WHITE PAPER

Best Practice in Third Party Risk Management

Ruleguard

Contents

Background

Third party risk management is top of the regulatory agenda.

It started with cyber risk management and the need to manage third party service providers. That initial concern increased to encompass a multitude of third party arrangements and has become a hot topic worldwide.

The regulatory message is that firms must consider the risk posed by third party relationships.

Regardless of whether a firm conducts activities itself or relies on another party, the firm remains accountable to the regulator. This point is one that supervisors worldwide are eager to stress.

Firms must have processes in place to appropriately manage and evaluate the risks associated with third party arrangements. Reliance upon third parties does not diminish a firm's regulatory obligations.

Ruleguard

What is Risk Management?

There is a basic requirement that all regulated firms must identify, assess and manage any risks to the business. How this requirement is interpreted varies widely from firm to firm.

Most firms will be familiar with the process of identifying and ranking risks according to the level of risk posed, but how many firms understand the links between that process and how it relates to their monitoring and audit processes? When the board reviews the reports from these reviews, do the senior managers understand how the findings relate back to the risks within the business?

The risk management process needs to be linked to a firm's strategy and raison d'être. It relies upon a robust governance process for setting standards of conduct and communications, both internal and external.

Key steps in Risk Management Framework

To be truly effective this process needs to be considered within individual departments to identify specific risks within each process and determine appropriate controls to mitigate any risks.

Given that the risk management framework supports the business to achieve its strategy, it's not surprising that firms have traditionally focused their attention internally. Aside from due diligence on potential suppliers, firms tend to forget about ongoing risk management of any third party arrangements.

What is a third party?

One simple definition of a third party relationship is that it generally excludes customers. It would include relationships such as:

- Suppliers - office facilities, storage facilities
- Contractors - ad hoc project managers or consultants
- Outsource providers - IT outsourcing providers, business process outsourcing providers, call centre providers, HR outsourcing providers
- Platform providers
- Fund management or administration
- Custodians
- Transfer agents
- Portfolio or investment management services
- Distribution agents

NB: any of the above could outsource or sub-contract to their own third parties. It also brings additional risk.

All these relationships add value by providing services which a firm is unable to fulfil themselves due to lack of skills, knowledge or resources. By using third parties, a firm might improve efficiencies and make cost savings.

Third Party Oversight

Given that firms need to identify and manage risks, it's important that a firm maintains a current list of all their third party relationships. Sadly, this is an oversight that the regulators have identified during its thematic reviews. The FCA's cross-sector survey from 2017-18 provides some context for consideration.

Cross-sector survey 2017/18

Issues at third parties included:

- IT failure in one important supplier accounted for 15% of incidents reported to the FCA.
- IT changes caused 20% of the operational incidents reported to the FCA
- 50% of firms do not have a comprehensive list of all third-parties with whom they do business and who have access to their systems and data
- 26% of firms did not have a board approved information security strategy
- Only 56% of firms said they could measure the effectiveness of their information asset controls

Source CP19/32

According to a supplier's individual risk profile, it's important that regular information is provided to boards to enable oversight and to inform decision-making.

For example, the proposals with Parliament to reform the audit and corporate governance standards in the UK. If these proposals are passed, the board will need to ensure that there are appropriate controls in place to prevent fraud. Auditors will consider these arrangements when undertaking the annual review.

Areas of Weakness

In order to implement appropriate controls, a firm needs to understand where risks could materialise and how to manage those risks.

Common weaknesses identified in third party risk management include:

- Lack of consistent approach
- Lack of common standards, instead firms manage providers on a case-bycase basis
- Lack of complete oversight frameworks

Additionally, firms tend to focus attention on selecting third parties and due diligence. This means that ongoing monitoring often receives less attention.

Oversight

(a) Board

A recurring regulatory message is that the board must have oversight of a firm's risk management framework. It's the board that sets the risk appetite within the firm's business strategy. Similarly, the board needs to decide where to invest its funds and resources to achieve its goals.

(b) Senior Manager

The board is also responsible for ensuring that a senior manager implements the agreed risk framework within the business. This includes ensuring:

- Risk policy and procedures that are documented and updated regularly
- Risk awareness to encourage the right corporate conduct that represents the firm's values
- Producing regular reports to the board on risk management both internally and externally
- Maintaining a risk register which includes risk owner attestations

What happens when it goes wrong?

Outsourcing helps firms become more efficient, but it also poses challenges, including an increase in regulatory action for breaches such as poor oversight.

FCA fines Aviva Pension Trustees UK Limited and Aviva Wrap UK Limited £8.2m for Client Money and Assets failings

Press Releases | First published: 05/10/2016 | Last updated: 03/11/2016

The Financial Conduct Authority (FCA) has today fined Aviva Pension Trustees UK Limited and Aviva Wrap UK Limited (together Aviva) £8,246,800 for failings in its oversight of its outsourced providers in relation to the protection of client assets.

