Grant Thornton

An instinct for growth™

A guide to third party risk management

Delivering effective risk management and assurance over your third party relationships

Contents

Why is third party risk management an industry priority?

Firms in the UK increasingly rely on third parties to support their core activities, and in tough market conditions outsourcing can help businesses gain a competitive edge. While the use of third parties can offer a range of benefits, increasingly complex supply chains bring additional risk and the need to effectively manage these relationships has never been higher.

The increased reliance on third parties may improve performance and create efficiencies across many departments, from operations to finance to HR. However, it is important to note – firms who outsource business processes still own the associated operational risks and, where relevant, retain regulatory responsibility for that outsourced process.

Despite the reliance on third party relationships, a recent survey by Thomson Reuters found that participating global organisations conducted due diligence on just 62% of their third parties, suppliers and distributors. Additionally, 61% did not know the extent to which their third parties outsourced their work, and just 36% monitored the associated risks on an ongoing basis.

While many organisations may not be taking the risks seriously, regulatory and legislative bodies are. In 2015, the PRA issued a fine of over £1 million for a firm who failed to adequately oversee their third party arrangements. Although it was viewed as a high fine at the time, an increasingly complex regulatory landscape may lead to higher fines and serious punitive measures in the future.

Third party relationships are already monitored through legislation around Anti-Money Laundering, Anti-Bribery and Corruption, the Sarbanes-Oxley Act and the Financial Instruments and Exchange Act; but the introduction of the EU General Data Protection Regulation (GDPR) and the Senior Managers and Certification Regime (SM&CR) bring additional governance and conduct requirements.

To demonstrate this in real terms, a high profile telecoms data breach (due to a cyber-attack on a third party), resulted in a fine of £400,000 from the Information Commissioner's Office (ICO). However, under the GDPR a fine could have been much higher – up to an equivalent to 4% of their annual turnover, which for this organisation would have been £59 million. Similarly, the SM&CR allows some management activities to be outsourced, but the regulatory responsibility for that activity remains with the relevant Senior Manager – and they are personally accountable for it. Any issue that could have been addressed through a reasonable steps assessment by the regulators may result in fines, remuneration clawback or even a prison term.

Organisations should be able to demonstrate to their clients and regulators that they have an adequate framework in place to control and minimise risk from their third party relationships. Failure to do so may result in regulatory censure, fines and loss of confidence amongst partners and stakeholders.

Ravi Joshi
Managing Director

Understanding third party relationships

There are risks involved when collaborating with any third party. However, some activities carry a higher risk, are more prone to attack or offer a greater potential for fraud than others. With the rise of cloud computing and outsourced IT operations and processes, cyber security is a key area of risk within third party relationships. Organisations should also consider their contractual arrangements and due diligence procedures.

Key third parties

Cloud services

Payment services

Shared service centres

Other in-group entities

Everything as a Service (XaaS) – including software, infrastructure and platform as a service

Investment management and administration

Clients (from a due diligence, Know Your Customer and Anti-Money Laundering perspective)

Website management and recovery services

Ways in which service providers can work with user organisations

User organisations can work with service providers in several ways to provide their stakeholders with third party risk assurance:

- Using a strong contractual and legal framework
- Having a systematic risk assessment and monitoring process, and a proportionate level of control over third parties
- Agreeing detailed service level agreements
- Using internal auditors to test the effectiveness of the outsourced control environment
- Using a system to effectively oversee the third party risk management lifecycle, from pre-selection and due diligence, through to the end of the contract
- Obtaining a service auditor report from the outsourced service provider
- Completing an independent review of compliance with security, operational risk and privacy requirements
- Undertaking regular assessment over third party services in a risk based manner

What are third party relationships?

Third parties include clients, those in the supply chain or an outsourced service provider. Outsourced services may be delivered through an external organisation, or through another entity within the same group. Due to new requirements around ring-fencing and operational continuity, large banking groups are typically establishing global service companies of this nature to centralise shared services, which may then be accessed by all entities across the organisation.

How to mitigate the associated risks

Effective third party risk management consists of three key components, as outlined below. Organisations should establish an effective control framework, undertake adequate security assessments and offer assurance to senior management and other stakeholders through service auditor reports.

