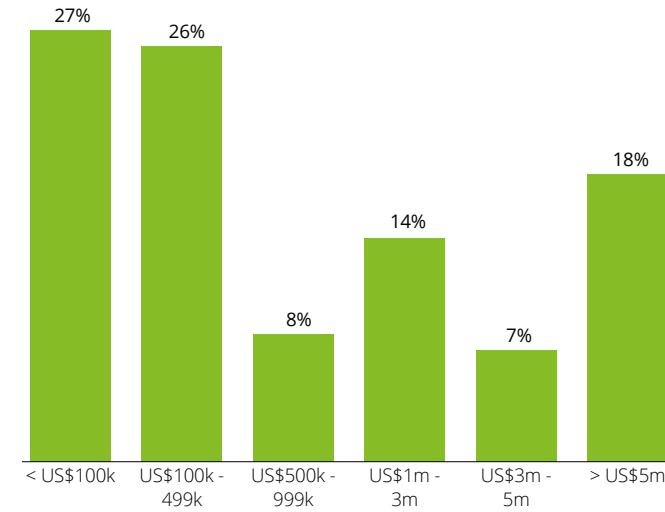


- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts

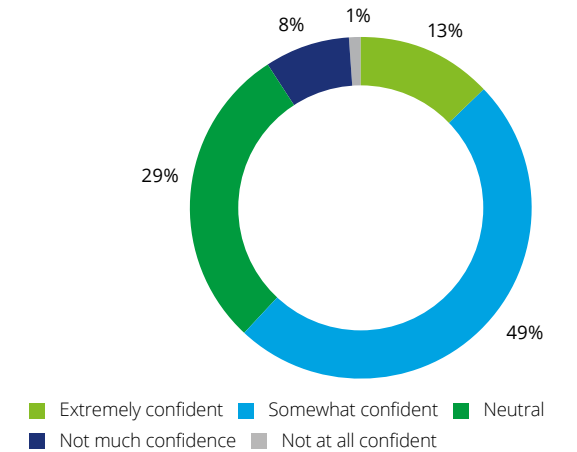
### Key factors driving business case for investment in EERM



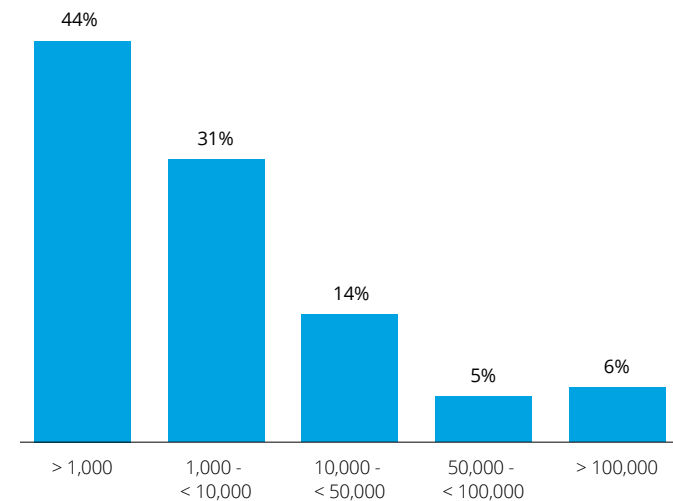
### EERM investment levels per year (estimated spend)



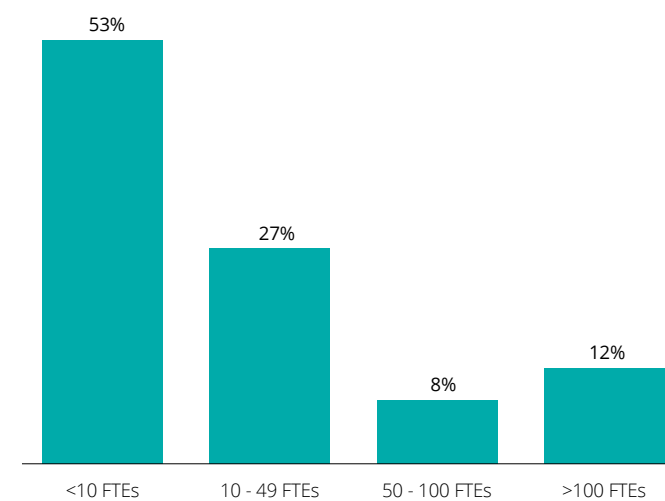
### Confidence in demonstrating realization of tangible benefits related to their organizations' business case for investment in EERM



### Number of third-parties engaged by organizations



### Number of full-time equivalent (FTE) staff involved in EERM















-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  02 Business case and investment
-  03 Centralized control
-  04 Technology platforms
-  05 Sub-contractor risk
-  06 Organizational imperatives and accountability
-  About the authors
-  Contacts

**Examples of tangible performance measures used by respondents to monitor business case realization**

Business case driver	Tangible performance measures
 <b>Cost reduction</b>	<ul style="list-style-type: none"> <li>Reducing five percent of total procurement spend through efficiencies in managing third-party suppliers.</li> <li>Zero tolerance on duplicate payments to suppliers and third-parties.</li> <li>A maximum of two percent overpayment on invoices not matching orders (tolerance level).</li> <li>Reduction of insurance premium by eight percent compared to previous year from better movement of goods between third-party locations.</li> </ul>
 <b>Increase in revenue</b>	<ul style="list-style-type: none"> <li>10 percent increase in revenue from newer geographies enabled by third-party alliances and partnerships.</li> <li>At least one new product offering in the financial year contributing to one percent of total revenues introduced using third-party expertise.</li> </ul>
 <b>Reduction in number of third-party related incidents</b>	<ul style="list-style-type: none"> <li>Zero incidence of third-party related disruptions that cannot be addressed in 24 hours or with financial implications greater than US\$1 million.</li> <li>100 percent third-party adherence to organizational standards.</li> </ul>
 <b>Reduction in regulatory exposure</b>	<ul style="list-style-type: none"> <li>Zero tolerance to regulatory breach.</li> <li>No regulatory fines or penalties.</li> </ul>
 <b>Addressing internal compliance requirements</b>	<ul style="list-style-type: none"> <li>100 percent compliance with HSE standards.</li> <li>Zero deviation from internal policies and processes unless covered by specific exemptions.</li> </ul>
 <b>Better response and increased flexibility to market uncertainty</b>	<ul style="list-style-type: none"> <li>25 percent flexibility in distribution capacity based on third-party arrangements to address market uncertainty.</li> <li>Improvement in customer ratings on increased customer flexibility over previous year.</li> </ul>
 <b>Unlock access to innovative/disruptive technology solutions</b>	<ul style="list-style-type: none"> <li>At least one out of 10 of new third-party arrangements in the financial year focused on bringing new strategic opportunities or have access to new technology.</li> <li>10 percent increase in automation through technology solutions for risk management year on year (measured through surveys of risk management team members).</li> </ul>
 <b>Increase in confidence in the organizational brand</b>	<ul style="list-style-type: none"> <li>Increase in share price by five percent year on year.</li> </ul>



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts



### Deloitte point of view

Risk management has long been associated with mitigating adverse financial consequences of “bad things happening,” which has historically positioned governance-related activities to avoid or mitigate risk.

Survey results reflect the transformation that respondent organizations are now going through with a renewed focus to recognize that good governance and risk management around their extended enterprise is not about eliminating risk, but rather managing it appropriately.

While risk mitigation (value preservation) will continue to remain a driver for investment in EERM, organizations are now increasingly starting to see the exploitation of the opportunity (value creation) as a driver for investment in EERM. Governance, a higher level process involving directing and managing risk management and related activities to address stakeholder expectations, is therefore finally starting to reinvent itself to focus on maximizing this opportunity, while also managing compliance requirements and the downside of risk. However, in this new thinking, the explicit linkage of risk and strategy, starting at the Board and C-suite level must be an integral part of the organizational strategy-setting process.

With EERM now having a more balanced outlook of addressing the downside of risk as well as capturing the upside opportunity, the related annual spend seems to have significantly increased. For instance, organizations that are *integrated or optimized* in managing their extended enterprise are now typically investing over US\$3 million annually on EERM initiatives, managed by more than 50 FTEs. Organizations that engage 50,000 or more third-parties in their extended enterprise are now typically investing over US\$5 million annually on EERM initiatives, managed by more than 100 FTEs.

However, ongoing success in being able to achieve this balance should be measured not only on how cost efficiently EERM frameworks are designed or operated, but primarily on how well risk is managed and mitigated with a continuous process of alignment with strategy and organizational risk appetite. Should organizations lose this strategic insight and reduce their annual investments in EERM, then that cost is likely to come at the expense of reputation, regulatory scrutiny, and ultimately consumer backlash.



### Industry highlights

While organizations across industry segments appear to be motivated by similar drivers of business case for investment in EERM, certain industry segments stand out:

- FS appears to be the most motivated by positive cost reduction in its overall spend on third-parties with **52 percent** respondents, closely followed by C&IP (**48 percent**) and E&R (**44 percent**).
- Several business cases for investment in EERM in the TMT sector (**49 percent**) appear to be driven by their ability to increase revenue, for instance by identifying unreported or under-reported revenue streams by third-parties, although this is a significantly less important driver in the other segments.
- For LSHC and E&R, the strongest drivers for EERM initiatives appears to be reducing the number of third-party related incidents (**46 percent** and **40 percent** of respondents, respectively). Similarly, reduction in regulatory exposure is a related driver in these two industry segments with **46 percent** and **58 percent** of respondents, as well as in FS (**48 percent** of respondents) while respondents from LSHC and PS are most concerned with meeting internal compliance requirements (**52 percent** and **50 percent** of respondents respectively).
- Among the new and emerging drivers for investment in EERM, the ability to achieve greater agility and flexibility in the marketplace seems to be most popular with one in three respondents from the E&R and LSHC industry segments, around one in four respondents from FS, TMT, and C&IP and one in five respondents from PS.



Home

Foreword

Executive summary

01 Inherent risk and maturity

02 Business case and investment

03 Centralized control

04 Technology platforms

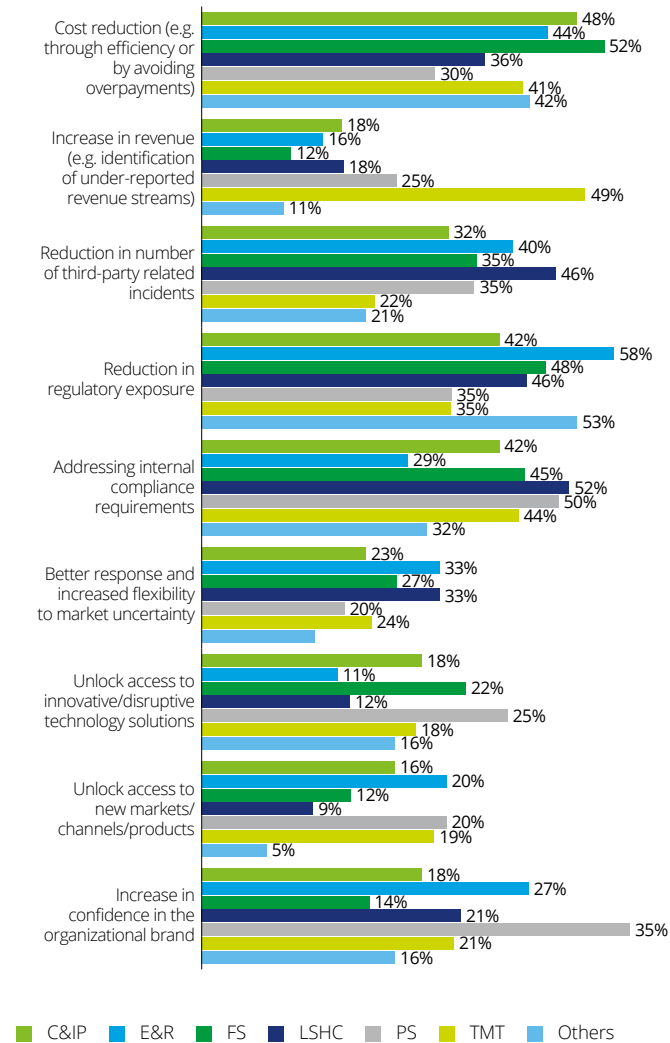
05 Sub-contractor risk

06 Organizational imperatives and accountability

About the authors

Contacts

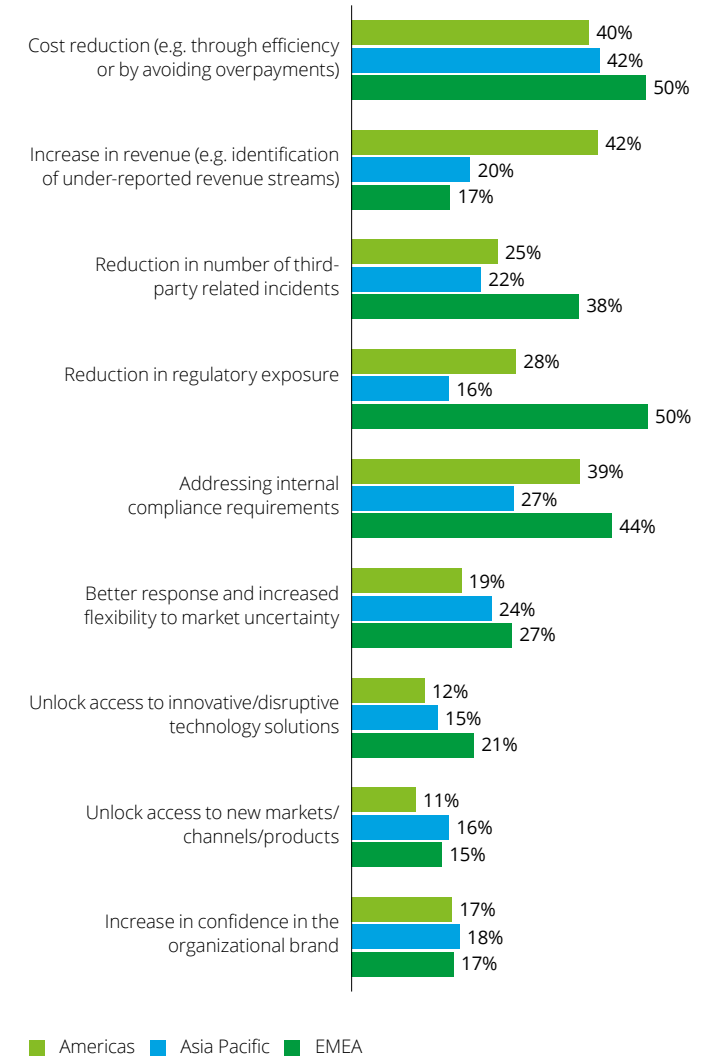
### Key factors driving business case for investment in EERM by industry



### Geography highlights

- The need to achieve positive cost reduction in total organizational spend on third-parties in the extended enterprise, either by bringing in efficiencies or by preventing over-payments, is the most common driver for business case for investing in EERM across all the three regions. However, this is relatively the most dominant driver in EMEA with **50 percent** of respondents, followed by Asia Pacific (**42 percent**) and Americas (**40 percent**).
- Respondents from the Americas are much more driven by the opportunity to increase revenue, for instance by the identification of unreported or under-reported revenue streams (**42 percent** of respondents) in comparison to other regions such as Asia Pacific (**20 percent** of respondents) and EMEA (**17 percent** of respondents).
- In terms of emerging drivers, EMEA is relatively more focused on unlocking opportunities for innovation through third-parties (**21 percent** of respondents) while Asia Pacific is more focused on gaining access to new markets, channels, and products (**16 percent** of respondents). All the three regions are almost equally focused on increasing the confidence in their organizational brand through third-parties (**17-18 percent** of respondents).
- Respondents from the Americas are the most confident about demonstrating the realization of tangible benefits related to their organizational business case for investment in EERM with **20 percent** extremely confident and another **48 percent** somewhat confident. However, EMEA respondents are not far behind in this regard with **12 percent** extremely confident and another **52 percent** somewhat confident. However, Asia Pacific is less confident with **seven percent** and **37 percent** respondents in each of these categories respectively.