FCA fines Charles Schwab UK £8.96 million over safeguarding and compliance failures

Press Releases | First published: 21/12/2020 | Last updated: 21/12/2020

The Financial Conduct Authority (FCA) has fined Charles Schwab UK Ltd (CSUK) £8.96 million for failing to adequately protect client assets, carrying out a regulated activity without permission and making a false statement to the FCA.

Customers affected by the breaches were all retail customers, who require the greatest level of protection.

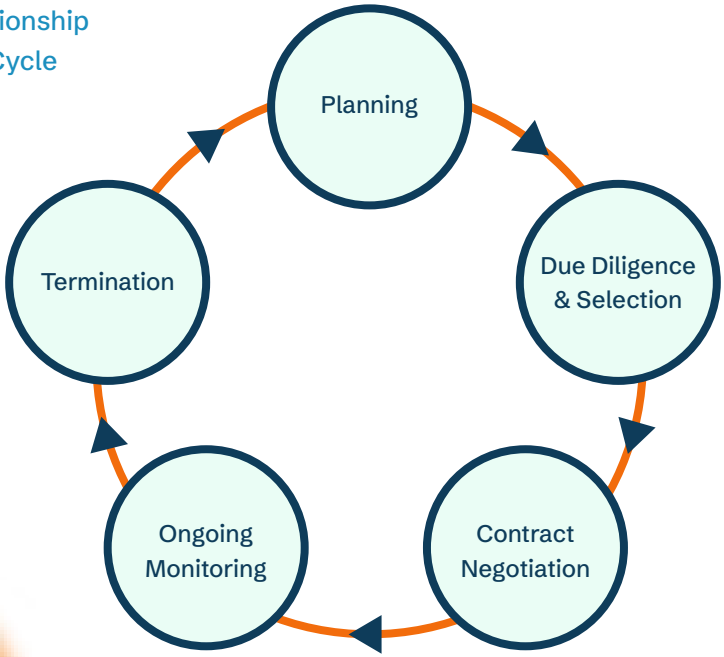
Mark Steward, Executive Director of Enforcement and Market Oversight at the FCA, said:

'Charles Schwab UK failed to get the correct permissions from the FCA; then failed to be open with us and, finally, failed to put in place the necessary safeguards to ensure, if required, there could be an orderly return of client assets.

Relationship Life Cycle

Effective third party risk management generally follows a continuous life cycle for all relationships and incorporates the following principles applicable to all stages of the life cycle:

Relationship Life Cycle



Steps for Success

The FCA's key priorities for 2022/23 are aligned to its Strategy.

1 DUE DILIGENCE

2 CONTRACT NEGOTIATION

3 ONGOING MONITORING

Due Diligence

Efficiencies and cost savings appeal to management, but when deciding to engage with a new supplier, what risks are considered?

Firms should review their due diligence processes to enable them to easily identify risks prior to engaging third party services.

1. Draft list of requirements
2. List of potential suppliers
3. Request due diligence information – how in-depth is this? Complete identity checks, but also understand the service provider's risk profile
4. Short list
5. Decision made – how is that decision made? Where in the process do you identify potential risks posed by each potential supplier and consider how you mitigate it?
6. Onboarding – not just initial checks, but ongoing, - how often do you monitor & review these relationships?
7. Own the relationship – a senior manager who has oversight of the relationship, reviews progress against the contract, service level agreement and metrics. Reporting to the board on the relationship and risks posed
8. Ongoing monitoring – third parties such as appointed representatives need greater oversight
9. Collate data from third parties about services provided – ensure that there is consistency in the information requested, including frequency and reporting periods
10. Implement an issues process for informing you when the third party has encountered a problem
11. Breaches – how quickly are they identified and escalated to ensure reporting on time.

Contract Negotiation

When discussing contractual arrangements, firms should ensure that risk management including reporting and escalation processes are included.

The contract should also outline responsibilities for the firm and the third parties (including any sub-contractors).

Sub-Contractors

Sub-contractors can pose additional risk. Often firms may be unaware of the underlying relationships or dependencies which a service provider has.

Firms should capture information relating to sub-contractors during the diligence and selection process. Early identification of such relationships aids decision-making.

Foreign-based Third Parties

Firms should understand that contracts may be subject to the interpretation of foreign courts relying on local laws. It is important to seek legal advice to confirm the enforceability of all aspects of a a proposed contract with an overseas third party and other legal ramifications of each such business arrangement, including privacy laws and cross-border flow of information.

Ongoing Monitoring

To assure the board that its risks are managed, the firm should have a monitoring programme that undertakes periodic reviews. The focus should be on how the firm delivers its services. How might you achieve this? What information do you need from the third parties and any sub-contractors?

This requires consistent reporting from all third parties on agreed key metrics. This information needs to be delivered at specific times. The accuracy of that data needs to be tested periodically to verify the data and provide assurance to the board. Firms require timely and accurate reporting.