Third party operational risk reviews and establishing a third party risk framework

- Effective management of third party activities helps to minimise a company's risk exposure through its service providers
- Establish a framework to:
  - Increase process efficiency
  - Provide greater risk based coverage
  - Deliver more consistent ongoing monitoring procedures of critical third party relationships

Third party security assessments

- Third party IT assessments help to identify the risk, and possible impact, of any information loss through third party vendors
- Assess controls over powerful user accounts
- Assess third party security arrangements
- Undertake remote or onsite due diligence over third party services
- Undertake security assessments including:
  - User access management
  - Malware management
  - System and network vulnerabilities

Service auditor reports

- Help to identify improvement opportunities and undertake various third party audits of outsourced projects and operational contracts
- Produce reports aligned to established frameworks, such as ISAE 3402, AAF or SOC reports
- Produce tailored third party assurance reports focusing on key areas of risk

Creating a risk management framework

Many organisations are using third parties to provide functions that were previously deemed to be core activities. While this can be a cost effective and efficient strategy, it can also add a considerable degree of complexity to the design and implementation of the risk and controls framework. In addition, regulatory requirements from the OCC, FCA/PRA and other international regulators can be challenging.

With regulatory responsibility still falling to the user organisation, outsourcing raises the organisation's risk exposure on an ongoing basis and demonstrates the need for a robust third party risk management framework. Designing a framework that is fit for purpose can pose a significant challenge, particularly for organisations with a global footprint who work across a number of regulatory jurisdictions.

Third party operational risks reviews

Third party operational risk reviews assess an organisation's current state and help to identify gaps in the third party risk management framework. Typical issues faced by organisations include:

- Absence of a third party risk assessment framework to enable effective categorisation and management of suppliers
- Inadequately worded service provision or contractual obligations
- Ongoing service provisions where target service levels are not monitored or even measured
- Lack of contingency plans for the catastrophic failure of the third party or the services that they provide
- Poorly established system functional requirements leading to the non-delivery of a service contract
- Undefined SLAs for systems which are not adequately tested prior to going live
- Inadequate and untested arrangements for continuity of services
- Ineffective risk management of action or remediation plans for the third party services

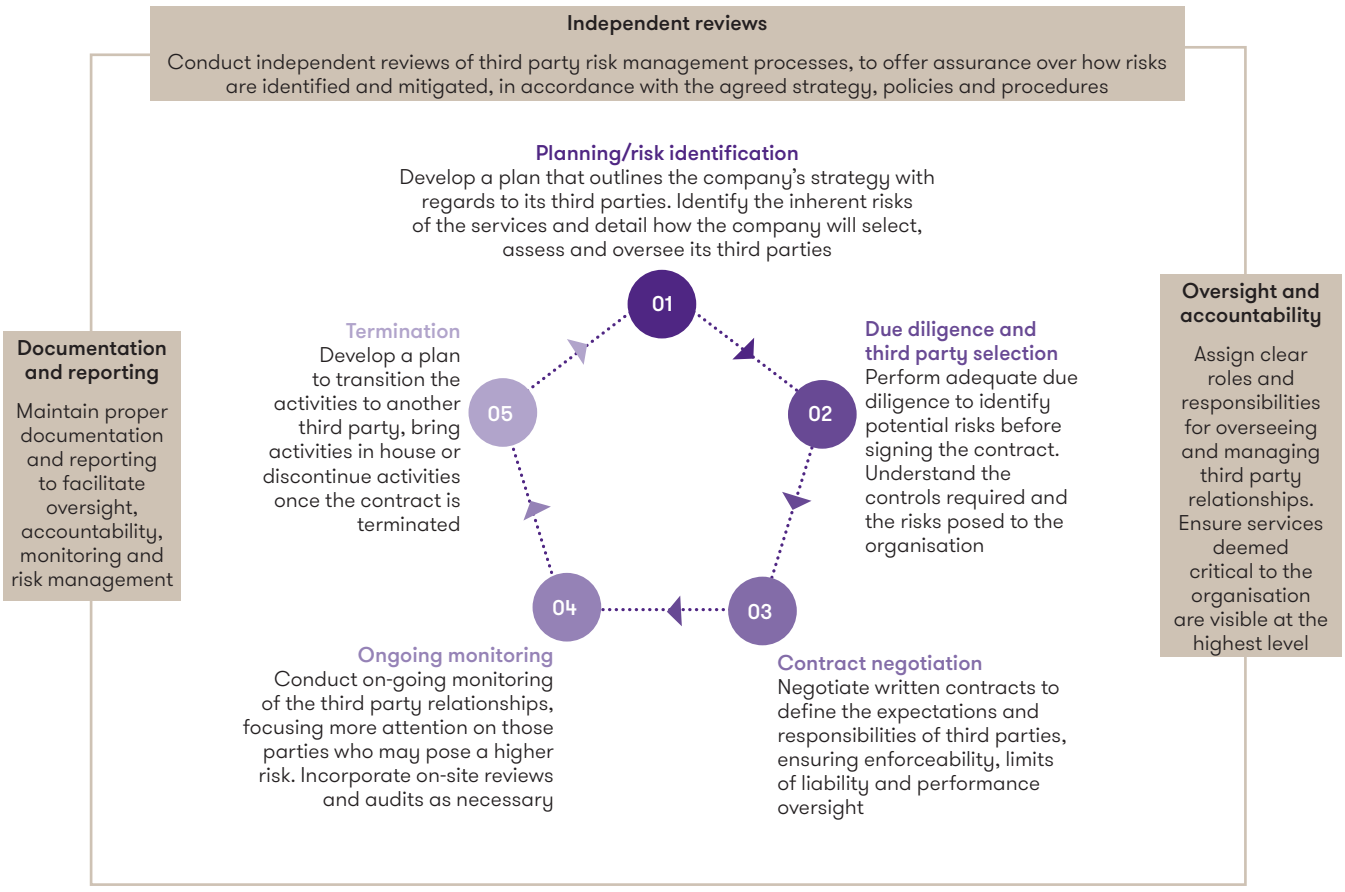
The assessment of third party risks across the financial services industry is inconsistent, costly, time consuming and often inaccurate. With no industry standard in place, firms define, measure and evaluate third party risk differently. Similarly, third party organisations are subject to multiple assessments from different user organisations to review their control environments. Not only does this create duplication of effort for third party organisations, but it is also expensive.