### Key factors driving business case for investment in EERM by region





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability

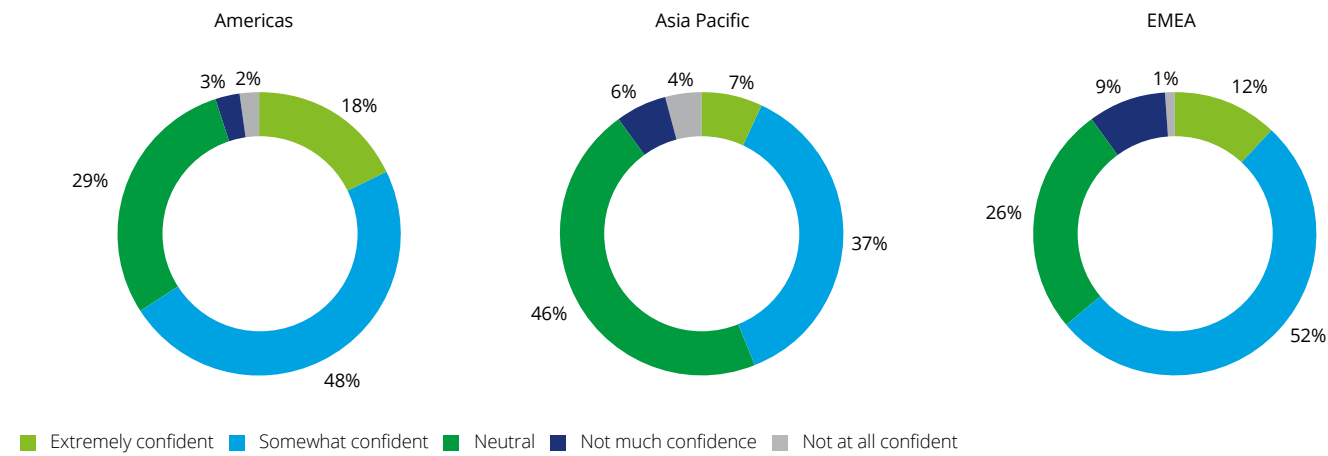


About the authors



Contacts

**Confidence in demonstrating realization of tangible benefits related to their organizations' business case for investment in EERM by region**





 Home

 Foreword

 Executive summary

 01 Inherent risk and maturity

 02 Business case and investment

 03 Centralized control

 04 Technology platforms

 05 Sub-contractor risk

 06 Organizational imperatives and accountability

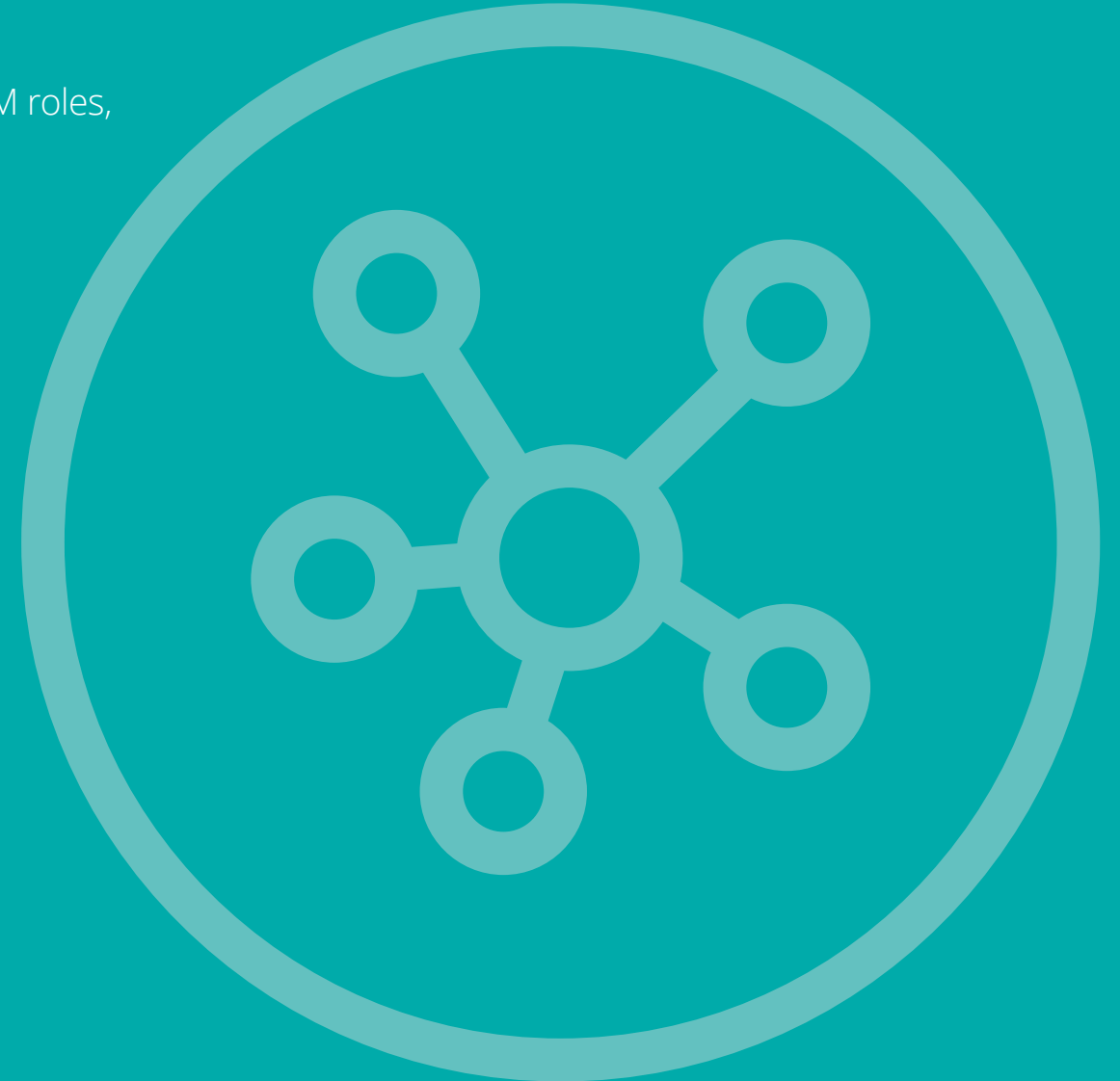
 About the authors

 Contacts

# 3. Centralized control

3a. Organizations are centralizing many elements of EERM roles, structures and technologies.

3b. COEs and shared service models represent the dominant operating model, along with an increased focus on market utility models.



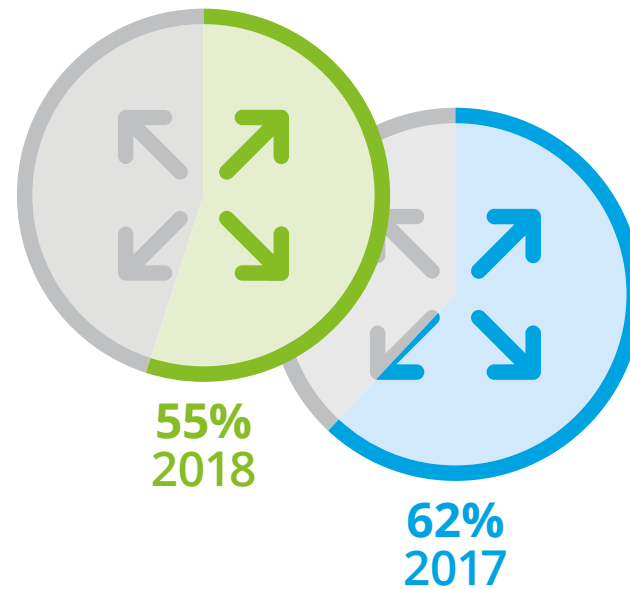


-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  02 Business case and investment
-  **03 Centralized control**
-  04 Technology platforms
-  05 Sub-contractor risk
-  06 Organizational imperatives and accountability
-  About the authors
-  Contacts



### 3a. Organizations are centralizing many elements of EERM roles, structures and technologies.

**55 percent** of organizations are now equally or more decentralized than centralized (down from **62 percent** last year).



#### Key messages

Decentralization in global organizations had been a common theme in our earlier surveys. Both prior surveys had reconfirmed that the majority of global organizations were equally or more decentralized than they were centralized (**75 percent** and **62 percent** of respondents from the 2016 and 2017 surveys respectively), across operating units/entities.

However, the increasing dominance of third-parties forming the extended enterprise in these decentralized operating units/entities presented potential concerns. Many respondents felt that a critical organization-wide matter such as EERM should not be left to the discretion of a divergent group of operational-level personnel and represented a potential challenge to a holistic and unified approach to third-party risk management, unless they scaled back on the degree of decentralization by introducing centralized ownership and management of the various elements in their EERM framework.

In line with this thinking, current survey results indicate that **55 percent** of organizations are now equally or more decentralized than they are centralized (down from **62 percent** last year), indicating a potential new trend of the diminishing dominance of decentralization in the overall organization.

Our 2016 whitepaper titled 'Addressing the challenges of decentralization' which focused on managing EERM in decentralized organizations had also suggested that an element of central oversight and management could help accelerate risk awareness and efficiency. The 2018 survey results show that more and more organizations are adopting this technique, resulting in the more decentralized EERM models being adapted with some component of central oversight. Accordingly, centralized elements in roles/structures and enabling technologies/processes are becoming more common-place.

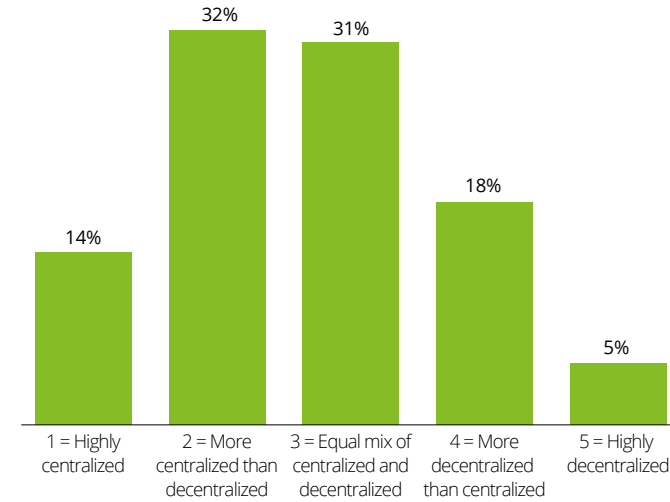
Out of the above **54 percent**, only **48 percent** of organizations now have EERM elements (roles/structures/technologies/processes) that are equally or more decentralized. The remaining 53 percent forms the current majority with more centralized EERM programs.



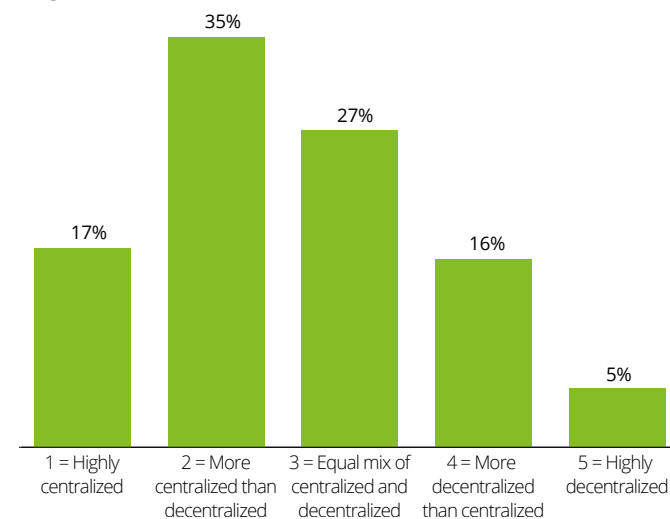


- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control**
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts

**Overall control structure**



**Organization structure for EERM**



**Deloitte point of view**

Deloitte experience indicates that global organizations have several choices in how they set themselves up from an EERM perspective to achieve the intended balance between centralized control and marketplace agility.

At one end of this scale of choices are organizations which operate through a greater degree of command and control with direct (referred to as “solid line”) reporting relationships with their operating units, fewer levels between the leaders in the corporate center and operating unit executives and formal task descriptions with authority specifications.

At the other end of this scale are those organizations that operate with decentralization following the “spirit” rather than the “letter of the law” with greater operational flexibility, taller organization structures between the corporate center and operating units and a combination of direct (solid line), indirect (referred to as “grey line”) and coordinating (referred to as “dotted line”) relationships with varying levels of clarity.

Irrespective of the degree of formality in decentralization, specific issues that must be addressed include the following:

- Establishing robust governance structures to manage third-party risk pervasively through the entire organization that flow down for decentralized business units to align to.
- Creating clear accountability on ownership of activities for EERM at the group level and across the decentralized business units.

- Creating awareness and engaging key stakeholders related to third-party risk at the group and local entity level.
- Allocating activity ownership around EERM to appropriately capable individuals at the group and local levels with decision-making authority.
- Implementing appropriate tools and technologies across centralized and decentralized operations, together with the availability of appropriate management information to facilitate the EERM framework.
- Articulating robust and achievable processes to manage third-party risk throughout the decentralized organization, integrating both group-wide and local requirements.
- Appropriately resourcing the governance structures, supported by the establishment of a common culture to facilitate communication and training to have a shared understanding of risk.

In general, the growing trend towards more centralized models for EERM appears to be a sensible way to proceed as there is much value (financial, efficiency, consistency, quality, etc.), to be gained from structuring a framework in this way. However, it should be noted that this is a general view and may not represent the most appropriate solution for all organizations.



- <
>
🏠 Home
- 💬 Foreword
- 📄 Executive summary
- 📈 01 Inherent risk and maturity
- 💰 02 Business case and investment
- 🌐 03 Centralized control
- 🔧 04 Technology platforms
- 🏢 05 Sub-contractor risk
- 📄 06 Organizational imperatives and accountability
- 👤 About the authors
- 👤 Contacts



### Industry highlights

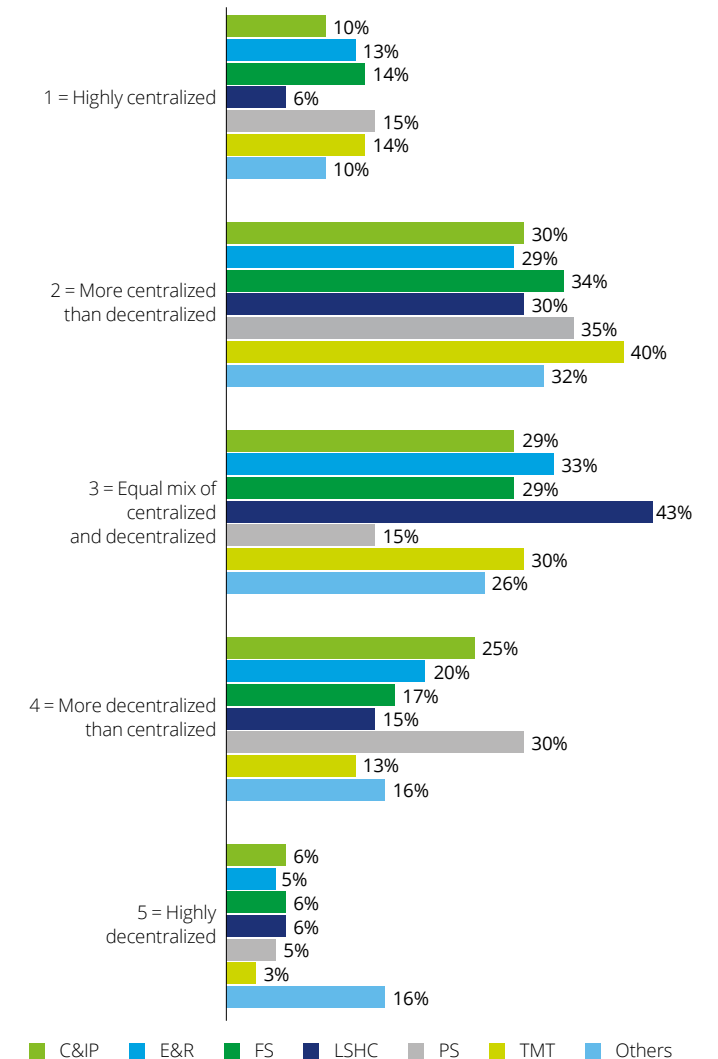
- The following diagrams to the right set out a comparative analysis across the major industry sectors between the overall control structure in organizations as compared to the organization structure for EERM from a decentralization perspective. As can be seen:

- LSHC and C&IP represent the two industry segments with the highest relative level of overall decentralization in their organizations, with **64 percent** and **60 percent** of respondents stating they are more equally or more decentralized than they are centralized.

