UK FINANCE

# THIRD-PARTY RISK MANAGEMENT

## Keeping control in a rapidly changing world

April 2019

EY
Building a better working world

## UK Finance

UK Finance is the collective voice for the banking and finance industry.

Representing more than 250 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

We work for and on behalf of our members to promote a safe, transparent and innovative banking and finance industry. We offer research, policy expertise, thought leadership and advocacy in support of our work. We provide a single voice for a diverse and competitive industry. Our operational activity enhances members' own services in situations where collective industry action adds value.

Contacts

**Dan Crisp**
Director, Digital, Technology & Cyber
Dan.Crisp@ukfinance.org.uk

**Ian Burgess**
Principal, Head of Cyber Policy
Ian.Burgess@ukfinance.org.uk

## EY – Financial Services

When the financial services industry works well, it creates growth, prosperity and peace of mind for hundreds of millions of people. No other industry touches so many lives or shapes so many futures.

At EY Financial Services, we share a single focus — to build a better financial services industry, not just for now, but for the future.

We train and nurture inclusive teams to develop minds that can transform, shape and innovate financial services. EY professionals come together from different backgrounds and walks of life to apply their skills and insights to ask better questions. It's these better questions that lead to better answers, benefitting EY clients, their clients and the wider community. Our minds are made to protect a better financial services industry. It's how we play our part in building a better working world.

ey.com/ukfs

Contacts

**Kanika Seth**
Partner, EMEIA Third-Party Risk Management Solution Leader, EY
kseth@uk.ey.com

**Tynan Beresford-Wylie**
Senior Manager, Banking and Capital Markets, EY
tberesfordwylie@uk.ey.com

**James Gower**
Senior Manager, Third-Party Risk Management, EY
jgower@uk.ey.com

**John Tenerowicz**
Senior Consultant, Technology Risk, EY
jtenerowicz@uk.ey.com

# TABLE OF CONTENTS

**Foreword** 2

**Introduction to third-party risk management** 3

**Regulatory expectations** 4

European Banking Authority's consultation paper on outsourcing arrangements 4

Operational resilience 5

**Challenges in the marketplace** 6

Regulatory changes 7

Third-party populations 8

Operating models 9

Fourth-party management 11

Oversight and governance 12

**Predictions for the future** 13

Industry alliances 14

**Conclusion** 16

**Contributors** 17

# FOREWORD

**Dan Crisp**
Director, Digital, Technology & Cyber,
UK Finance

**Kanika Seth**
Partner,
EMEIA Third-Party Risk Management
Solution Leader, Ernst and Young LLP

## THIRD-PARTY RISK MANAGEMENT KEEPING CONTROL IN A RAPIDLY CHANGING WORLD

Third parties play an important role in the financial services sector. Given the complexity of their operations, organisations are typically unable to provide all required service and business operations themselves on an in-house basis. Or at least they may not be able to do so to the high standards that a third party, which is able to concentrate solely on a small number of services, can provide. With the rapid emergence of new technologies aligned with greater customer expectations, the need for third parties continues to increase.

Given the importance placed upon third parties, it is no surprise that they are increasingly relied upon to provide critical components of a financial institution's range of services. However, with this reliance comes added risk to an organisation given the shared responsibility for services and transfer of data. As a result, there is an increasing need for oversight and governance of third parties to manage those risks and, where it is deemed appropriate, to mitigate them as far as possible.

The risks to organisations of not managing their third parties properly could include a loss of customer data or the inability to process customer payments, amongst many others. The implications for customers who have placed their trust in any financial institution is significant and the potential harm that could arise from such an incident should not be downplayed.

Any organisation affected in such a way should expect significant reputational damage and, where organisations are deemed to have been negligent, supervisory action by regulators. Such incidents do not necessarily follow on from an incident experienced by an organisation's third parties, but while the possibility exists, a robust third-party risk management function is crucial in managing an organisation's risk levels.

Moreover, the expectations from customers and regulators are that organisations are responsible for their third parties and that they cannot transfer the risk or, following an incident, culpability. With this in mind, organisations must be conscious that the performance of their third parties will directly reflect upon them. A service can be outsourced, but a risk cannot be. In order for each organisation to have confidence in their third parties they need to be managed correctly.

This paper will lay out some of the regulatory drivers that require organisations to manage their third parties and the associated challenges. It will also delve more deeply into what a 'good' third-party risk management function should look like and different approaches that organisations are taking, as a result of the increasing complexity that they are experiencing.