(a) Risk Management:

- Evaluate the effectiveness of the third party's own risk management, including policies, processes, and internal controls.
- Consider whether the third party's risk management processes align with your firm's policies and expectations surrounding the activity.
- Assess the third party's change management processes, including clear roles, responsibilities, and segregation of duties are in place.
- Where applicable, determine whether the third party's internal audit function independently and effectively tests and reports on the third party's internal controls.
- Evaluate processes for escalating, remediating, and holding management accountable for concerns identified during audits or other independent tests.

(b) Incident Reporting and Management Programs:

- Review and consider the third party's incident reporting and management programs to ensure there are clearly documented processes, timelines, and accountability for identifying, reporting, investigating, and escalating incidents.
- Confirm that the third party's escalation and notification processes meet the firm's expectations and regulatory requirements.

(c) Complaints Handling:

- Ensure the contract includes responsibilities and provisions for assisting in complaint investigations. Access to data and reporting on such matters should be provided to the firm.

Operational Resilience

Assess the third party's ability to deliver operations through a disruption from any hazard with effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.

Assess options to employ if a third party's ability to deliver operations is impaired.

Termination

The contract needs to have termination clauses, but also needs to have realistic timeframes to enable a collaborative handover to a new party.

Where permitted, include reporting requirements on complaints, identified risks and emerging risks; termination rights should include sub-contractor arrangements.

Conclusion

Third party risk management processes need to be appropriate to size and scale of firm, but also the complexity and level of risk posed.

We see regulators encouraging firms to use technology to improve efficiencies, reduce costs and aid risk management.

Ruleguard's Supplier Oversight Solution

Ruleguard for Supplier Oversight takes the core benefit of the Ruleguard platform – powerful rules-mapping and evidencing – and uses it to bridge the gap between a firm and its third parties.

Ruleguard provides a seamless control environment between you and your transfer agents and administrators for genuine oversight.

Any information maintained within the Ruleguard system can be selectively shared with others. Control and process documentation, along with all relevant mapping links to rules and regulatory frameworks, can be provided at the touch of a button.

As information changes over time, differences are automatically highlighted to ensure that up-to-date records are being maintained.

Ruleguard allows you to map received information into your own data, letting you incorporate third party regulatory information into your own risk or monitoring frameworks. For example, you can generate and automatically maintain compliance documents that reference third party controls – clearly labelled with the provider that operates them – within your account.

This can radically transform the third party oversight capabilities of a compliance function and allow it to extend best practice beyond the borders of the firm.

Why Ruleguard?

Ruleguard is an end-to-end GRC software platform designed to help regulated firms manage the burden of evidencing and monitoring compliance. It has a range of tools to help firms fulfil their obligations across the UK, Europe and APAC regions.

An ever-changing regulatory environment requires firms to identify the changes impacting their business and to adapt their processes and controls quickly to meet those requirements. It can be time consuming and overwhelming to be constantly monitoring rule changes from various supervisory bodies both in the UK and internationally. Senior Management require evidence to demonstrate that business risks are being managed effectively. Collating data from various sources to generate timely management information, enable decision making and facilitate oversight is a key requirement.

Ruleguard has been designed to help you demonstrate and evidence compliance, by using its comprehensive rules-mapping, risk and control tools, automated reporting features and powerful dashboards. At its core, Ruleguard is a single unifying solution for all your compliance processes and procedures for managing your ongoing compliance.

Our SaaS-delivered software platform, Ruleguard, has been designed to manage the complex and burdensome issues associated with regulatory compliance, especially when processes and procedures in place are manual and fragmented widely across multiple companies, departments and systems.

Using Ruleguard will enable you to show regulators and auditors how your business has complied with the rules, including providing effective governance and oversight to your firm.

About Ruleguard

Ruleguard started out in 2013 as a software ‘design and build’ agency that specialised in financial services projects, particularly those with a unique requirement for data and functionality that was far from being available ‘off the shelf’.

Fast-forward to 2024 and we have established Ruleguard as one of the foremost offerings in the RegTech space, providing genuine compliance oversight to some of the largest and most complex financial institutions globally.

Most importantly, we continue to work closely with our clients to identify the most painful aspects of compliance oversight and strive to build-out our platform to improve that governance with increased efficiency and reduced cost.

Ruleguard

Get in touch!

0800 408 3845

marketing@ruleguard.com

www.ruleguard.com

Key points of contact

Priscilla Gaudoin

Head of Risk & Compliance

Priscilla.Gaudoin@ruleguard.com

Ed Buckman

Director of Commercial Strategy

Ed.Buckman@ruleguard.com

Matthew Bruce

Platform Director

Matthew.Bruce@ruleguard.com

BOOK A DISCOVERY CALL →

Ruleguard

Disclaimer:

This document is intended for general information purposes only and does not take into account the reader's specific circumstances and may not reflect the most current developments.

Ruleguard disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Ruleguard does not provide legal, regulatory, audit or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

Copyright © 2024 Ruleguard. All Rights Reserved.

Ruleguard 2024
WP-Oct-2024