However, only **45 percent** of respondents in both these segments felt that their EERM initiatives were more decentralized than centralized. This, in turn, implies that that the balance **18 percent** and **16 percent** respectively of respondent organizations have now incorporated various aspects of centralized ownership and management in their EERM frameworks.

- An unexpected trend emerged in responses from the FS industry where it was identified that while **53 percent** of respondents feel that the overall control structure in their organization is equally or more decentralized than centralized, a higher number of respondents (**56 percent**) feel that their EERM organization structures are equally or more decentralized, in contrast to the relationship between these metrics in other industry sectors. Upon closer inspection it was noted that the proportional increase in the number of respondents from the smaller and relatively new non-traditional players in the FS marketplace (such as the new breed of “fintechs”, challenger banks, etc.) in comparison to the larger, more traditional organizations has driven this outlier in the results. The structures and operational processes in these non-traditional FS organizations are typically leaner with a lower appetite to establish large central utilities/teams and instead a desire to drive autonomy to end users in the business, with consistency obtained through organization-wide technology solutions, policies, guidance materials, and central oversight.

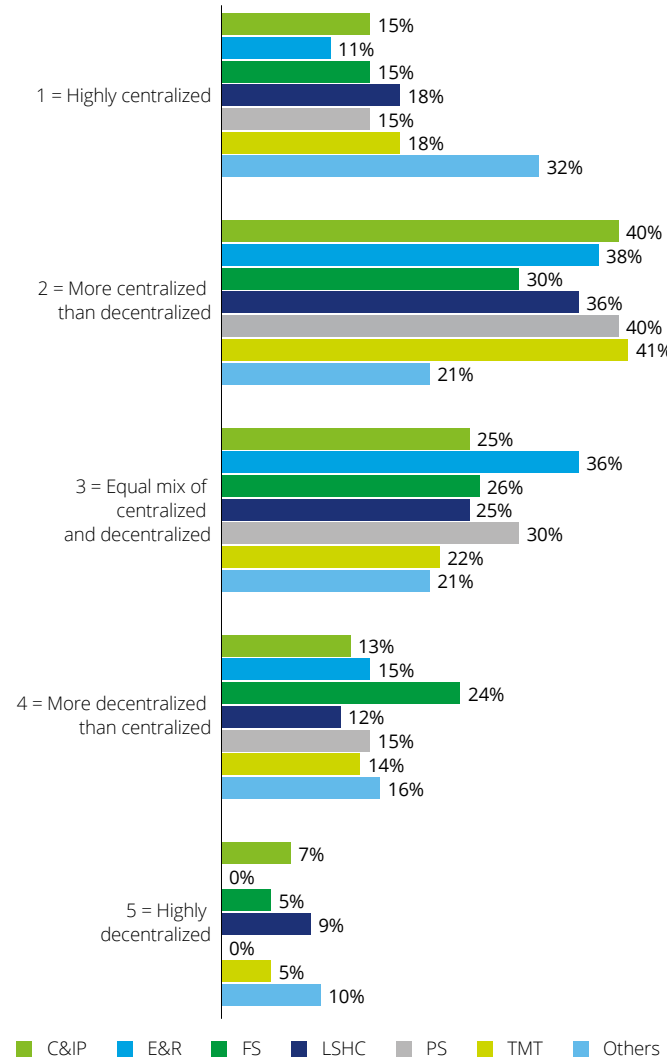
Overall control structure by industry





- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts

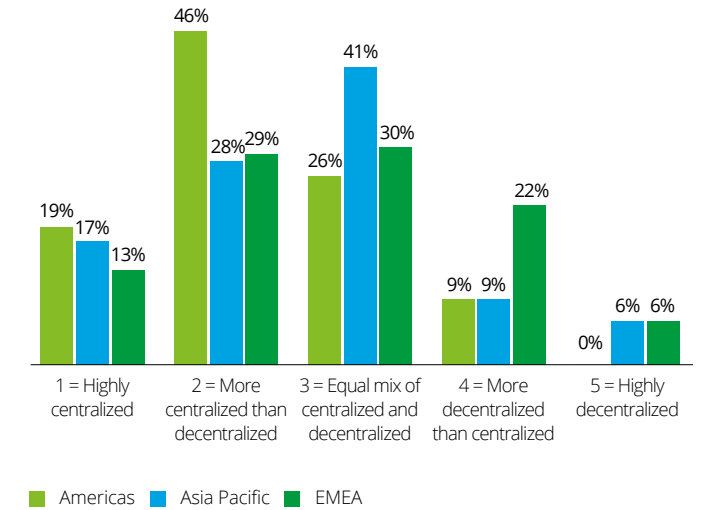
### Organization structure for EERM by industry



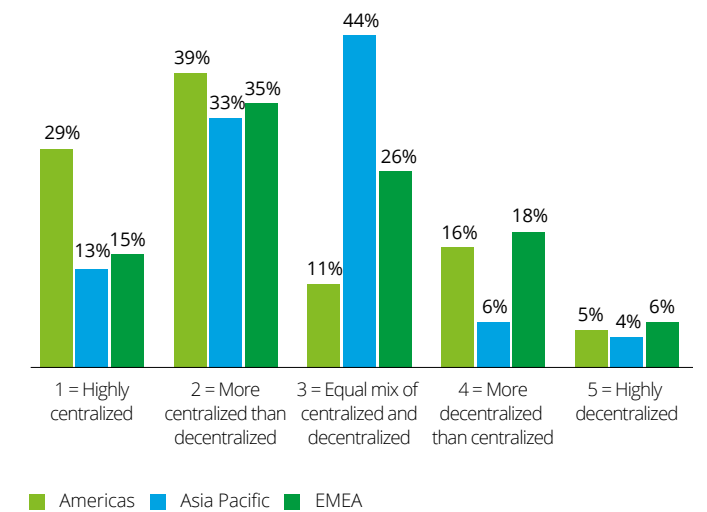
### Geography highlights

- The Americas is clearly the region with the highest level of centralization with only **35 percent** of respondent organizations believing that they are equally or more decentralized. This, in turn, corresponds to the related EERM initiatives also being largely centralized (with only a minority i.e. **33 percent** of respondent organizations believing that their EERM initiatives are equally or more decentralized).
- Asia Pacific with its regional diversity has evolved to be far more decentralized in general with **56 percent** of respondents from that region evaluating their organizations' overall control structures to be equally or more decentralized. In line with this, **54 percent** of respondents believe that their organizational structures for EERM are also in this same decentralized position.
- 58 percent** of respondents from EMEA evaluated their organizations' overall control structures to be equally or more decentralized, reversing the trend of higher decentralization in structure observed up to and including last year. More surprisingly though, a large number of respondents from this region (as many as **50 percent**) believe that their organizational structures for EERM are also equally or more decentralized, implying business unit led silos still dominates EERM initiatives in this region (also reflected by the lowest proportion of respondents in the region who utilize an ERP or procurement backbone for a more centralized approach to EERM).

### Overall control structure by region



### Organization structure for EERM by region



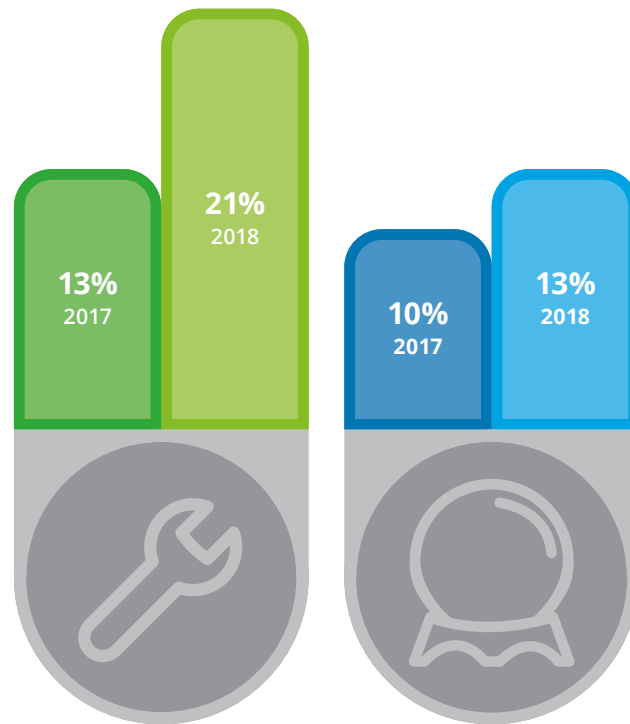


-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  02 Business case and investment
-  03 Centralized control
-  04 Technology platforms
-  05 Sub-contractor risk
-  06 Organizational imperatives and accountability
-  About the authors
-  Contacts



3b. COEs and shared service models represent the dominant operating model, along with an increased focus on market utility models.

**21 percent** of respondents are already utilizing market utilities for EERM (up from **13 percent** last year) with another **13 percent** intending to do so in the near future (up from **10 percent** last year)



**Key messages**

With a shift of gears towards centralization in the current survey, most respondents (**75 percent**) told us that their centralized EERM operations sat either in a CoE or shared service center (whether fully operated by in-house teams or with some coordination with outsourced service providers) to bring in the desired standardization as well as specialized skills and scarce talent.

Various hybrid and innovative delivery models such as federated structures and the “hub-and-spoke” model are also appearing (**29 percent** of respondents) that combine the characteristics of centralized and decentralized organizations and can, in some cases enable an organization to remain more agile and competitive in the marketplace.

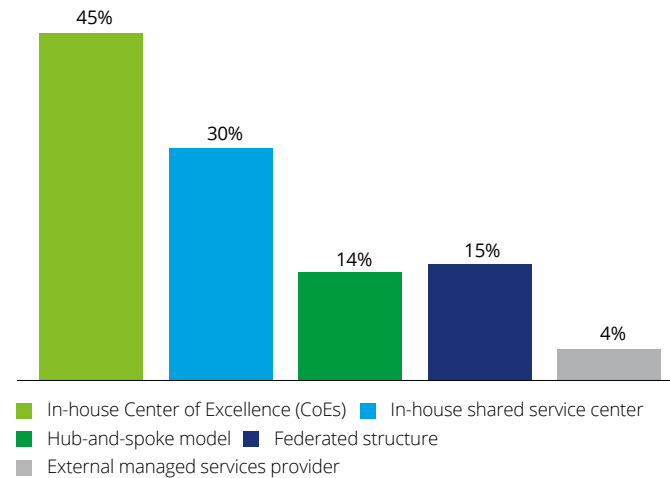
**Four percent** of respondents are progressively moving to a fully outsourced managed services environment as a bespoke external utility for EERM, reflecting early days of another emerging trend to achieve the desired consistency in processes and access to scarce talent.

At the same time, the increasing focus on collaboration (sharing of information across organizations) is rapidly gaining popularity as a key enabler for successful governance and risk management in the networked world. In keeping with this top trend, information hubs (community models) available as market utilities on EERM have emerged. **33 percent** of our survey respondents suggested they either used market utility models in some form or intend to do so in the future to supplement specific aspects of EERM activity.

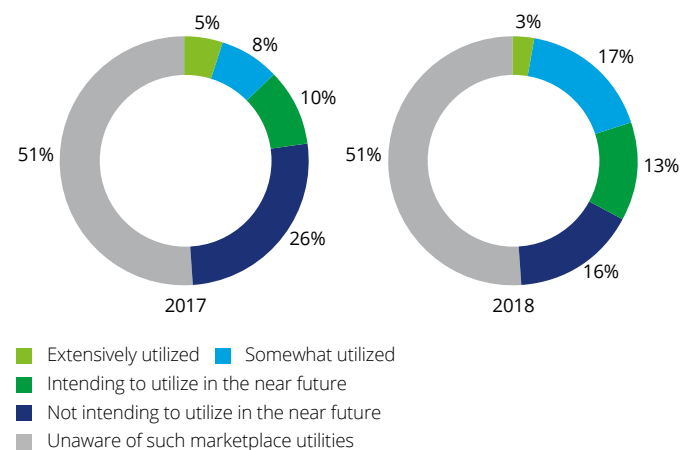


- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control**
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts

**Operating models to coordinate operational, oversight, and assurance roles for EERM talent**



**Utilization of information hubs available as marketplace utilities on third-party risk**



**Deloitte point of view**

Deloitte believes that organizations that are moving to internal CoEs and SSCs are primarily driven by the need to retain organizational control over this critical activity.

However, a managed service option can enable an organization to achieve the desired level of customization it requires (not deliverable from most market utilities), while keeping the cost lower than that of an internal team.

CoEs and managed services models enable setting consistent standards, defining uniform process, implementing common technology across business units with a longer term strategic focus, providing training, executing risk assessments and providing guidance. However, business leadership retains the responsibility for managing risks and governance.

Further, market utility models are heralding in a uniquely innovative approach where the members of the community (typically large global organizations with significant third-party ecosystems) work together to reduce duplication of effort in third-party pre-qualification and retention.

These participating organizations agree common standards for third-parties as well as performance data and collaborate to collect it. Such collaboration is often facilitated by external infomediaries<sup>10</sup> who are making these community information hubs available as market utilities via a subscription-based service. Using cloud-based or other agile technologies, the infomediary then provides access to an independent hub for validated

data and analytics, which helps organizations assess and manage risk. In this way, the controlled sharing of non-confidential information can increase efficiency, raise compliance standards, and reduce costs for the community as a whole.

In addition to compliance with minimum standards for pre-qualification based on criticality of the third-party, potential areas where information related to ongoing governance and risk management of third-parties can be shared include, for instance, data privacy and protection, cybersecurity, regulatory compliance, corporate social responsibility (CSR), ethics and sustainability, supply disruption and continuity, anti-bribery and corruption, safety and quality, EU procurement compliance, and financial distress. Some of the available market utilities also offer independent audit capability and Significant Event Notification and Tracking (SENT), which allow member organizations to manage community-wide disruptive events proactively.

However, community models do not take away the need for organizations to continue investing in their own EERM frameworks and undertaking assessments specific to their standards and third-party arrangements. Some information-hub/market utility providers are also emerging as managed services providers, thus further accelerating the trend.

Consistent with last year, half of respondents were unaware of managed service/utility options available to them, which is understandable, given that such opportunities are relatively new and are still evolving.