# Introduction to third-party risk management

**Third-Party Risk Management (TPRM) involves the oversight function of key service providers that contribute to the operations of a separate entity. These third parties may have access to data owned either by the primary organisation or its clients, which exposes both parties to confidentiality, integrity, and availability risks. Therefore, many organisations maintain an inventory of third parties and the services they provide, along with a method for assessing the criticality of these third parties based on the inherent risks of sharing data.**

Once a population of critical third parties has been established, organisations are able to begin assessing these third parties based on the services they provide, and the nature of the data shared between organisations. These assessments often take the form of on-site or remote reviews using a pre-established list of questions relating to various domains including information security, business continuity and data privacy, as may be applicable to each third party. Once completed, organisations are able to identify risks to the confidentiality, integrity, or availability of the services provided by a third party, including risks to data held by them, and so they are able to incorporate these risks into their own risk register. These risks can then either be reduced or mitigated by the third party, or accepted by the primary organisation, leaving a residual risk which can be monitored and reviewed on an ongoing basis.

Regulators are taking an increasingly proactive role in managing third parties by encouraging primary organisations in the financial sector to maintain current inventories of their third parties and review the critical third parties regularly. There is also an increasing reliance on tools used to manage and monitor third-party relationships, as well as engaging external entities to outsource the third-party review process. The key industry trends and challenges are explored in later sections of this report.

# Regulatory expectations

## EUROPEAN BANKING AUTHORITY'S CONSULTATION PAPER ON OUTSOURCING ARRANGEMENTS

The European Banking Authority's (EBA) revised guidelines on outsourcing arrangements were published on 25 February 2019, and provide an insight into the risks of outsourcing, as well as suggested methods of understanding, addressing and minimising these risks. While the guidelines were written with a focus on supporting financial services organisations, the principles can be applied across industries to other sectors, given third-party risk can impact any organisation regardless of the nature of the business.

Along with an underlying theme of building 'trust' in the financial sector, the guidelines focus on a number of key themes around the risks associated with outsourcing arrangements, as well as how to understand and manage these, including:

- Concentration risk, which is becoming an increasing concern as third parties develop bespoke service offerings and dominate within these areas
- Proportionality of an organisation's governance arrangements based on the nature, scale and complexity of its activities
- Scoping considerations that assess the service provider's criticality and importance to the primary organisation, including how to standardise these assessments across business functions, as well as the due diligence to be performed based on these assessments
- Intra-group outsourcing, and how it poses different risks to an organisation, including avoiding the assumption that intra-group outsourcing is less 'risky' overall given a typical assumption that entities within the same group will have similar control frameworks
- Arrangements for service organisations operating out of third countries, which require special considerations to help maintain organisational and operational standards required by the primary organisation

The guidelines also outline the fact that regulatory and customer requirements do not change when using third parties as part of the operating model, and that internal management is still responsible for maintaining appropriate controls and oversight over both the business functionalities and data flows, which need to be maintained at a standard in line with those legally required and industry recommended across Europe. It is recommended that the process outlined should be supported with a written policy specific to each individual organisation for reference and as a standard. There is also an emphasis on the role of internal audit functions within organisations to maintain an understanding and oversight of business practices performed by service organisations as part of their own service delivery model.

Documentation requirements for outsourcing arrangements are encouraged, including detail of the methods of service delivery, third-party on-boarding and off-boarding, and the controls to be put in place to meet business and regulatory expectations.

Overall, the EBA guidelines provide a strong basis for the areas of focus necessary to promote appropriate outsourcing arrangements, which largely align with the key focuses of this report.

# OPERATIONAL RESILIENCE

– **How confident are you that the service providers that you rely on are resilient enough to meet your needs?**
– **How engaged are you in understanding your ecosystem, putting joint plans in place with your service providers and testing them?**

The financial services sector has long been dependent on service providers, but recent evolutions in business models and advances in technology have only increased the extent and relative complexity of inter-dependencies. Third, fourth and even fifth parties can be crucial to the provision of critical business services, and many organisations only identify vulnerabilities and choke points in times of crisis. Increasingly complex and geographically diverse group structures, including service companies and a range of intra-group arrangements driven by structural reform or operating model decisions, mean that the challenge extends beyond the scope of traditional vendor management programmes.

Operational resilience is the ability of an organisation to anticipate, prepare for, respond and adapt to change and sudden disruptions in order to survive and prosper. Strategies to achieve this require a holistic and integrated approach, considering not just the operational infrastructure but also people, policies and processes.