Case study

We were engaged to conduct third party risk management reviews for a leading European bank to provide assurance over critical IT services. The reviews revealed that the service provider was failing to maintain an effective service regime and comply with its service obligations. Our team were able to subsequently help the client with the design and methodology of an appropriate third party risk management programme, to offer more effective oversight over all of its critical suppliers and third parties.

Establishing an effective third party risk management framework

The findings from a third party risk review can form the foundation for an effective risk management framework. Organisations should consider third party risk in the context of their specific business activities and operational processes. The diagram below demonstrates a comprehensive approach to addressing third party risk management:



Key considerations

When designing their third party frameworks, organisations should consider the following:

- Appropriate selection of third parties
- Onboarding criteria
- Terms and conditions
- Fourth party considerations
- Oversight arrangements including reporting and metrics
- Resilience and contingency planning in the event of the failure of a third party
- Offboarding to enable a smooth transition of services
- Post relationship management to include any residual operational risks

Assessing security risks

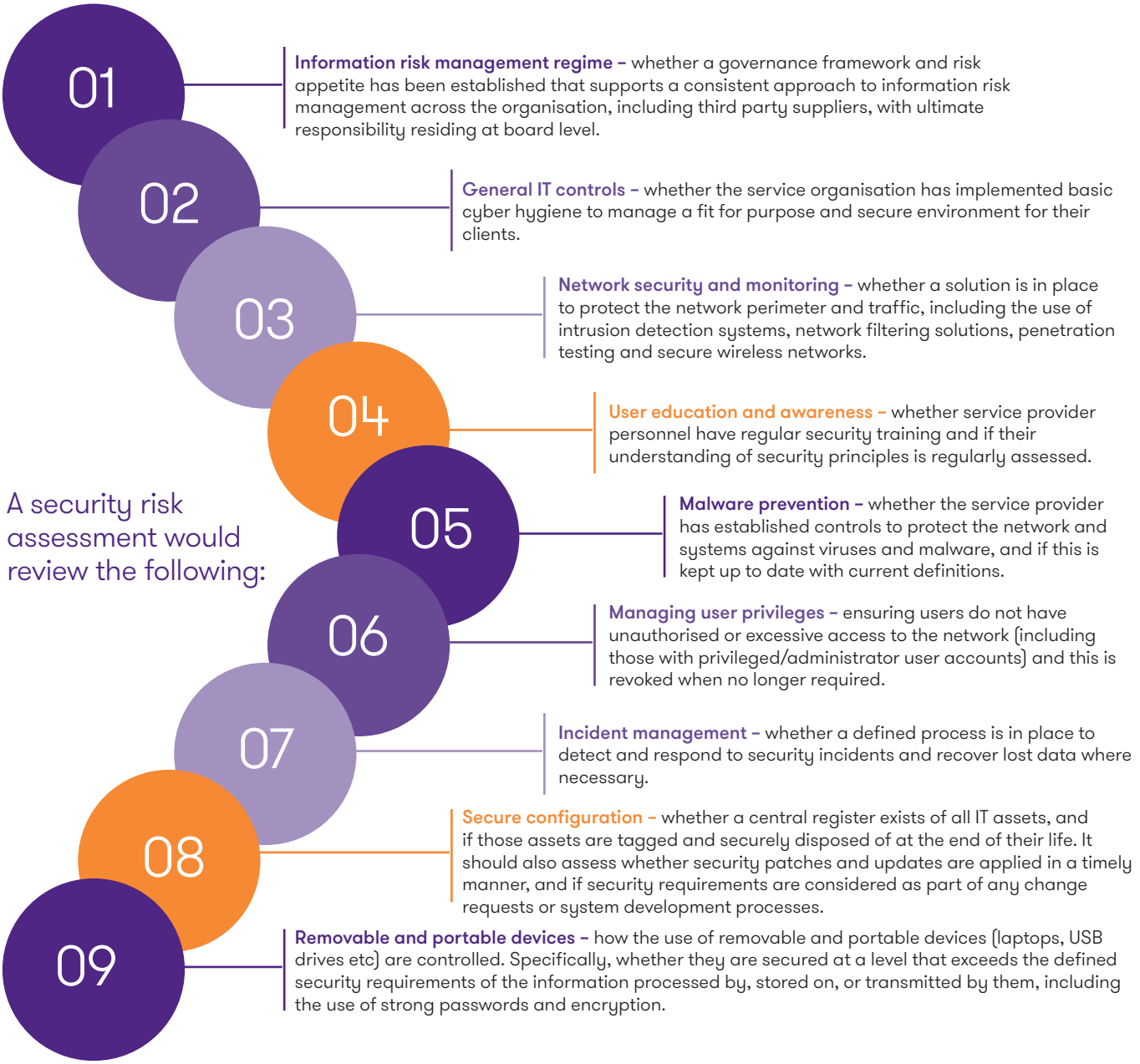
As businesses continue to embrace new technologies, supply chains are becoming increasingly integrated and may raise an organisation's operational risk profile on an ongoing basis. Innovations such as cloud computing, software as a service and mobile computing introduce new risks, which organisations must identify and effectively manage.

Organisations should strive to culturally embed an understanding of information and cyber security, and develop a mature control environment. As with all regulatory responsibilities, firms remain accountable for data shared with a third party, and are liable to fines from the ICO under the GDPR for any associated data breaches.

User organisations must also appreciate the risk of interrupted service provision due to a third party IT failure or a cyber incident. Third parties must have the necessary IT infrastructure and business resilience to deliver a consistent service, and to continue to fulfil their contractual obligations.

A security risk assessment can offer assurance over third party controls, in alignment with the government's National Cyber Security Centre's guidance.

A security risk assessment would review the following:



Information risk management regime – whether a governance framework and risk appetite has been established that supports a consistent approach to information risk management across the organisation, including third party suppliers, with ultimate responsibility residing at board level.

General IT controls – whether the service organisation has implemented basic cyber hygiene to manage a fit for purpose and secure environment for their clients.

Network security and monitoring – whether a solution is in place to protect the network perimeter and traffic, including the use of intrusion detection systems, network filtering solutions, penetration testing and secure wireless networks.

User education and awareness – whether service provider personnel have regular security training and if their understanding of security principles is regularly assessed.

Malware prevention – whether the service provider has established controls to protect the network and systems against viruses and malware, and if this is kept up to date with current definitions.

Managing user privileges – ensuring users do not have unauthorised or excessive access to the network (including those with privileged/administrator user accounts) and this is revoked when no longer required.

Incident management – whether a defined process is in place to detect and respond to security incidents and recover lost data where necessary.