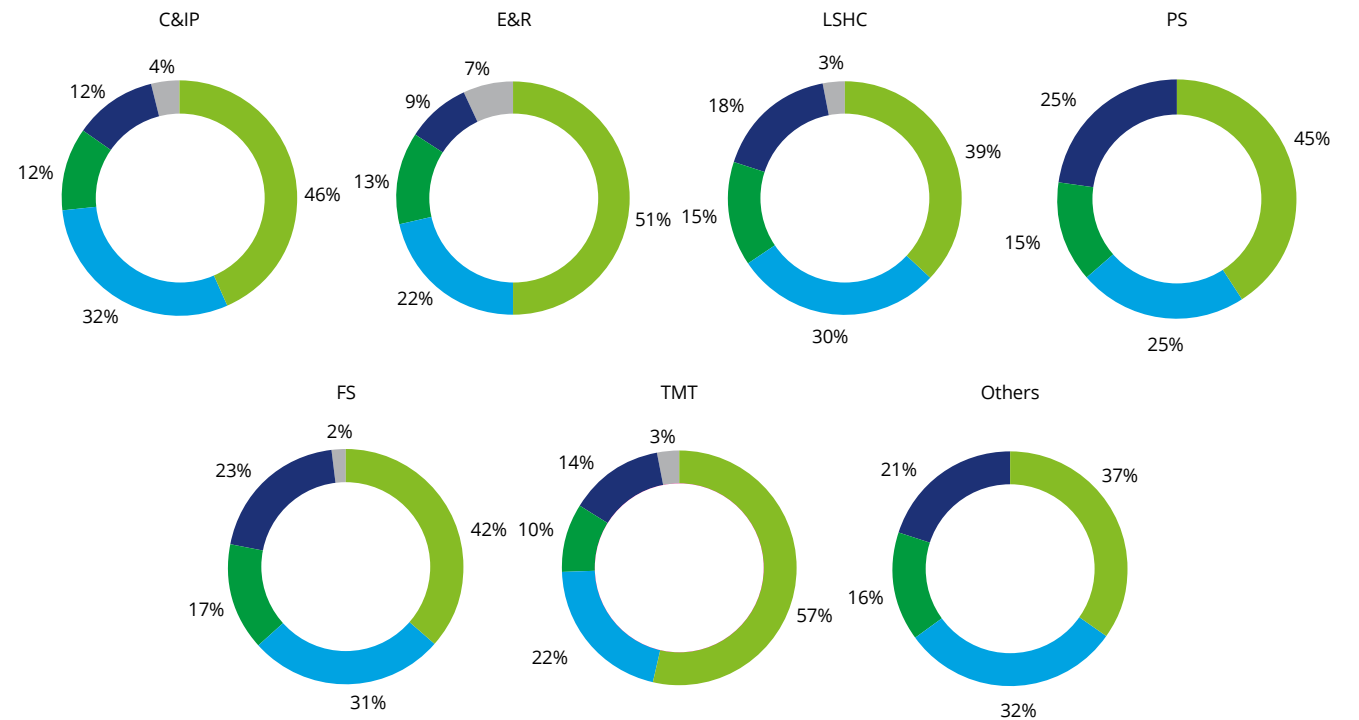
- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control**
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability
- About the authors
- Contacts



### Industry highlights

- The uptake on CoEs and SSCs are fairly consistent across the various industry segments, with the range being **69-79 percent**.
- TMT has the highest level of uptake on CoEs and SSCs with **79 percent** of respondent organizations adopting this operating model, followed by C&IP with **78 percent** and then by E&R and FS with **73 percent** in each case.
- E&R seems to have outsourced the most to managed service providers (**seven percent** of respondents), followed by C&IP (**four percent**) while those doing so the least are FS with **two percent** and PS with **NIL**.
- FS has been leading the way with regard to community models/market utilities since 2016 with the emergence of four key players. Industries that are following suit include LSHC (increase in actual utilization from **16 percent** to **24 percent** during 2017), CB (e.g. FMCG) (**11 percent** to **18 percent**), and TMT (**12 percent** to **27 percent**). E&R (**28 percent** to **33 percent**), while the leading industry segment in exploring market utilities, has some way to go to fully embrace the opportunities here through extensive usage (with only two percent of the latter **33 percent** using such models extensively but the vast majority represented by the other **31 percent** making only limited use). But already we have seen movement to progress in this space at the back end of 2017.

### Operating models to coordinate operational, oversight and assurance roles for EERM talent by industry



- In-house (centralized) Center of Excellence (CoEs) with specialized talent for EERM
- In-house (centralized) Shared Service Center (SSC) with administrative staff for EERM support processes
- Hub-and-spoke model
- Federated structure
- EERM operations are managed fully or predominantly by an external managed services provider (with centralized decision-making retained in the organization)





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts

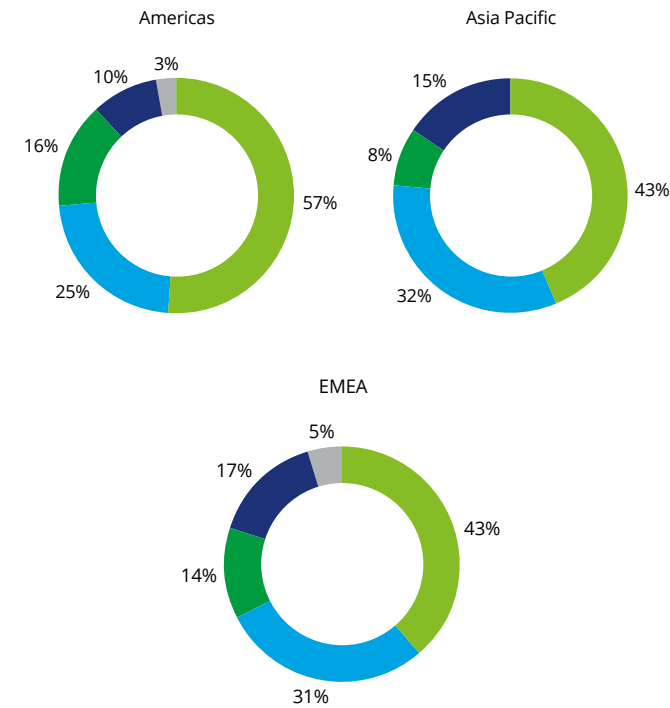


### Geography highlights

The Americas region is ahead of the other regions with **82 percent** of respondent organizations having implemented CoEs or SSCs for EERM, followed by Asia Pacific (**75 percent**) and EMEA (**74 percent**).

- Outsourcing EERM substantially to a managed services provider is still a relatively new concept across all the three regions. While none of the respondents from Asia Pacific have done this, three percent of respondents from the Americas and five percent of respondents from EMEA are following that approach, possibly due to these fully integrated managed service models only recently becoming available in the marketplace.
- EMEA appears to be leading the way on market utilities/ community models with **34 percent** uptake as compared to **21 percent** in the Americas. Respondents from Asia Pacific are either unaware or lack the clarity at this stage to be able to take a decision at this stage.

### Operating models to coordinate operational, oversight and assurance roles for EERM talent by region



- In-house (centralized) Center of Excellence (CoEs) with specialized talent for EERM
- In-house (centralized) Shared Service Center (SSC) with administrative staff for EERM support processes
- Hub-and-spoke model
- Federated structure
- External managed services provider



 Home

 Foreword

 Executive summary

 01 Inherent risk and maturity

 02 Business case and investment

 03 Centralized control

 04 Technology platforms

 05 Sub-contractor risk

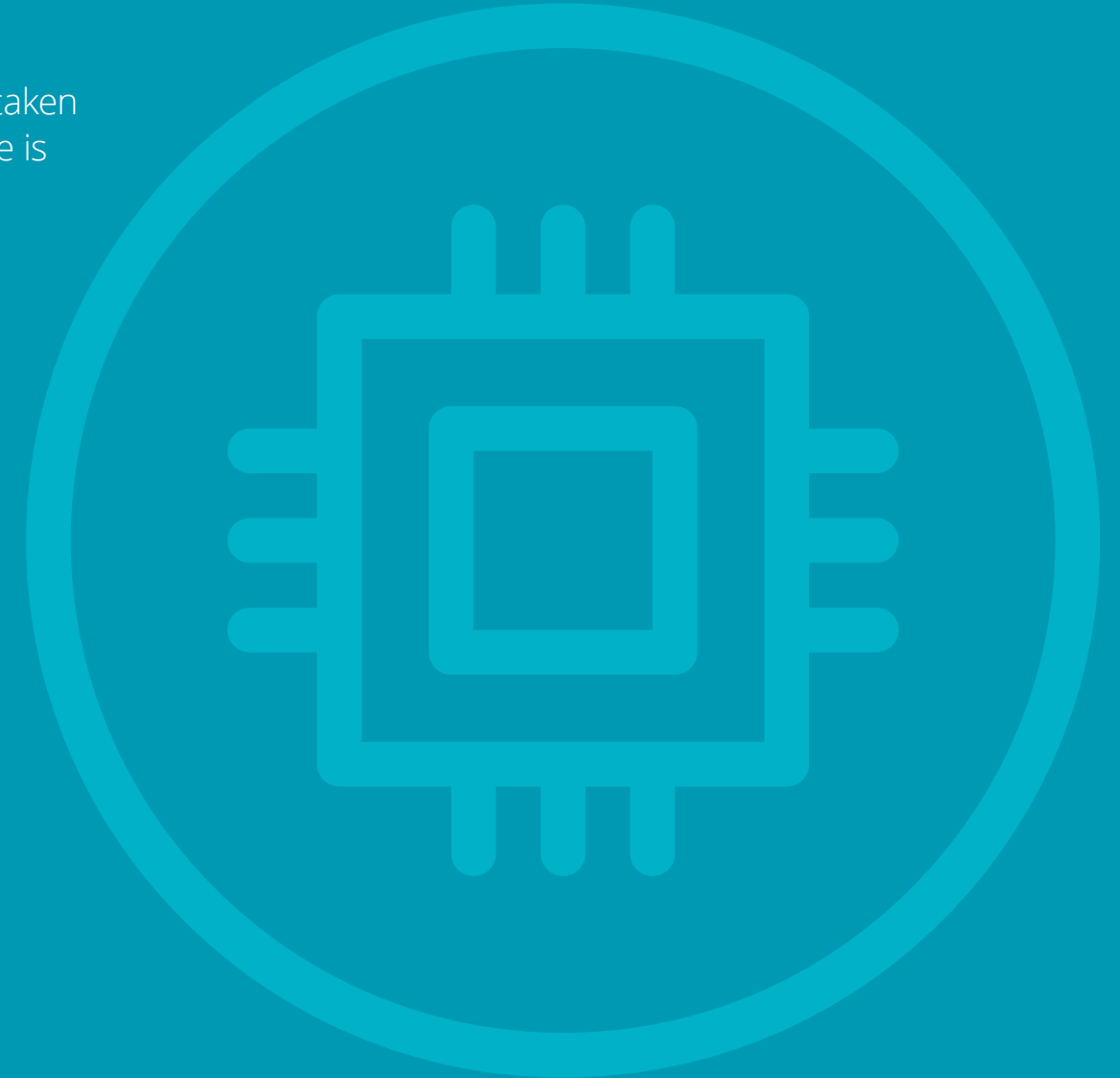
 06 Organizational imperatives and accountability

 About the authors

 Contacts

# 4. Technology platforms

Technology decisions for EERM solutions are now being taken more centrally and a three-tiered technology architecture is emerging.





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



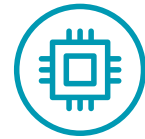
06 Organizational imperatives and accountability



About the authors

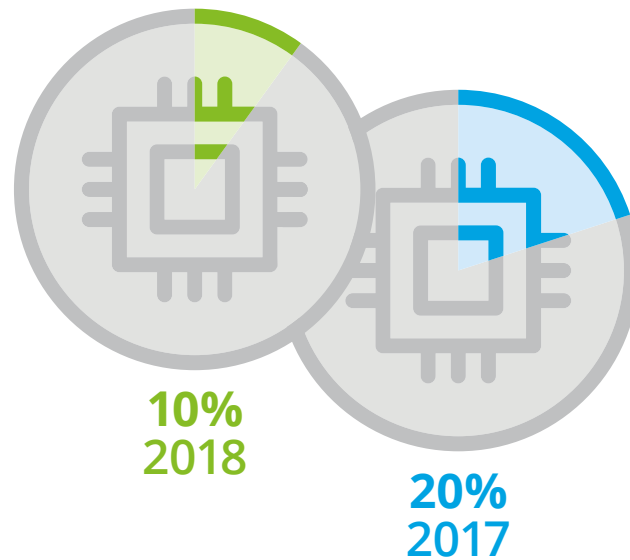


Contacts



4. Technology decisions for EERM solutions are now being taken more centrally and a three-tiered technology architecture is emerging.

Less than **10 percent** of respondents are currently using bespoke systems for EERM, a sharp drop from just over **20 percent** last year.

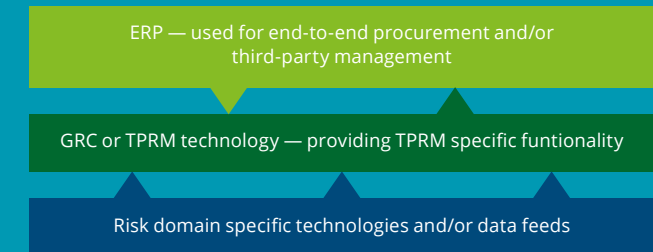


**Key messages**

Our earlier survey results had indicated a somewhat disorganized approach to the use of technology to enable EERM processes from end-to-end, using a combination of more than one platform to manage either different aspects of third-party risk or even different types of third-parties, in some cases, across multiple business units in a piecemeal manner.

However, in keeping with the new trend of increased centralized oversight of EERM activities revealed by the current survey, technology decisions are now being taken more centrally and a standard tiered technology architecture is emerging, particularly among those organizations that have an integrated or optimized status in their EERM maturity scale.

**The evolving tiered architecture for EERM tools and technologies**



- ERP systems or other backbone applications for procurement (ERP + Procurement)
- Generic GRC software or EERM - specific risk management packages or those tailored from specialized risk domains (GRC + TPRM utility + TPRM solutions)
- Other niche packages for specific EERM processes or risks with feeds from specialized risk domains

The 2018 survey results suggest that this three-tier technology architecture will increasingly work in tandem to form a common setup for organizations around EERM and typically comprises of (i) ERP systems or other backbone applications for procurement; (ii) generic GRC software or EERM-specific risk management packages tailored to the organization; and (iii) other niche packages for specific EERM processes or risks with feeds from specialized risk domains. This third tier includes emerging technologies that use natural language processing and machine learning to collect and analyze data from across multiple sources (including the internet) on a scale, and with accuracy levels, that previously were not thought possible without significant and highly expensive human oversight and processing.

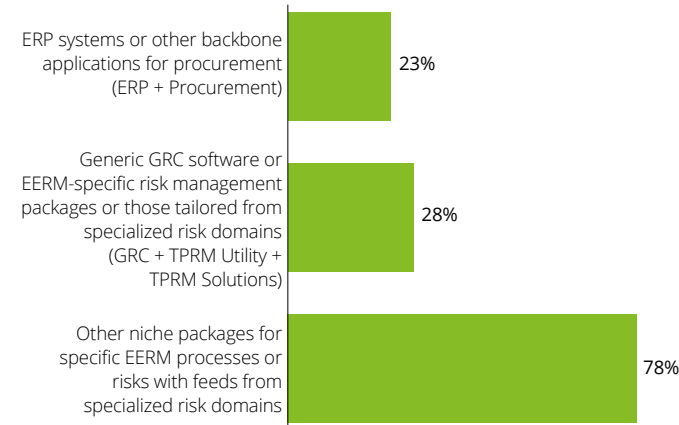


- ⏪
⏩
🏠 Home
- 💬 Foreword
- 📄 Executive summary
- 📈 01 Inherent risk and maturity
- 💰 02 Business case and investment
- 🌐 03 Centralized control
- 🔧 04 Technology platforms
- 🏢 05 Sub-contractor risk
- 📄 06 Organizational imperatives and accountability
- 👤 About the authors
- 👤 Contacts

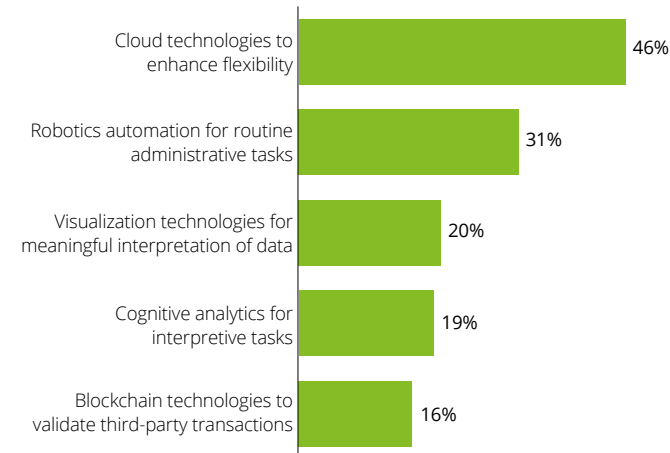
Aligned to this trend, qualitative responses from the survey indicate that organizations are no longer keen to invest in developing complex bespoke solutions for EERM, which, together with the use of its existing ERP platform in the past may have significantly lowered the confidence of stakeholders in the quality and reliability of the overall technical solution for EERM. Less than **10 percent** of respondents are currently using bespoke systems for EERM, a sharp drop from just over **20 percent** last year.

Standardization of technology architecture for EERM using a combination of ERP systems and other backbone applications for procurement packaged solutions is supported by an increasing intent by management to invest in emerging technologies for EERM. Cloud technologies that enable agile business operations with standardization represent the most popular emerging technology platform being investigated by survey respondents. RPA features second on this list, offering the opportunity to automate routine tasks related to EERM. **46 percent** of respondents are planning to utilize standardized cloud technologies for EERM while **31 percent** are considering using RPA for routine EERM tasks across the organization.