Understanding dependencies between parties that support critical business services is crucial to identifying concentration risk, single points of failure and gaps in response and recovery capabilities. Furthermore, establishing strong contracts including service level agreements, robust monitoring, and oversight of the resilience capabilities of third parties is crucial in identifying weaknesses throughout the supply chain.

Given the increasing complexity of service provision and the number of parties in any given chain of service provision, many organisations are going beyond understanding the capabilities of individual service providers and testing end-to-end incident response and continuity arrangements. These tests often identify challenges relating to information sharing and coordination between organisations during a crisis, to the detriment of recovery times as well as to consumers and markets. The executive committee and board of directors of an organisation need to understand how their firm has factored in third and fourth party risk and what future plans are in place to improve the organisation's understanding and reduce the risk of a failure causing a critical outage of their own. Further, deeper scrutiny on operational resilience is ahead for the industry, with both the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) focusing heavily on this topic, as demonstrated by the recent joint discussion paper 'Building the UK financial sector's operational resilience'. The discussion paper specifically refers to the increased risk from engaging with third parties and the need for board and senior management oversight of this risk. The paper emphasises that risk increases with the number and complexity of third parties and that organisations are responsible for mapping critical services supporting critical functions, whether these critical services are conducted by internal departments or third parties.

Organisations are likely to have a number of the required components in place already, including business continuity planning, disaster recovery and crisis management. However, this narrow approach is no longer sufficient. It is clear that a key challenge for organisations is the need to integrate these functions into a holistic approach, breaking down existing organisational and process silos.

# Challenges in the marketplace

There are a number of notable challenges associated with managing the risks resulting from using third parties to deliver business services common to organisations across the financial sector. Each organisation has developed their own programme to combat these challenges based on different values and risk considerations, but there is not a standard best-practice model available for organisations to draw upon or benchmark their programme against. Some of these key challenges are outlined below:

- Organisations may suffer from unclear roles and responsibilities. Operating models, interactions between stakeholders, and the roles and responsibilities associated with managing third-party risks may not be clearly defined. This may be exacerbated by inadequate change management, operating procedures and training amongst staff.
- There may be an incomplete or inconsistently applied inherent risk model. This model may not be consistently executed and information collected may not be accurate or complete. Risk models driving risk assessment and oversight activities may not be transparent or easy to understand.
- A lack of operational efficiency or effectiveness may restrict the risk management function. A risk-based approach may not be applied to the third-party base. Risk treatment protocols may be inconsistent across each third party, and high issue management volumes and redundancy increase assessment fatigue, preventing timely issue closure.
- There may be a lack of clarity around the third-party population. A sustainable approach for compiling and maintaining the "golden source" third-party master file may not be defined or sustainable. Non-traditional third parties can be difficult to proactively identify.
- Inadequate coverage across each risk domain may become embedded in the TPRM practice. TPRM activities conducted pre and post-contract may not cover all risk domains affected by the provision of this service, which may also change over time.
- Limited technology may further impede the accurate management of risks. Market available platforms can be costly to deploy and maintain and often may not have significantly improved the function. Multiple governance, risk, and control platforms across organisations can hinder streamlined reporting / issue management.
- It may also be difficult for organisations to keep pace with the ongoing requirements to manage third-party risks. Regulatory change, new technology and third-party events can be expensive to implement, monitor and remediate. Monitoring is comprised primarily of "one time at a specific time" routines across third parties.

However, organisations can aim to mitigate these challenges, building TPRM programmes which address the following questions:

- Does the risk model and resulting monitoring ensure that TPRM routines are risk based and focused on risk mitigation?
- Is the business aware of third-party risks and those considered critical to the organisation?
- Are continuous monitoring tools being utilised to provide real time risk metrics on high risk and critical third parties?
- Are new regulatory requirements relatively easy to incorporate into the function?
- Does TPRM data provide a complete and consistently accurate view of the function?
- Is governance and oversight sufficiently advanced to demonstrate that the function has "teeth"?
- Are synergies and cost savings being leveraged through industry utilities or third-party managed service solutions?

The next section of this report outlines how organisations may choose to mitigate the afore-mentioned challenges relating to TPRM, as well as trends across the financial sector industry and predictions for the future. However, it is worth noting that every organisation experiences unique challenges in creating their TPRM function, which may not all be common across the financial sector or explored within this paper.

# REGULATORY CHANGES

As noted in the overview of the EBA guidelines on outsourcing and, as a key component of the PRA/FCA discussion paper on operational resilience, third-party management is becoming an increasing area of focus for regulators, which encourages organisations to invest more time and resource into developing their TPRM function.