Secure configuration – whether a central register exists of all IT assets, and if those assets are tagged and securely disposed of at the end of their life. It should also assess whether security patches and updates are applied in a timely manner, and if security requirements are considered as part of any change requests or system development processes.

Removable and portable devices – how the use of removable and portable devices (laptops, USB drives etc) are controlled. Specifically, whether they are secured at a level that exceeds the defined security requirements of the information processed by, stored on, or transmitted by them, including the use of strong passwords and encryption.

What if there is a breach?

Business continuity

While strong perimeter defences and effective controls are the basis of strong cyber security, they are not a guarantee against disruption of service. User organisations should review how resilient their third parties are in the event of a serious business disruption, including the following:

- Ensuring third parties have up to date and validated business continuity processes (checked through testing and exercising), IT disaster recovery and incident or crisis management arrangements in place
- Understanding how third parties will work with the user organisation during any cyber breach or other type of business disruption, and ensuring that they will continue to appropriately meet their clients' support requirements during such a situation
- Checking current systems comply with industry, regulatory and legal standards
- Ensuring third parties have ongoing programmes to stay up to date with business continuity processes and evolve their procedures accordingly

Case study

We have undertaken security assessments over several third party service providers for a leading FTSE 100 media organisation. We established a bespoke testing framework to meet specific client needs and undertook systematic testing for a given period, communicating findings to both the third party service provider and the user organisation.

Checking that controls are working effectively

Service auditor reports offer assurance over third parties and demonstrate that controls are operating effectively. There are several types of reports available and organisations must understand the differences between each reporting framework in order to select the appropriate reporting type.

The UK AAF and ITF frameworks, the International Standard, ISAE 3402 and the US SOC and SSAE frameworks are the most commonly used Service Auditor's Reports in the UK. Each report has its own merits and organisations should select the appropriate report based on the type of service delivered, the service provider and the user organisation's requirements.

Additional benefits of service auditor reports may include:

- Meeting Sarbanes-Oxley requirements associated with understanding the operating effectiveness of outsourced controls
- Providing comfort that controls are being exercised over data
- Providing assurance beyond the standard service level agreement
- Helping to identify process and technology weaknesses
- Identifying the controls at the client organisation that are necessary to complement those of the outsourced service provider

Case study

We have helped many clients in obtaining service auditor reports against the AAF, ISAE 3402, SOC and SSAE frameworks. For one FTSE 350 services client we initially held communications/understanding workshops to enhance awareness and communicate the implications of a service auditor report. We then facilitated identification of in-scope control objectives and associated control activities before performing a gap analysis. We have subsequently completed a number of Type 1 and Type 2 AAF reports in different parts of the client's business. We have also helped numerous clients migrate between different service auditor reporting standards, as they respond to their changing client needs.

How we can help

Grant Thornton UK LLP is part of one of the world's leading organisations of independent advisory, tax and audit firms. We help dynamic organisations unlock their potential for growth by providing meaningful, forward looking advice.

With an increased regulatory focus on third party risk, we understand the challenges faced by firms with complex supply chains. Our experts can support your team to establish a robust risk management framework, embed a greater understanding of third party risk and offer assurance over your existing controls.

Drawing on expertise covering business resilience, cyber security and data protection, we can support your business at every stage of the third party risk management lifecycle. Bringing insight of best practice from across the financial services sector, our experienced team offer pragmatic, proportionate advice in line with our clients' needs.

We can support your business through the following:

- Development/review of risk management frameworks
- Risk reviews of IT outsourcing projects
- Project reviews over outsourcing programmes
- Third party functional and IT performance audits
- Third party security and data privacy audits
- Conducting third party security assessments
- Undertaking service auditor reports in line with SSAE 16, AAF 01/06, ITF 01/07 and ISAE 3402 standards

For further information, please contact our team below:

Sandy Kumar
Head of Financial Services Group and Business Risk Services UK
T +44 (0)20 7865 2193
E sandy.kumar@uk.gt.com

Manu Sharma
Partner
Head of Cyber Security and Privacy
T +44 (0)20 7865 2406
E manu.sharma@uk.gt.com

Ravi Joshi
Technology Assurance Director
Business Risk Services
T +44 (0)20 7865 2571
E ravi.joshi@uk.gt.com

Grant Thornton
An instinct for growth™