### The evolving tiered architecture for EERM tools and technologies



### Emerging technologies for EERM



### Deloitte point of view

Deloitte believes that with the right technology enablement for EERM processes, companies can implement and manage EERM programs that drive efficiency, reduce costs, improve service levels, and increase return on equity. In fact, as outlined in our whitepaper titled “Unlock the value in your technology investments”, organizations with a well-defined technology-enabled EERM framework typically tend to realize an additional four to five percent return on equity.

Better tools and technology can significantly reduce the time spent on pre-contract, post-contract, and ongoing tracking/monitoring activities, thus making available time for focusing on the broader strategic areas of risk management and value creation (e.g. performance, strategy, innovation, commercial, etc.).

Most survey respondents desire integrated technology that would address as many of the dimensions of EERM as possible (e.g. performing due diligence and ongoing risk assessments, recording and presenting KPIs and other performance data through dashboards, facilitating documentation and escalation of issues etc.). The current tiered approach has its advantages in leveraging multiple dimensions of available technology, but those organizations in managed status or below are still being compelled to build in some spreadsheet or manual process-based intervention to bridge the gaps.



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



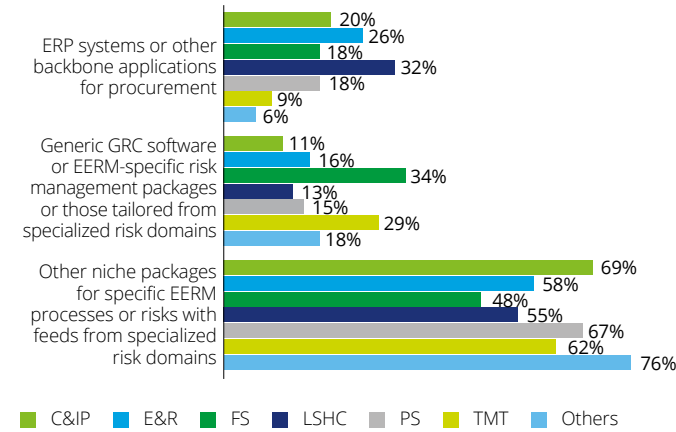
Contacts



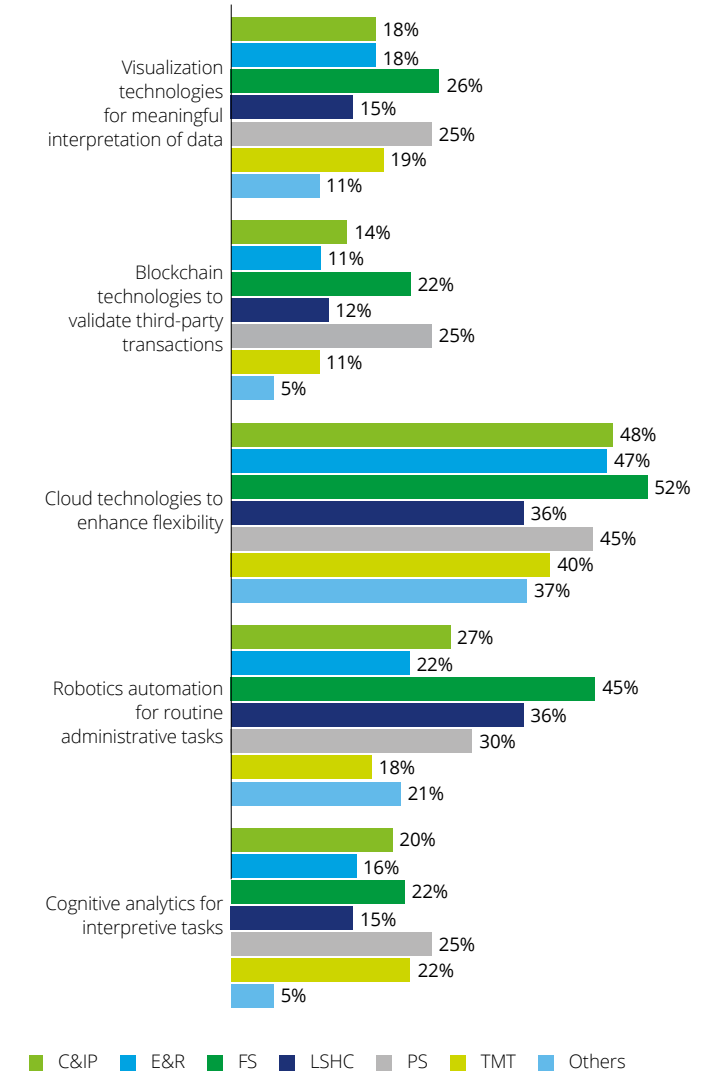
### Industry highlights

- The use of features of the existing ERP system or other organization-wide backbone systems for procurement seem to be the highest in E&R and LSHC industries (**26 percent** and **32 percent** of respondents, respectively) and the lowest in FS, PS, and TMT (**18 percent**, **18 percent**, and **nine percent** of respondents, respectively).
- The uptake of generic GRC packages is highest in FS with **34 percent** of respondents subscribing to this option, followed by TMT (**29 percent**) but lowest in C&IP (**11 percent** of respondents).
- Use of other niche packages appears to be the dominant trend in C&IP (**69 percent** of respondents) and lowest in FS (**48 percent**).
- The overall average of organizations using all of the three-tiers in tandem with each other is around **20 percent** which roughly equals the number of respondents who have achieved integrated or optimized status in the EERM maturity scale.
- All industries appear to be interested in exploring future technologies and are broadly following a similar trend.

### Evolving tiered architecture for EERM tools and technologies by industry



### Emerging technologies for EERM by industry





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



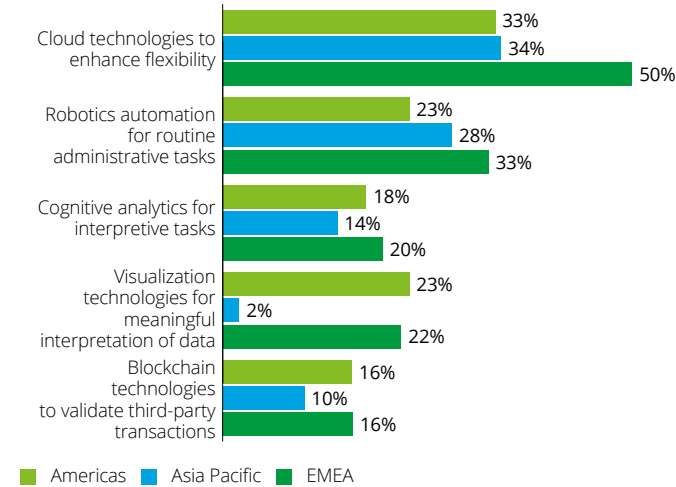
Contacts



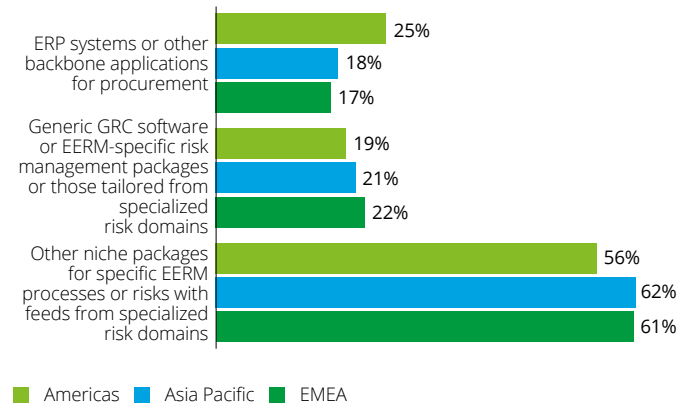
### Geography highlights

- Using the features of the organizational ERP system or other backbone procurement applications for EERM appears to be most common-place in the Americas (**25 percent** of respondents) but the lowest in EMEA (**17 percent** of respondents) where using a combination of niche packages for specific EERM processes or risks with feeds from specialized risk domains make up for the difference, although all three regions broadly follow a similar trend.
- Organizations in EMEA appear to be taking the lead with cloud-related initiatives for agile EERM (**50 percent** of respondents) as well as in exploring robotics automation (**33 percent**), cognitive analytics (**20 percent**), and other emerging technologies for EERM, although once again the overall trend is broadly similar across the three regions with some limited exceptions.

### Emerging technologies for EERM by region



### Evolving tiered architecture for EERM tools and technologies by region







Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



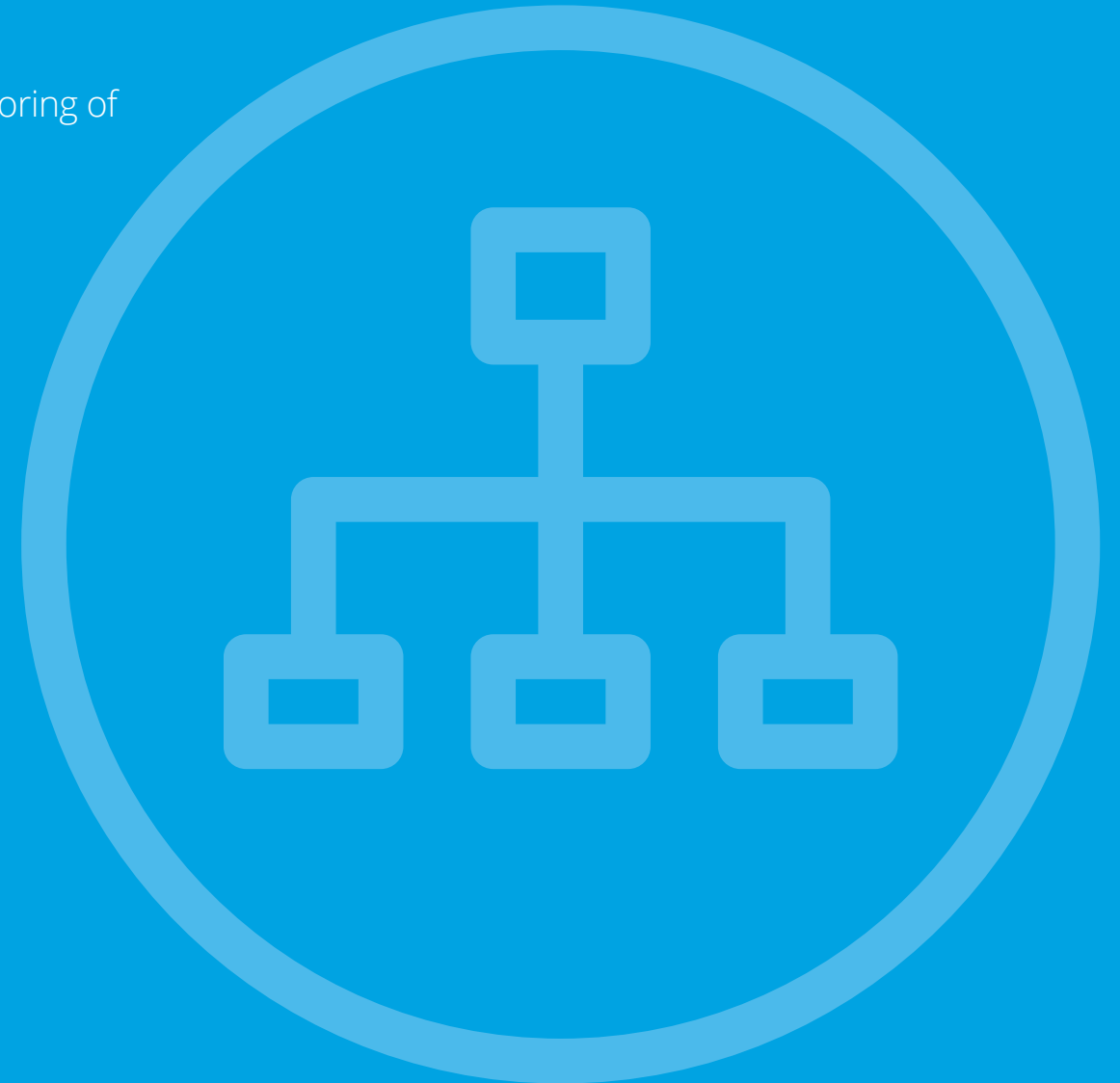
About the authors



Contacts

# 5. Sub-contractor risk

Organizations are lacking appropriate visibility and monitoring of sub-contractors engaged by third-parties.





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors

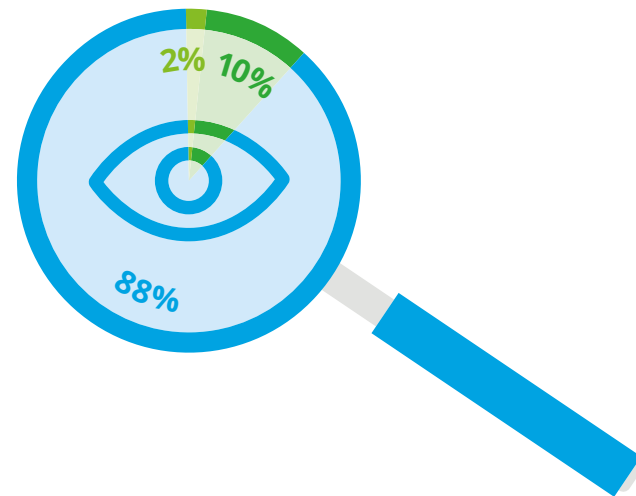


Contacts



## 5. Organizations are lacking appropriate visibility and monitoring of sub-contractors engaged by third-parties.

Only **two percent** of respondents regularly identify and monitor their sub-contractors (fourth/fifth parties) while another **10 percent** do so only for those sub-contractors identified as critical.



### Key messages

Our survey results reveal that respondent organizations lack appropriate visibility of instances where sub-contractors are engaged by their third-parties. The majority (**57 percent**) of survey respondents do not have adequate knowledge and appropriate visibility of sub-contractors engaged by their third-parties and a further **21 percent** are unsure about whether anyone at all in their organization has such visibility or not.

Further, only **two percent** of respondents regularly identify and monitor their sub-contractors (fourth/fifth parties) while another **10 percent** do so only for those sub-contractors identified as critical. The other **88 percent** either rely on their third-parties to do so; have an unstructured/ad hoc approach; do not do so at all; or do not know their organizational policy and practices in this regard.

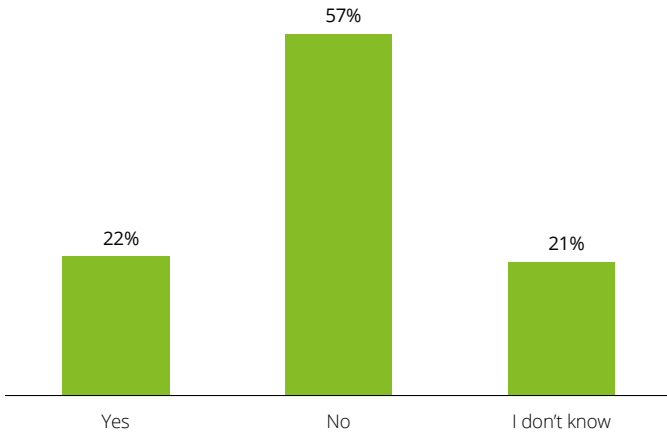
This is making it difficult for organizations to determine their strategy and approach to the management of sub-contractor risk and to apply the appropriate amount of discipline and stringency. Recent regulation such as the Modern Slavery Act and GDPR, which include requirements to manage layers of fourth/fifth parties, where they exist, makes this a matter of increased concern.

Finally, only **18 percent** of organizations periodically review the concentration risk associated with their fourth/fifth parties quarterly or half-yearly; while the vast majority (**82 percent**) review this annually or even less frequently, making it a matter of serious regulatory concern in the highly regulated industries.