**Figure 1**, taken from the EY's Global financial services and key risk management survey 2018, shows the degree of focus both the regulatory bodies and the internal audit departments included in the survey had when reviewing the third-party management function within organisations. The results show that there is a disparity in the objectives of the external regulators and the internal audit programmes. The former appears to place heavier focus on the criticality of third parties, fourth-party oversight, cyber security, and consumer protection, while internal audit places more focus on inherent risks, oversight and governance, operating models, and the maintenance of the third-party inventory. However, there were some common themes for focus across both groups, indicating an industry-wide focus on certain areas including third-party criticality, oversight and governance, and cyber security.

**Figure 1**

| Most important areas of focus | Regulatory body | Internal audit |
|---|---|---|
| Inherent risk assessment | 15% | 21% |
| Onboarding activities | 8% | 13% |
| Enterprise-critical third parties | 29% | 15% |
| Oversight and governance | 42% | 70% |
| Fourth-party oversight | 12% | 6% |
| Operating models | 8% | 15% |
| Foreign-based third parties | 2% | 2% |
| Issues management and/or risk acceptance | 10% | 9% |
| Cybersecurity | 42% | 30% |
| Residential risk model | 0% | 2% |
| Maintenance of third-party inventory | 10% | 26% |
| Consumer protection | 8% | 2% |
| Privacy/confidentiality | 9% | 11% |
| Nontraditional third parties (eg., brokers, agents, financial intermediaries) | 4% | 2% |
| Our program has not yet been assessed by a regulatory body | 17% | 4% |

# THIRD-PARTY POPULATIONS

The first step in ensuring an effective TPRM strategy is to establish the full population of service organisations used by the primary organisation. This will likely involve input from each business unit/department in order to represent an accurate image of all the third parties used. There will also need to be a method for adding new third parties into the population, most likely through the procurement function within an organisation. The EY TRPM survey 2018 noted an increased use of third-party inventory tools, including procurement, compliance, and cloud-based tools in order to manage the population, and allow individuals to add additional third parties easily.

Once the full population of third parties has been established, an organisation then needs to implement a tiering mechanism to categorise these third parties based on the risks associated with using them. These risks can be specific to the organisation and are therefore open to interpretation, but usually include two key areas: the business impact of the third party exposing data to confidentiality, integrity, or availability concerns; and the business impact of the service organisation being unable to provide its contracted services in the short term. This categorisation of third parties is therefore based on the risks being shared with or transferred to the service organisation and considers themes of cyber security and resilience, given their increased focus across the financial sector.

A large number of third parties creates added complexities and can lead to increased risk for organisations that might have limited resources to manage their third parties. That could be one reason why there has been a reduction in the average number of third parties that an organisation uses. The number of surveyed organisations that engaged fewer than 10,000 service organisations increased from 58 per cent in 2015 to 80 per cent in 2018. Other factors an organisation may consider when evaluating its third parties in varying degrees are the inherent risks of services provided, strategic importance, and the delivery of customer-facing services.

Further, as organisations revise and update their tiering mechanisms, there has been a decrease in the number of third parties ranked in the top two tiers of their TPRM structure, which require the most detailed oversight and review process. **Figure 2** highlights this change in focus. The majority of organisations surveyed also stated that less than ten per cent of their third-party base ranked in the highest-risk tier, and less than 20 per cent in their second-highest tier. The reduction in the number of service organisations included within the TPRM programme allows organisations to focus more sharply on the third parties rated in the higher risk categories, allowing them to be assessed in more detail and monitored more closely.

**Figure 2**

| EY Survey Question | 2014 | 2018 |
|---|---|---|
| The number of third parties included in the TPRM programme is less than 25 per cent of the total third-party population | 47% | 68% |

# OPERATING MODELS

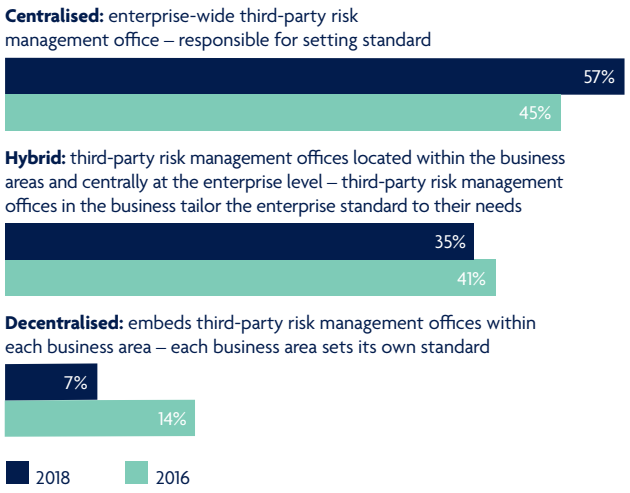
The operating model used to manage third parties, including the review process, can vary greatly between organisations, and there is no single best-practice example. Therefore, a variety of models have been developed to establish the risks exposed to the organisation through its relationship with each third party, and how these are reviewed, monitored, and resolved.