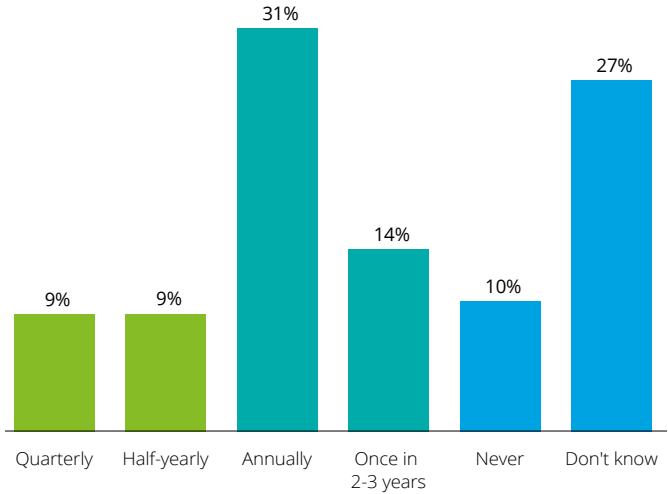


- ⏪ Home
- 💬 Foreword
- 📄 Executive summary
- 📈 01 Inherent risk and maturity
- 💰 02 Business case and investment
- 🔗 03 Centralized control
- 🔧 04 Technology platforms
- 🏗️ 05 Sub-contractor risk
- 📄 06 Organizational imperatives and accountability
- 👤 About the authors
- 👤 Contacts

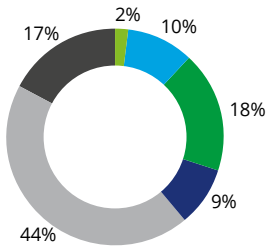
**Adequate knowledge and an appropriate level of visibility over sub-contractors engaged by third-parties**



**Frequency of periodic review of the concentration risk**



**Monitoring sub-contractors engaged by third-parties and retaining records along with corrective action**



- Fourth/fifth parties are identified and regularly monitored
- The most critical fourth/fifth parties are identified and regularly monitored
- Some fourth/fifth parties are identified and reviewed on an ad hoc basis
- Fourth/fifth parties are reviewed at the initiation of any new contract with a third-party
- Our organization relies upon and monitors the procedures within its third-parties as the primary basis
- Fourth/fifth parties are not identified, reviewed or monitored at all



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts



### Deloitte point of view

The growth of subcontracting as a global phenomenon in recent years has been driven by exactly the same factors that have contributed to the rise of the extended enterprise ecosystem. As a matter of fact, sub-contractors are nothing other than the extended enterprise of suppliers and service providers to the focal organizations covered by the survey. Their suppliers and service-providers have also been motivated by the desire to gain competitive advantage through the involvement of third-parties, i.e. enable better product or service innovation, facilitate expansion to new markets, and provide access to skills and capabilities not available internally, while they (as suppliers of goods and services) continue to focus on their core business processes. Sometimes the sub-contractor (referred to as fourth parties to the focal organization) may also be further sub-contracting some of the sub-contracted processes, creating fifth parties, sixth parties, and so on to the focal firm.

At the same time, disruptive incidents globally are increasingly confirming that these suppliers have themselves been much less focused on bringing in a holistic and integrated approach to their own third-party ecosystem than their customers, as many of these customers may be subject to third-party regulation in their respective industry segments which the suppliers or sub-contractors are not. But as these suppliers take their extended enterprise to

new levels of criticality in dependence, their sub-contractors (referred to as fourth parties) are now exposing not just them but their end-customers to the threats of high profile customer service disruption and other major business failures. These failures are now attracting the attention of the regulators who are holding organizations accountable for lack of oversight of third-parties and their sub-contractors. Where these risks have been realized, this has compromised organizational reputation, broken down business continuity, and attracted substantial penalties and regulatory enforcement action.

We understand most organizations are focusing on identifying, assessing, and managing the risk in their third-parties and believe that, for the moment, just having an awareness of sub-contractor relationships is sufficient. The tug of war between the regulatory requirements to manage the risks all the way through the extended enterprise versus the legal/contractual view that your responsibility stops at your third-party is emerging as an interesting area of debate.

Some organizations will continue to rely on their third-parties' own EERM procedures but in critical scenarios/ certain situations they may want the ability to intervene on a more real-time basis.



### Industry highlights

- In general, the lack of stringency and discipline in monitoring/oversight of sub-contractors by respondent organizations is common to all industry segments and geographic regions.
- It is counter-intuitive to note that the more regulated industries (in relative terms) such as FS and LSHC are the weakest performers in this regard with as many as **81 percent** and **85 percent** of respondents, respectively, acknowledging that they do not have appropriate knowledge and visibility over their fourth/fifth parties. C&IP and E&R, both with **75 percent** of respondents in this position follow in their footsteps.
- Similarly, only **15 percent** of the respondents from FS as well as an equal proportion of respondents from C&IP review concentration and other risks from their fourth and fifth parties either quarterly or half-yearly, followed by **24 percent** in TMT and **33 percent** in E&R.



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability

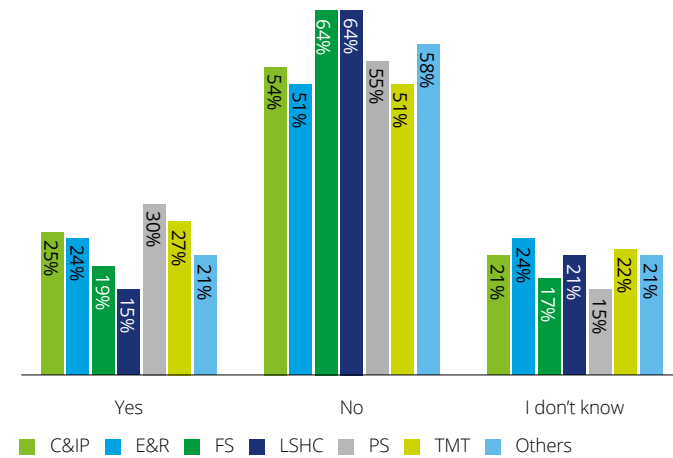


About the authors

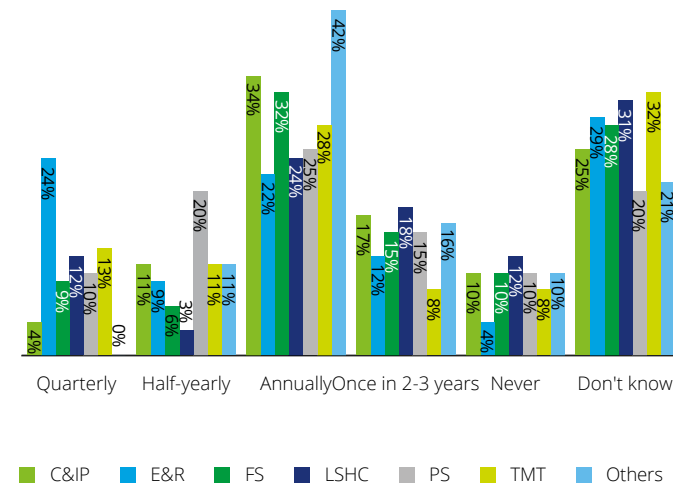


Contacts

### Adequate knowledge and an appropriate level of visibility over sub-contractors engaged by third-parties by industry



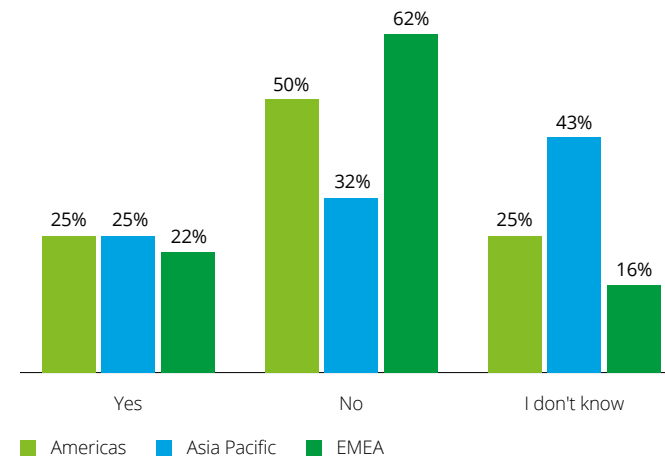
### Frequency of periodic review of the concentration risk by industry



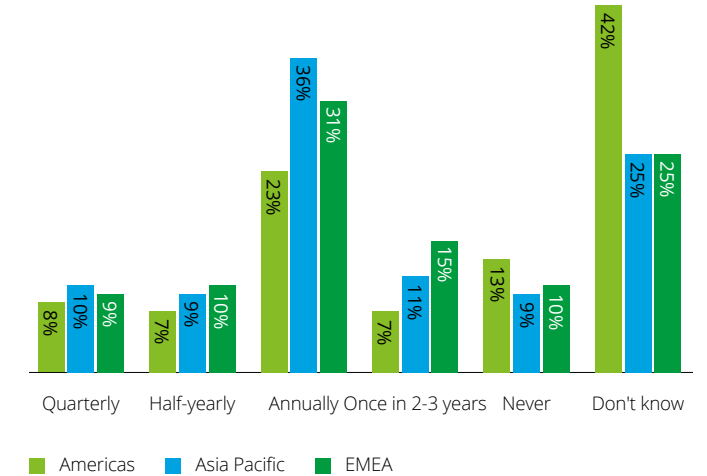
### Geography highlights

- The lack of knowledge and visibility of sub-contractors is fairly consistent across all the three geographic regions spanning around **three out of four respondents** in each region.
- The periodicity of monitoring is however the least in Americas with the majority of respondents (**55 percent**) acknowledging that they either do not monitor such sub-contractor risks at all or do not know if anyone in their organization does so as against **35 percent** of respondents being in that position in EMEA and **34 percent** in Asia Pacific. However, even in the latter geographies, only **19 percent** of respondents monitor this half-yearly or quarterly (**15 percent** in Americas), implying far more needs to be done in this regard.

### Adequate knowledge and an appropriate level of visibility over sub-contractors engaged by third-parties by region



### Frequency of periodic review of the concentration risk by region





- Home
- Foreword
- Executive summary
- 01 Inherent risk and maturity
- 02 Business case and investment
- 03 Centralized control
- 04 Technology platforms
- 05 Sub-contractor risk
- 06 Organizational imperatives and accountability**
- About the authors
- Contacts

# 6. Organizational imperatives and accountability

- 6a. Ultimate ownership and accountability for EERM suggests it is well and truly established in the C-suite roles with need for improvement in engagement.
- 6b. Challenges over internal coordination, talent and processes represent areas of highest (organizational) concern over EERM.



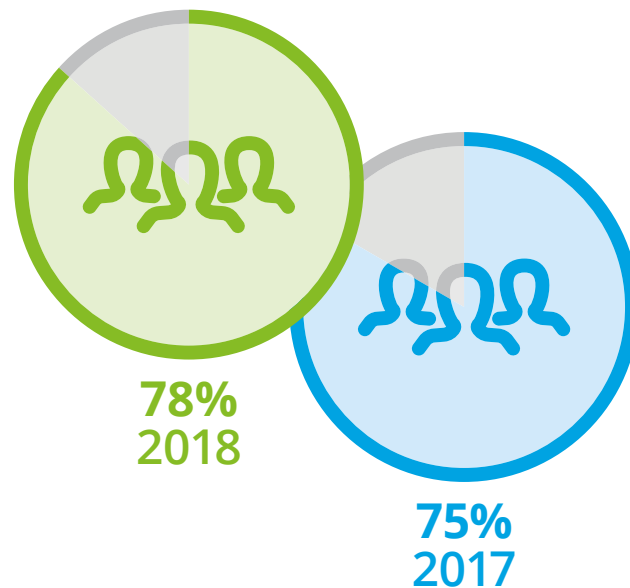


-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  02 Business case and investment
-  03 Centralized control
-  04 Technology platforms
-  05 Sub-contractor risk
-  **06 Organizational imperatives and accountability**
-  About the authors
-  Contacts



6a. Ultimate ownership and accountability for EERM suggests it is well and truly established in the C-suite roles with need for improvement in engagement.

Either the CEO, CFO, CPO, CRO, or a member of the Board is ultimately accountable for EERM in **78 percent** of the organizations, up from **75 percent** last year.



**Key messages**

Survey results around the ownership and accountability for EERM suggests it is well and truly established in the C-suite with **78 percent** of organizations suggesting that either the CEO, CFO, CPO, CRO, or a member of the Board is ultimately accountable for this topic. This includes a member of the Board being ultimately accountable for EERM in **19 percent** of the cases and **33 percent** suggested the CEO (**21 percent**) or CFO (**12 percent**) had a similar responsibility.

In some cases, there appears to be a small shift in ultimate accountability from CPOs and Vendor/Alliance Managers to Heads of Risk and CFOs under Board/CEO supervision, although this is not still true where the organizational supply-chain forms the most significant component of the extended enterprise. In such organizations which still form the majority, the CoEs and shared services are also largely owned by procurement teams.

Survey respondents however believe that there is room for improvement in the level of engagement on the EERM agenda by Board members and risk domain owners. Only **20 percent** of Board members have a high level of engagement, where a member of the Board has ultimate accountability. This, in turn, implies that levels of engagement in the remaining **80 percent** of organizations where the Board operates in an oversight or supervisory role are at best moderate (**42 percent** of respondents) if not low (**19 percent**), absent or unknown (**seven percent** and **12 percent** respectively).

The data relating to the levels of engagement of risk domain owners is also not very encouraging. Only **16 percent** of risk domain owners had a high level of engagement and understanding of EERM with the vast majority represented by the remaining **84 percent** of respondents who felt risk domain owners had at best moderate (**45 percent**), low (**17 percent**) or levels of engagement that were absent (**seven percent**) or unknown (**15 percent**). Survey respondents believe that relatively lower levels of engagement and understanding by risk domain owners negatively impacted the level of coordination with other stakeholders as discussed in our finding 6(b) on page 58.

Survey respondents believe that a key underlying factor for this limited engagement is the lack of regular supervisory review by the Board. Only **11 percent** of organizations surveyed have formal Board reviews on a quarterly basis with at best another **10 percent** doing this on a half-yearly basis. For **35 percent**, this is just another annual processes to be completed while **38 percent** do not know when they had such a review or whether they had it at all.





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability

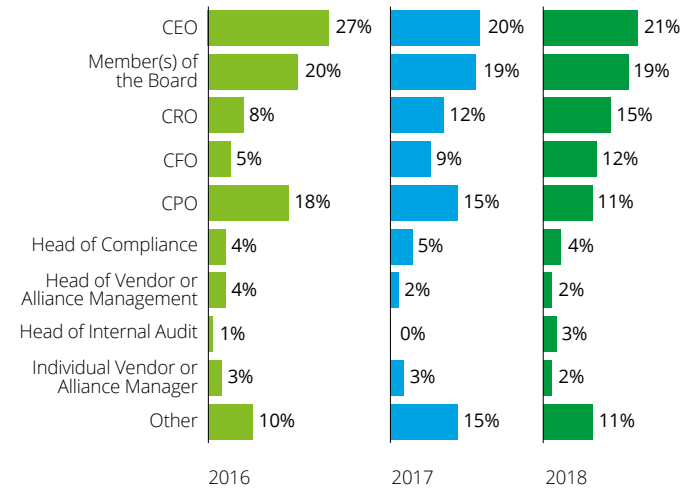


About the authors

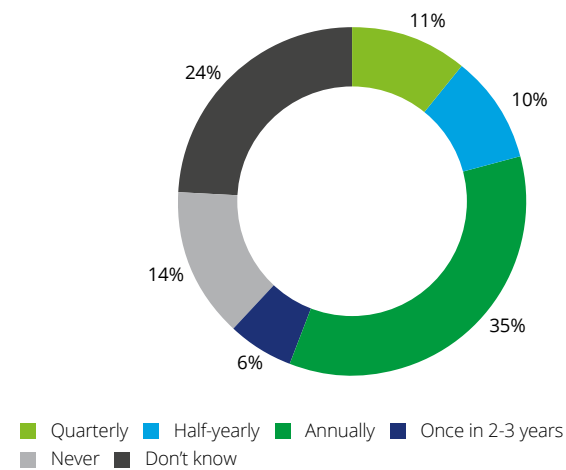


Contacts

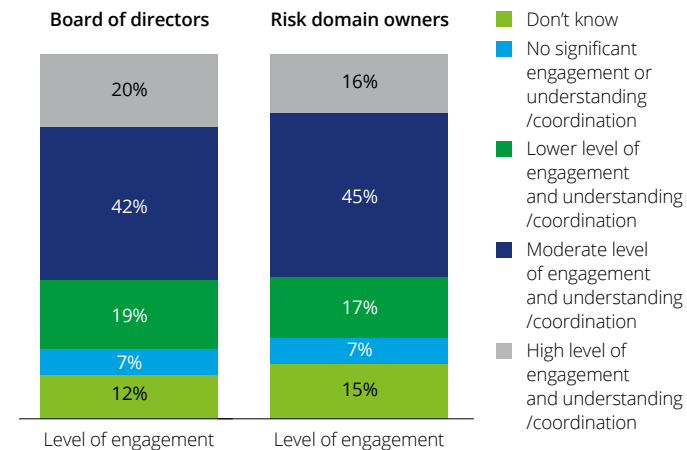
**Ultimate accountability for EERM**



**Frequency of board-level EERM review focused on alignment with strategic plan and risk appetite**



**Level of engagement of Board members and risk domain owners in EERM**



**Deloitte point of view**

As extended enterprise risks grow, along with shareholder, political, legal, and regulatory activism, there is likely to be a greater demand placed on management and boards to be accountable for major risk events, whether the events occur within the organization or across its extended enterprise. In this scenario, Deloitte believes that Boards in their governing (supervision and oversight) capacity should have deeper levels of engagement and more frequent reviews to ensure management has elevated EERM to appropriate levels and established robust risk management structures and processes.

Deloitte specialists recognize that Boards are already very busy. But as extended enterprises expand and grow in strategic importance, the expectation is that Boards will play a more engaged role with regard to third-party risks.

Today, a large number of global Boards carry out their risk oversight responsibilities either by themselves or at best with some support from CFOs and its audit committee. As extended enterprises grow in complexity and scale, we predict that more Boards globally may be considering the establishment of risk committees or similar focus groups to assist them in ensuring a more systematic and broader oversight of strategic and operational risks, as is currently an emerging trend in North America.



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



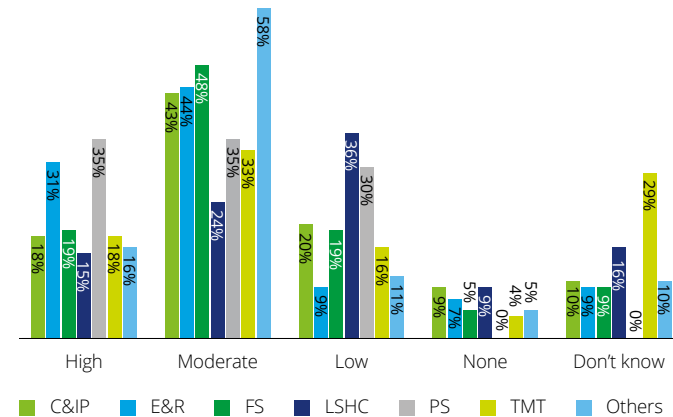
Contacts



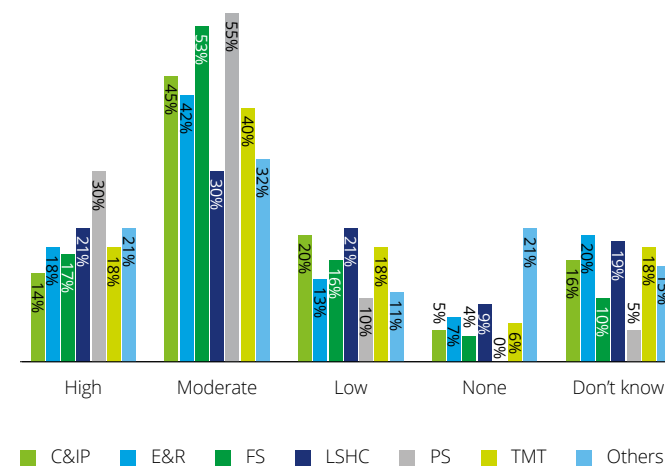
### Industry highlights

- The level of engagement and knowledge of EERM by the Board appears to be the highest in PS (**35 percent** of respondents) and E&R (**31 percent**) and the lowest in LSHC (**15 percent**), C&IP (**18 percent**), and TMT (**18 percent**), followed closely by FS (**19 percent**).
- High levels of engagement and coordination by risk domain owners is once again the highest in PS (**30 percent** of respondents), followed however by LSHC (**21 percent**), E&R (**18 percent**), and FS (**17 percent**).

### Level of engagement and understanding of board of directors with risks relating to the extended enterprise of their organization by industry



### Level of engagement and coordination between risk domain owners and the EERM team by industry



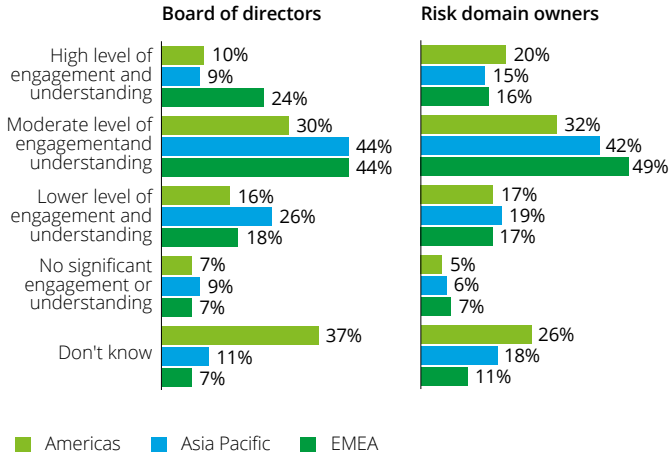
### Geography highlights

- Organizations from EMEA appear to have the highest level of engagement in relative terms from their Boards with **24 percent** demonstrating a high level of engagement and understanding, as compared to only **10 percent** in the Americas and **nine percent** in Asia Pacific. The lack of awareness by respondents on the level of Board engagement in EERM is also the highest in the Americas with as many as **37 percent** respondents unaware of the actual position, as against only **seven percent** in EMEA and **11 percent** in Asia Pacific.
- This diversity across regions is supported by the fact that only **seven percent** of respondents from the Americas have quarterly or half-yearly supervisory reviews of EERM by the Board, compared to **24 percent** in Asia Pacific and **23 percent** in EMEA.
- The engagement of risk domain owners however is relatively much higher in the Americas with **20 percent** of respondents having a high level of engagement and understanding, compared to **16 percent** in EMEA and **15 percent** in Asia Pacific. However, **27 percent** of respondents from the Americas are not aware of the position in this regard, as against only **11 percent** in EMEA and **18 percent** in Asia Pacific.

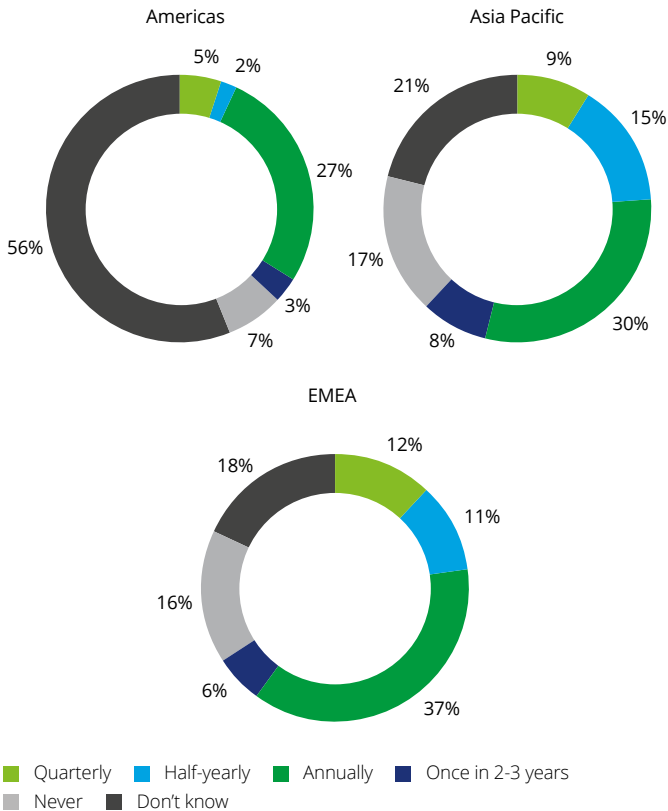


- ⏪ ⏩
🏠 Home
- 💬 Foreword
- 📄 Executive summary
- 📈 01 Inherent risk and maturity
- 💰 02 Business case and investment
- 🌐 03 Centralized control
- 🔧 04 Technology platforms
- 🏗️ 05 Sub-contractor risk
- 📄 06 Organizational imperatives and accountability
- 👤 About the authors
- 👤 Contacts

**Level of engagement of board members and risk domain owners in EERM by region**



**Frequency of board-level EERM review focused on alignment with strategic plan and risk appetite by region**



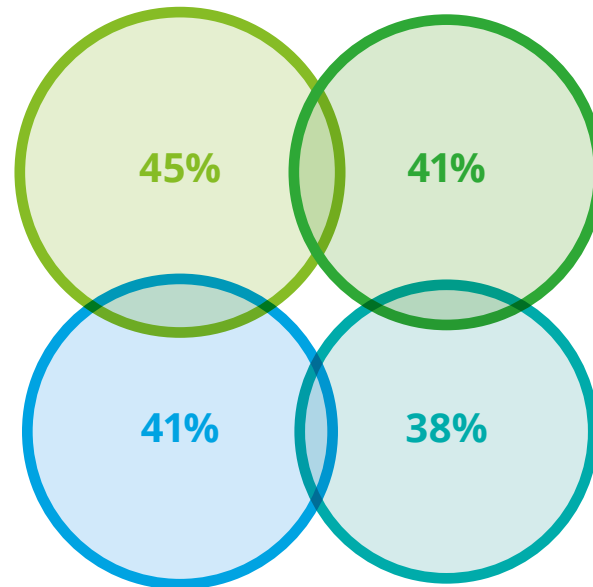


-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  02 Business case and investment
-  03 Centralized control
-  04 Technology platforms
-  05 Sub-contractor risk
-  **06 Organizational imperatives and accountability**
-  About the authors
-  Contacts



6b. Challenges over internal coordination, talent and processes represent areas of highest (organizational) concern over EERM.

Skills, bandwidth and competence of talent appears to be the most significant concern related to EERM (**45 percent** of respondent organizations); followed by the clarity of roles and responsibilities (**41 percent**), EERM processes (**41 percent**), stakeholder awareness and commitment to third-party risks (**38 percent**).



**Key messages**

Survey results indicate that skills, bandwidth, and competence of talent engaged in EERM-related activities appears to be the most significant concern for respondents (**45 percent**), followed by the clarity of roles and responsibilities and EERM processes (**41 percent** in either case).

Stakeholder awareness and commitment to third-party risks have emerged as a newer area of concern with **38 percent** of respondents, an issue that we have not seen in the forefront in our earlier surveys in general terms, although a more specific need to get attention of the Board and feature as an ongoing priority item in the related agenda had been expressed by respondents.

Other areas of emerging concern include achieving organizational agreement/clarity in (a) identification of strategically critical third-parties (**32 percent** of respondents) and (b) structure of the third-party management organization (**30 percent** of respondents), implying the need for better alignment and coordination from an *intrapreneural*<sup>1</sup> rather than an entrepreneurial perspective.

It is therefore no surprise to see that as many as **40 percent** of respondent organizations have prioritized the need to establish better coordination between risk domain owners, business unit leaders, functional heads, legal, and internal audit teams, etc. as the top organizational imperative related to EERM.

Aligned to the concern of non-standardized processes and lack of clear roles/responsibilities, the need to strengthen due diligence activities prior to onboarding new third-parties is second on the list of top organizational imperatives related to EERM (**35 percent** of respondent organizations). This, in turn, is followed by the need to build stronger resilience to disruption caused by third-party related incidents (**24 percent**) and ensure a proportionate EERM approach based on the categorization of the most strategic third-parties to the organization (**24 percent**).



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability

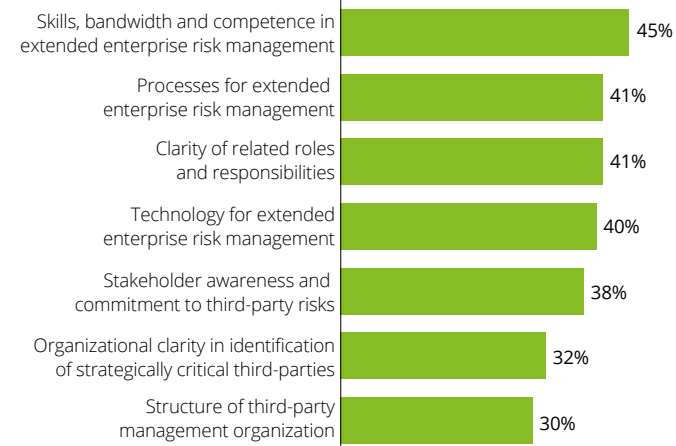


About the authors

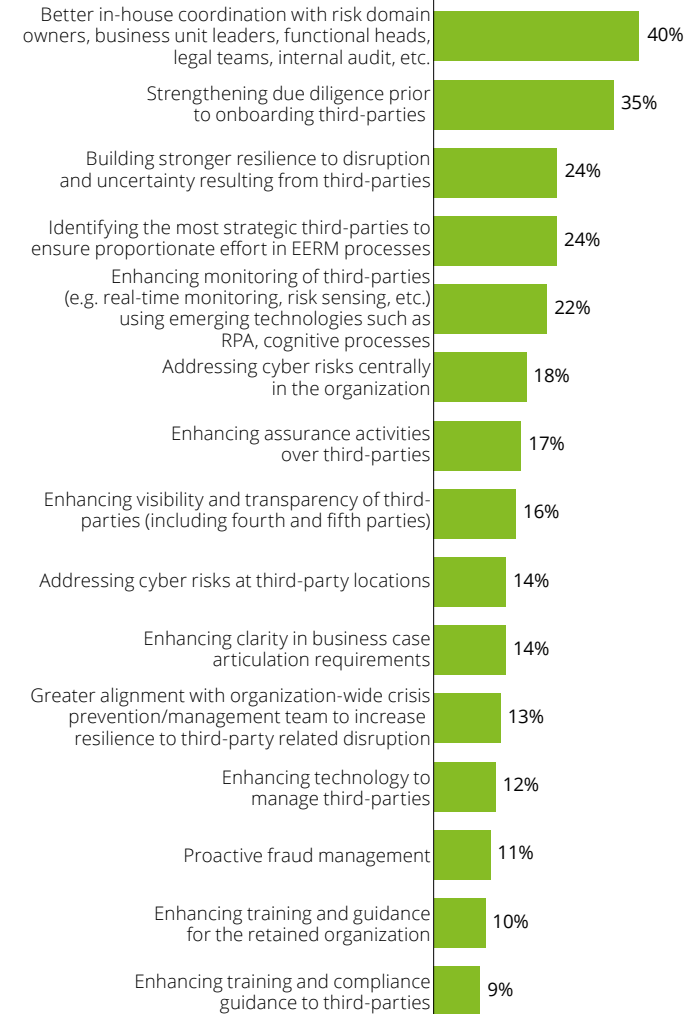


Contacts

### Leadership concerns around EERM



### Top organizational imperatives related to EERM





Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts



**Deloitte point of view**

There has been a significant change in organizational priorities and underlying leadership concerns since our previous survey where tools and technologies used for EERM had concerned a vast majority (more than **90 percent**) of respondents. Respondents to our previous survey had indicated that this concern around the lack of a single unifying technology to manage EERM, together with the disparity of third-party management processes across the depth and breadth of increasingly decentralizing organizations had created an “execution gap” that came in the way of integrating and optimizing EERM.

Deloitte specialists believe that two trends over the last 12 months, both discussed earlier in this report, have been key to reducing this overwhelming concern. First, the introduction of centralized ownership and management within the more decentralized structures supported by the increasing dominance of CoEs and SSCs (see key finding 3a). Second, although a single technology solution for EERM is still yet to emerge, the standardization of the three-tier technology architecture (see key finding 3b) has gone a long way in showcasing the tiered way forward for technology enablement that can address the execution gap. There is however more to do in articulating and standardizing “best-of-breed” processes.