TPRM can sit under a number of different business units within an organisation, due to the nature of the work undertaken by third parties and the various departments feeding into and impacted by their use. The percentage of respondents to the EY TRPM survey 2018 who consider TPRM the responsibility of procurement, information security, operational risk, enterprise risk, and line of business departments is outlined below in **Figure 3**. This graph shows that the procurement department was most regularly assigned ultimate responsibility for TPRM. However, a number of organisations have begun associating TPRM directly with the business functions that leverage the services of these third parties. Organisations may choose to assign ownership of the programme to the procurement function, because it is best placed to add new organisations to the third-party inventory and encourage risk assessment when first entering into a relationship with a third party. However, it may not be the best team to flag the need for continual assessment and review, nor to understand the business operations and information security risks associated with these parties. Therefore, many operating models include inputs from each of the above-mentioned departments, as well as other interested groups, to manage the risks associated with engaging third parties.

**Figure 3**

Organisations may also choose to focus their TPRM efforts through a centralised, mixed or decentralised model based on their own internal structure and ethos. Amongst the organisations surveyed, there has been a trend towards incorporating more centralised models to manage third-party relationships, given the required input across business service lines. This method is designed to establish a standard review and management process across each third party and allows organisations to track common risks across third parties and identify any trends emerging that may require a response.

**Figure 4**




Overall, we expect to see a continued trend towards centralising third-party risk, though the ownership of this process may vary based on organisational needs and structure. However, multiple business units will need to continue feeding in to the third-party management process in order to understand the full scope of services provided, and the residual risks associated with maintaining these relationships.

# FOURTH-PARTY MANAGEMENT

Fourth parties are the organisations that provide services to support the operations of another organisation (the third party), which in turn provides services to the primary organisation. Therefore, these fourth parties may be directly supporting the services delivered to the primary organisation, exposing this organisation to service delivery risks. Through these services, fourth parties may also have access to data owned by the primary organisation, and any risks to this data while held by the fourth party remain the responsibility of the primary organisation, from both the regulators' and customers' perspectives. Therefore, the significance and risks associated with fourth parties are becoming of particular interest to organisations and regulators.

In the EY TRPM survey 2018, 83 per cent of organisations surveyed noted that they identify fourth parties, but of these, 60 per cent do not maintain a formal inventory of these fourth parties for monitoring and governance purposes. 78 per cent of organisations rely on the contractual terms established between themselves and the third party in order to manage fourth parties, while only 15 per cent perform independent assessments on critical fourth parties. This shows that a number of organisations are facing challenges in both identifying fourth parties and obtaining assurance over how these fourth parties operate. This is especially prevalent with smaller organisations, which may have less traction with their third and fourth parties to understand the scope of services being provided by fourth parties. There is also the risk that a third party may bring in a new fourth party to support its service delivery, without informing the primary organisation. To combat this, organisations are placing more reliance on direct oversight and monitoring controls in place between the third party and fourth party, encouraging the third parties to take a more proactive approach to managing their critical fourth parties. This approach means that these questions can be 'added on' to the existing risk assessment questionnaire and review process and allows organisations to focus on the 'critical' activities being provided by fourth parties.

In the future it is anticipated that organisations and regulators will continue to expand their focus on fourth party management, encouraging even greater pressure on both primary organisations (to establish inventories of fourth parties, and potentially independently assess the most critical of these), and on third parties (to implement and execute monitoring controls, including their own independent assessments, such as through a TPRM programme of their own). This is likely to be especially prevalent in the financial sector where concentration risks around third/fourth parties become increasingly critical. This issue is highlighted by the increasing use of private cloud hosting platforms, which are replacing traditional data centres. Currently just three private cloud providers account for over half the market share, and with high costs of entry to the market, this figure is unlikely to change soon.

# OVERSIGHT AND GOVERNANCE

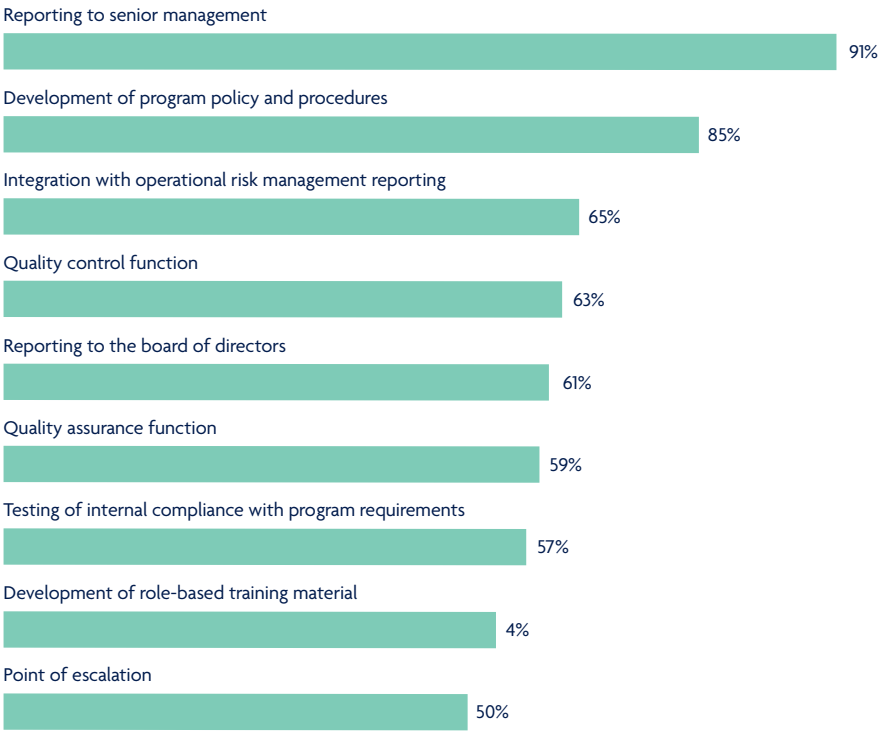
Over the last few years, there has been a steady shift towards more mature reporting and quality assurance of an organisation's TPRM programme. This has been reflected in the quality of assessments performed on third parties, which are reviewed regularly as part of the third-party lifecycle. However, for organisations who review their third parties on demand, and therefore carry out assessments less regularly, similar levels of increased maturity have not been seen. The following trends have also been noted:

- 81 per cent of organisations surveyed found that reporting on critical third parties could be done on demand. Reporting on other aspects of the third-party risk management programme may take upwards of a week
- Less than 25 per cent of organisations are reporting third-party breaches or incidents and significant issues to the board, while over 60 per cent report the same to senior management
- 83 per cent of organisations have a quality assurance function as of 2018, up from 72 per cent in 2017. As programmes mature, there has been an increased focus on quality assurance.

These statistics show that many organisations are still developing their TPRM programmes in line with industry trends, reaffirming the idea that a 'best-practice' model is still to be determined. As mentioned in the 'Third-Party Populations' section of this report, we expect to see a growing focus on spending resources on reviewing more critical third parties in greater detail, such as through the use of on-site assessments, with less consideration being given to less critical service organisations, which should reduce the pressures on quality assurance overall.

**Figure 5**, outlines the key activities performed to allow governance and oversight of the third-party risk management functions amongst the organisations surveyed. The graph highlights an emphasis on formal procedures such as developing a policy and integrating the activities with the operational risk teams, as well as reporting to senior management, and slightly less of a focus on quality controls and quality assurance of the programme, as well as reporting to the board level.

**Figure 5. Organisational oversight activities**



# Predictions for the future

Over the years, TPRM has become a greater part of an organisation's operating model as regulators increase scrutiny, customers raise expectations and technology advances at an unprecedented pace. Financial institutions need to account for how other companies use and protect their data and manage sustainable operations, especially for critical services.

Since 2013, following a shift in regulatory expectations for organisations to enhance their TPRM functionality, there has been an increased volume of onsite assessments being performed. Previously any identified issues and their associated remediation tracking had, in many cases, been performed on spreadsheets; now there appears a steady migration to technologies developed specifically to assist in managing third parties. Organisations also continue to enhance their methodologies to better scope, assess and prioritise risks arising from third parties. Maturity of thinking and enhanced programmes have enabled organisations to focus their resources and efforts on higher-risk third parties and specific risk areas. Organisations have also been seeking alliances, consortiums and managed services to further improve operational effectiveness and reduce costs. Cross-industry utilities look set to become an integral part of TPRM beyond 2019, as organisations seek cost reductions while enabling ongoing, effective monitoring of third parties.