As risk management and governance becomes an overarching strategic issue, aligned to business strategy and operations drilling down to individual business units, it is natural that more and more people at various levels, functional areas, and stakeholders will have a role to play. Further, a much broader and newer set of risks and strategic assets which are more difficult to leverage, manage, and protect will continue to emerge—including people, intellectual property, customers, marketing efforts, and even, for example, “the crowd” in emerging phenomena like crowdsourcing. This will need new skills to be infused into the organization and roles to be redefined. Apart from the emerging risk domains as well as the owners of these new risk domains, organizations should consider external stakeholders who herald a more *outside-in* perspective including, for instance, customers, bloggers, information trendsetters, and marketplace/security analysts.

Each of these players brings a unique set of perspectives and skill-sets to risk management and governance which can be an invaluable asset to every business, provided they are orchestrated to ensure that:

- There is complete clarity on who does what in the area of risk management.
- There are neither overlaps nor underlaps in who does what.
- Limited risk management resources are deployed effectively across the organization to address the most significant areas of concern and opportunity across the business.

As a result, internal coordination (specifically between risk domain owners, business unit leaders, functional heads, legal, and internal audit teams) has now emerged as a key concern in the current survey in addition to ensuring the ongoing relevance of skills, roles, and responsibilities as compared to realistic reassessments of available staff bandwidth.

Accordingly, organizational imperatives that address issues around coordination, talent and processes and “putting the house in order” have now overshadowed the technology-related concerns expressed in earlier surveys.



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts

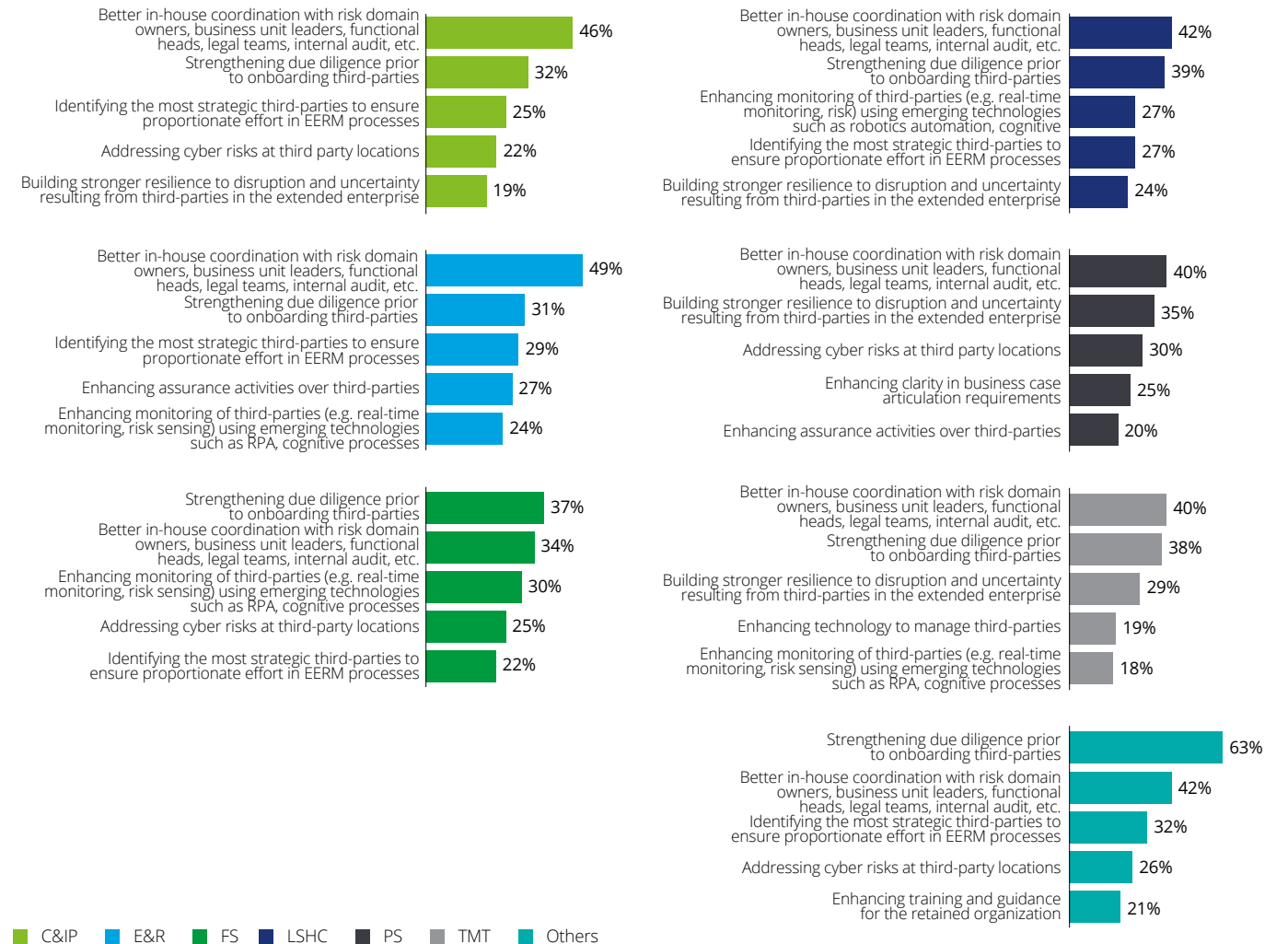


### Industry highlights

The need to build better in-house coordination with risk domain owners, business unit leaders, functional heads, legal, and internal audit teams, etc. consistently features as a top organizational imperative within all the key industry sectors, followed by the need to strengthen due diligence prior to onboarding third-parties and more generally enhance assurance activities or monitoring within the extended enterprise.

- Identifying the most strategic third-parties to ensure proportionate EERM effort is a top imperative across the C&IP, E&R, FS, and LSHC industry segments.
- Addressing cyber risks is a top organizational imperative in the C&IP, FS, and PS industry segments.
- Building stronger resilience to disruption is a key action item for respondents from C&IP, LSHC, PS, and TMT industry groups.
- Enhancing technology to address EERM requirements, however remains a top imperative for TMT, possibly due to the growth of online or platform-based collaboration in this industry segment.

### Top five organizational imperatives related to EERM by industry







- ⏪ Home
- 🗨️ Foreword
- 📄 Executive summary
- 📈 01 Inherent risk and maturity
- 💰 02 Business case and investment
- 🌐 03 Centralized control
- 🔧 04 Technology platforms
- 🏢 05 Sub-contractor risk
- 📋 06 Organizational imperatives and accountability
- 👤 About the authors
- 👤 Contacts

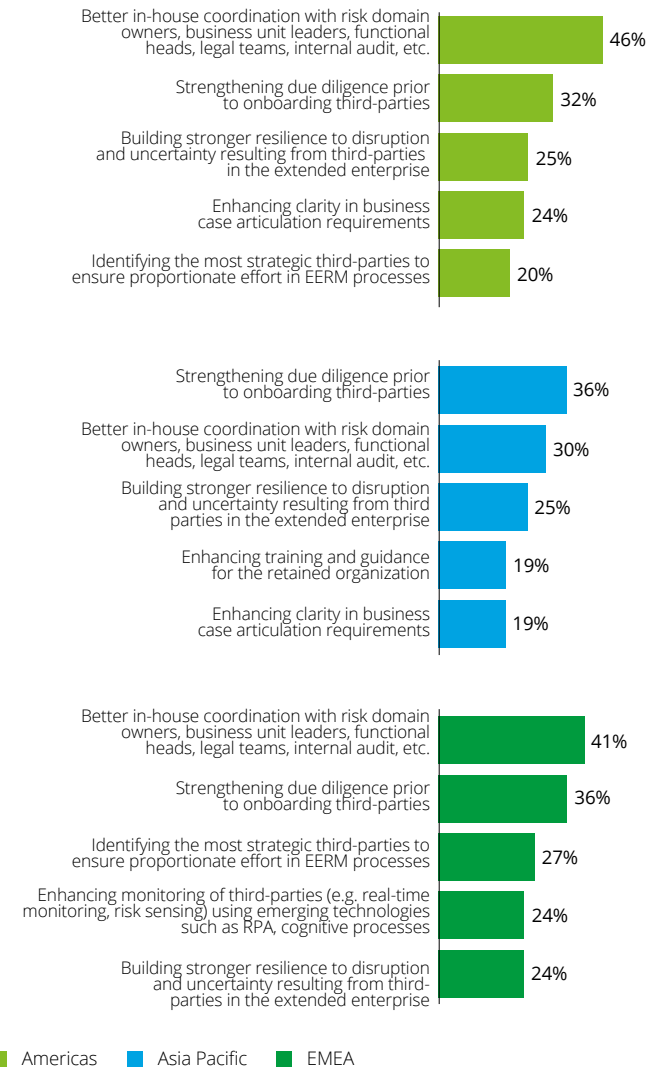


### Geography highlights

Regional analysis of top organizational imperatives related to EERM also indicate the need to build better in-house coordination with risk domain owners, business unit leaders, functional heads, legal, and internal audit teams, etc. as a common imperative across all the key regions, followed by the need to strengthen due diligence prior to onboarding third-parties and the need for strengthening resilience over disruption and uncertainty arising from the extended enterprise. Additionally:

- Respondents from the Americas are focused on the need to articulate better business cases for investment in EERM and identifying the most strategic third-parties for proportionate EERM effort.
- Respondents from Asia Pacific share the Americas’ need to articulate better business cases for EERM and additionally enhance training and guidance for their retained organization.
- Respondents from EMEA share a common priority to identify the most strategic third-parties for proportionate EERM effort, but are also focused on enhancing real-time monitoring of third-parties using emerging technologies.

### Top five organizational imperatives related to EERM by region





-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  02 Business case and investment
-  03 Centralized control
-  04 Technology platforms
-  05 Sub-contractor risk
-  06 Organizational imperatives and accountability
-  About the authors
-  Contacts

## About the authors



**Kristian Park**  
**EMEA Leader, Extended Enterprise Risk Management**  
 Global Risk Advisory

**Kristian Park** leads the Extended Enterprise Risk Management team in the EMEA region, as well as leads Deloitte’s Global Third-party Risk Management (TPRM) 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 risks, looking at both process and technology solutions; performs inspections of third-party business partners on his client’s behalf; and assesses third-party compliance with contractual terms and conditions.

In addition, Kristian is responsible for Deloitte UK’s Software Asset Management and Software Licensing teams and assists clients in managing their software licensing obligations—driving efficiencies and savings. He has experience across a broad variety of industry sectors including Life Sciences, Financial Services, Energy & Resources, Sport, Technology, Media, and Consumer & Industrial Products.



**Danny Griffiths**  
**Director, Extended Enterprise Risk Management**  
 Deloitte LLP

**Danny Griffiths** is a Director in our London based EERM team. He has 11 years of experience providing assurance and advisory services to his clients in the area of third-party risk. Danny leads the Third-party Advisory (TPA) proposition within our UK EERM team, and specializes in supporting clients in the development of Third-party Governance & Risk Management frameworks. He has worked extensively in the Financial Services sector in this regard as well as advising organizations across many of the other industry sectors and he regularly hosts roundtables and presents at forums on this topic.

In addition, Danny has significant experience leading compliance programs for large national and multi-national organizations, assessing third-party compliance against contractual obligations. Danny has led inspections across a range of third-parties including suppliers, outsourcers, marketing agencies, distributors, resellers, and licensees. He has practical experience working in a broad range of industries including Financial Services, Technology & Media, Consumer Business, Sports Business, Energy & Utilities, Real Estate, and Public Sector. He has led projects in multiple jurisdictions within EMEA, the Americas, and Asia.



-  Home
-  Foreword
-  Executive summary
-  01 Inherent risk and maturity
-  02 Business case and investment
-  03 Centralized control
-  04 Technology platforms
-  05 Sub-contractor risk
-  06 Organizational imperatives and accountability
-  About the authors
-  Contacts



**Mark Bethell**  
**Director, Extended Enterprise Risk Management**  
 Deloitte LLP

**Mark Bethell** is a Director in the UK EERM practice. Mark re-joined Deloitte in June 2015 having spent 4 years working in industry at a global oil major. While at the oil major Mark led the design and implementation of a global risk management framework designed specifically for joint ventures operated by others. Mark's other roles at the major 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 non-joint ventures).

Since returning to Deloitte, Mark has led a number of projects to help clients, across multiple 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 has a particular focus on implementing EERM Managed Services for his clients and the ongoing development of technologies to support in automated risk screening and monitoring.



**Sanjoy Sen**  
**Doctoral Research Scholar**  
 Aston Business School

**Sanjoy Sen** is the Head of Research and Eminence for EERM at Deloitte LLP, based in the UK. He is a Chartered Accountant (FCA), a Cost and Management Accountant, and a Certified Information Systems Auditor (CISA) with over 29 years of experience, which includes 17 years of partner-level experience at Deloitte and another competing Big 4 firm.

Sanjoy is currently enhancing his experience in strategic governance and risk management around outsourcing and shared services through a Doctoral Research Scholarship at Aston Business School, Birmingham, while continuing to provide professional advice to Boards, senior leadership, Heads of Risk, and Internal Audit. His ongoing research has been published globally through various academic and professional channels with over 200 citations in frontline newspapers, professional journals, and conference papers since 2014 in addition to co-authorship with Deloitte's global EERM leaders.

His prior experience in strategic governance and risk management of the extended enterprise, outsourcing, and shared services spans the UK, Gibraltar, India, and various countries in the Middle East. This includes assisting clients in strengthening their business strategy frameworks through effective strategic outsourcing and shared services initiatives through a combination of risk advisory and internal audit roles in client engagements.



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts

## Contacts

### Global EERM 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 Abisor	+33 1 58 37 94 03	gabisor@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	Dean Chivers	+27 1180 51159	dechivers@deloitte.co.za
Spain	Oscar Martín	+34 914432660	omartinmoredada@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 Arab Emirates	Huzaiifa Hussain	+97 1043 7688 88	HuzHussain@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	Sachin Paranjape	+91 22 6185 4903	sapananjape@deloitte.com
Japan	Masahiko Matt Sugiyama	+81 9098 09 6885	masahiko.sugiyama@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	Patricia Muricy	+55 21 3981 0526	pmuricy@deloitte.com
Canada	Nathan Spitse	+141 687 433 38	nspitse@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



Home



Foreword



Executive summary



01 Inherent risk and maturity



02 Business case and investment



03 Centralized control



04 Technology platforms



05 Sub-contractor risk



06 Organizational imperatives and accountability



About the authors



Contacts

## End notes

1. In preparing our report, we have considered both fully as well as partially completed survey responses (to the extent survey questions have been answered by these respondents). However, the increased proportion of respondents from regions where levels of understanding and organizational maturity in third-party risk is starting to increase, compared to more mature territories, has limited our ability to compare current results with last year's survey in some cases.
2. Industry segments covered by the survey include Financial Services (FS), Energy & Resources (E&R), Public Sector (PS), Technology, Media and Telecommunications (TMT), Consumer and Industrial Products (C&IP), Life Sciences & Health care (LSHC), and others. Other industries relates to survey responses where the respondent did not indicate the nature of their industry or did so ambiguously.
3. Figures set out on page 7 relate to centralized spending on EERM as estimated by respondents. Some respondents have indicated that their organizations may be spending significantly higher amounts related to EERM, given the decentralized nature of spend and activity.
4. This model presents a hybrid of various characteristics of centralized and decentralized structures combining the benefits of some standardization and centralized planning with (decentralized) local leadership and some flexibility.
5. Also referred to as community models.
6. This typically operates with a centralized in-house specialist pool supported by representatives from this pool co-located geographically across multiple "hubs" to support business/departmental functions or regions within its purview on EERM-related issues.
7. Nearly three out of four respondents had experienced a third-party related disruptive incident in the last three years as per our Global EERM Survey, 2017.
8. Excluding Australia and New Zealand from where we also had a very limited participation in this survey.
9. Also referred to as community models.
10. The Business Dictionary defines an infomediary as an information intermediary, typically a trusted third-party provider of information or advice on selection of goods or services, competitor information or research data (also called knowledge broker).

# Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 264,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2018. For information, contact Deloitte Touche Tohmatsu Limited.

Designed and produced by The Creative Studio at Deloitte, London. J14519