# INDUSTRY ALLIANCES

## Market drivers for an industry utility

As organisations continue to enhance the methodologies used to understand the risks of third parties, an enhanced focus is developing on technology integration and board reporting capabilities.

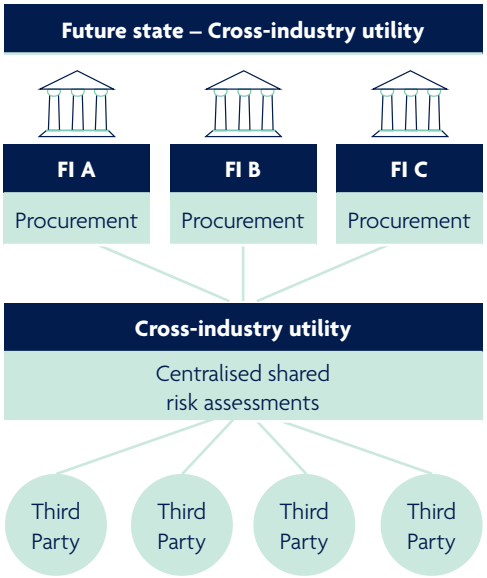
Risk governance requirements are routinely cited in new regulations, with significant focus on consumer compliance, cyber, enterprise resilience, and IT security related to third-party providers.

With the combination of the above, cross-industry utilities look set to become an integral part of TPRM beyond 2019, as organisations seek cost reductions while enabling ongoing, effective monitoring of third parties. From the EY TRPM survey 2018, nearly half of respondents have considered using an alliance or consortium to gain efficiencies.

The strong interest in industry alliances represents a new trend in the market. In the past, alliances have been attempted without success; however, there are now active alliances with varying structures and value propositions that have the support and resources of some of the most mature financial services organisations and service providers in the industry. These alliances have the potential to disrupt how the industry manages third-party risk.

## What is a market utility?

A market utility gathers and provides third-party assessment information using a proprietary methodology. Each institution uses the output to make its own informed risk decisions.



| Key features of a utility |
| --- |
| **People**<br>• Centralised and consistent risk assessment and language capabilities |
| **Process**<br>• Optimised alignment across the industry for third-party assessments<br>• Based around the principle of "done once, share multiple times"<br>• Could also be extended to perform customer services, including KYC, FATCA, CRS |
| **Technology and data**<br>• Real time, self-service views of risk profiles<br>• Provision of information to all stakeholders across financial institutions, third parties and customers<br>• Digital passport solution |

| Third party – benefits |
| --- |
| • Third-party digital passport making it easier to service their client base<br>• Reduced effort in completing due diligence assessments<br>• Market/sector benchmarking data (e.g. real time view of current market footprint) using advanced data analytics tools |
| **FS institutions – benefits** |
| • Cost saving and efficiencies through reduction of duplicated information gathering<br>• Timely access to a full suite of global risk and regulations including real time monitoring capabilities<br>• Large skilled pool of resources to meet unpredictable needs |
| **Regulators and government – benefits** |
| • Consistent documented auditable evidence of TPRM across financial institutions<br>• Market resilience – moving financial sector towards a market-leading TPRM practice |

A market utility will conduct assessments, typically covering:

- Collection and review of third-party responses with related evidence
- Validation of third-party responses through risk assessments
- Identification of observations and reporting.

## Case study – US market

Many consider the US market to be the most mature with regards to TPRM. In 2018, a consortium of five US institutions (Amex, Bank of America, BNY Mellon, J.P. Morgan Chase and Wells Fargo) formed an alliance to provide an end-to-end solution for third-party assessments using industry leading methodology. They established an independent entity – TruSight – to conduct the assessments.

TruSight was designed to combine the best practices from across the founding members to deliver a comprehensive third-party risk assessment service. It stores third-party data on a secure platform that financial institutions of all sizes can utilise to assess and manage relationships with third-party service providers. Each institution then uses the information to make its own vendor risk and engagement decisions.

# CONCLUSION

As outlined throughout the previous narrative, it is expected that the trend towards increasing the focus and quality of TPRM will continue to strengthen, alongside increased oversight and expectations from regulatory bodies. These enhanced risk management methods and regulatory scrutiny are also expected to be mirrored across other sectors and industries, eventually becoming common practice across any organisation.

TPRM is likely to become more integrated across business areas, including risk management, procurement, and operations and resilience. This integrated ownership approach is expected to further drive increased quality assurance work, especially around identifying the key third parties and the specific operational risks associated with the services they provide. Collaborations could also be seen across organisations as utilities become a more streamlined solution to managing third parties, with multiple clients using the same or similar solutions.

Above all, the trends in third-party risk are likely to mirror wider privacy and information security themes, with further regulations and industry/consumer expectations driving greater change and scrutiny.

Building a robust and inclusive TPRM framework is becoming an increasingly important priority across organisations, based on a comprehensive understanding of each organisation's reliance on third parties, and the services they provide.

# CONTRIBUTORS

## DAN CRISP
### Director, Digital, Technology & Cyber, UK Finance

Dan is the Director for Digital Technology & Cyber at UK Finance, overseeing policy initiatives including FinTech, cloud computing and data protection. Dan is also focused on projects to operationalise industry utilities for technology risk and E-ID.

Prior to joining UK Finance, Dan was the Chief Operations Officer for Barclays Global Information Security, primarily responsible for the technical integration of global acquisitions. Dan has also held various senior risk and compliance roles at JP Morgan and Citigroup. Most recently, Dan served as the Chief Technology Risk Officer for BNY Mellon where he led the innovation, development and deployment of global technology risk regulatory controls.

Dan is a board member for the Internet Security Alliance, a Non-Executive Director for Huntswood and a charter member of the Cloud Security Alliance metrics group. He is also a mentor at Level 39, Europe's largest FinTech accelerator and incubator.

Dan holds qualifications from the University of Memphis (US) and Stanford University (US). He has also completed the Strategic Management Program at Cambridge University (UK).

## IAN BURGESS
### Principal, Head of Cyber Policy, UK Finance

Ian is the head of Cyber Policy at UK Finance, primarily focused on operationalising the Financial Sector Cyber Collaboration Centre (FSCCC), an industry utility designed to promote cyber intelligence sharing amongst financial institutions and increase the cyber resilience of the whole sector. He also leads on cyber security regulatory or policy responses that impact UK financial services.

Most recently Ian was part of the BNY Mellon EMEA technology risk leadership team where he led on the development and deployment of a global system to map technology risk regulatory controls to global regulations. He also managed the redesign of the entire suite of technology risk metrics.

Prior to this, having commissioned from the Royal Military Academy Sandhurst, Ian served eight years as a British Army Officer managing complex strategic communications installations and providing leadership and communications training.

Ian holds a BA (Hons) degree in Business Studies from Coventry University, and is a certified Project Management Professional (PMP), Certified Information Security Manager (CISM) and Certified in Risk and Information Systems Controls (CRISC).

## KANIKA SETH

Partner,
EMEIA Third-Party Risk Management
Solution Leader, Ernst and Young LLP

Kanika is a Partner within the Financial Services Advisory practice at EY with more than 15 years experience in third-party management, operational resilience, information security, IT risk, regulatory change and data management. Kanika has led the delivery of third-party risk management methodologies, frameworks and related processes for a number of large global banks.

## TYNAN BERESFORD-WYLIE

Senior Manager,
Banking and Capital Markets, Ernst and Young LLP

Tynan is a Senior Manager in EY's Financial Services practice, with over 10 years' experience of delivering large scale, complex design, change and managed service programmes. Tynan is also the business development lead for EY's TPRM UK Utility proposition, working with UK Financial institutions, regulators and industry bodies

## JAMES GOWER

Senior Manager,
Third-Party Risk Management, Ernst and Young LLP

James has worked in EY's Cyber Security team for 8 years, focusing on Third-Party Risk Management. James oversees several global accounts for TPRM and is responsible for engagements which assess hundreds of third parties every year. James has also been involved in multiple TPRM Framework and Benchmarking reviews, and has been part of designing and implementing end-to-end Third-Party Risk Management solutions. James passionately facilitates training on TPRM both internally at EY, and with clients.

## JOHN TENEROWICZ

Senior Consultant,
Technology Risk, Ernst and Young LLP

John has worked in EY's Technology risk department for 3.5 years, working across risk assurance and third-party risk management engagements. In his TPRM work, he has been involved in both assessing third parties, as well as building out and maturing the processes for identifying and risk assessing both new and existing third parties. As well as designing the pathway for continual review and assessment in order to more effectively manage the associated risks.