Customer Due Diligence & Third-Party Assurance Guide

Supporting Supplier Risk Management, Regulatory Compliance and Enterprise Procurement

Table of Contents

Introduction

Third-party risk management has become a board-level priority for organisations operating in regulated and high-risk environments. Financial institutions, fintechs, government agencies and multinational enterprises are increasingly expected to demonstrate that suppliers are subject to appropriate oversight, governance and assurance.

Regulators now expect organisations to understand not only the services their suppliers provide, but also the risks those suppliers introduce. As a result, supplier due diligence has evolved beyond simple questionnaires into comprehensive assessments covering governance, privacy, security, operational resilience and regulatory compliance.

At 1datapipe, we recognise that enterprise customers require transparency, evidence and accountability when evaluating suppliers. This guide explains how we support customer due diligence activities and provide assurance regarding our governance framework, operational controls and compliance programme.

Understanding Supplier Assurance

Supplier assurance is the process through which organisations gain confidence that a third party can deliver services safely, securely and in compliance with applicable legal and regulatory requirements.

For many regulated organisations, supplier assurance is no longer optional.

Regulators increasingly expect organisations to demonstrate:

- Effective third-party risk management
- Ongoing supplier oversight
- Appropriate governance controls
- Information security assurance
- Operational resilience considerations
- Compliance with privacy requirements

The objective is to ensure that supplier relationships do not introduce unacceptable risks to customers, shareholders, employees or the wider market.

Our Approach to Customer Assurance

We view customer due diligence as an opportunity to demonstrate transparency and accountability.

Our approach is based on three principles:

Transparency

Customers should be able to understand how we operate, how decisions are made and what controls are in place to manage risk.

Evidence

Assertions alone are insufficient. Customers increasingly require documented evidence supporting governance, security and compliance claims.

Continuous Improvement

Assurance is not a one-time activity. Controls, processes and governance arrangements must evolve alongside changing regulatory requirements and customer expectations.

Governance Framework

Strong governance provides the foundation for effective assurance.

Governance responsibilities are clearly defined across key business functions, including:

- Compliance
- Regulatory oversight
- Data protection
- Information security
- Risk management
- Operations

This structure supports accountability and ensures that governance considerations are incorporated into operational decision-making.

Compliance, Regulatory and Data Protection Oversight

Compliance and privacy governance are embedded throughout our operating model.

Oversight activities include:

- Regulatory horizon scanning
- Privacy reviews
- Risk assessments
- Policy management
- Control monitoring
- Internal governance reporting

These activities help ensure that legal and regulatory obligations are identified, assessed and incorporated into operational processes.

Information Security Assurance

Information security remains a primary area of focus during supplier due diligence exercises.

Customers frequently seek assurance regarding:

- Security governance
- Access management
- Encryption controls
- Incident management
- Vulnerability management
- Employee awareness programmes

Security assurance activities support confidence that information assets are protected appropriately and that security risks are actively managed.

Operational Resilience

Regulators increasingly expect organisations to assess the resilience of critical suppliers.

Operational resilience focuses on an organisation's ability to continue delivering important services despite disruptive events.

Examples include:

- Cyber incidents
- Technology failures
- Supplier disruptions
- Human error
- External events

Our resilience activities are designed to support continuity, recovery and effective incident response.

Risk Management Framework

Risk management forms an integral part of our governance structure.

Risks are identified, assessed, managed and monitored through structured processes that support informed decision-making.

Risk assessments may consider:

- Regulatory risk
- Privacy risk
- Security risk
- Operational risk
- Third-party risk
- Reputational risk

This approach enables risks to be managed proportionately and consistently.

Documentation Available During Due Diligence

Enterprise customers often require access to supporting documentation as part of supplier evaluations.

Depending on customer requirements and confidentiality considerations, documentation may include:

Governance Documentation

- Governance summaries
- Organisational structures
- Policy frameworks
- Oversight arrangements

Privacy Documentation

- Privacy notices
- Data protection policies
- Data subject rights procedures
- DPIA summaries
- Legitimate Interest Assessment summaries

Security Documentation

- Information security policies
- Security overviews
- Incident response summaries
- Security governance information

Compliance Documentation

- Compliance programme summaries
- Regulatory monitoring processes
- Risk management frameworks
- Governance reporting structures

Supplier Management Documentation

- Due diligence processes
- Supplier onboarding controls
- Contractual governance arrangements

The availability of specific documentation may vary depending on contractual, legal and confidentiality requirements.

Supporting Procurement Teams

Procurement teams are often responsible for coordinating supplier reviews across multiple stakeholders.

Typical stakeholders include:

- Legal teams
- Privacy professionals
- Information security teams
- Compliance functions
- Operational risk teams
- Procurement specialists

Our objective is to provide clear, accurate and consistent information that helps stakeholders complete assessments efficiently.

Supporting Legal Teams

Legal teams frequently focus on:

- Contractual obligations
- Liability considerations
- Data protection requirements
- International transfers
- Regulatory compliance

Supporting documentation and subject matter expertise can help facilitate these reviews and address specific concerns.

Supporting Privacy Teams

Privacy professionals often seek assurance regarding:

- Lawful basis
- Data subject rights
- International transfers
- Privacy governance
- Supplier controls

Our governance framework is designed to support transparency and accountability in these areas.

Supporting Information Security Teams

Security teams typically assess:

- Security governance
- Access management
- Monitoring capabilities
- Incident response processes
- Resilience controls

Providing accurate and consistent responses helps support efficient reviews and informed decision-making.

Supporting Regulators and Auditors

Many customers operate within environments subject to regulatory examination and independent audit.

As a result, supplier assurance activities must often withstand scrutiny from:

- Financial regulators
- Data protection authorities
- Internal auditors
- External auditors
- Risk committees

Our governance and assurance approach is designed with these expectations in mind.

Frequently Asked Questions

Do you complete customer due diligence questionnaires?

Yes. We regularly support customer onboarding and supplier assurance activities through structured due diligence responses.

Can supporting documentation be provided?

Where appropriate and subject to confidentiality requirements, supporting documentation may be made available during onboarding and review activities.

How do you manage regulatory change?

Through ongoing regulatory monitoring, horizon scanning and governance review processes.

Do you maintain formal governance structures?

Yes. Governance responsibilities are assigned across relevant business functions and supported through documented processes and oversight activities.

How do you demonstrate accountability?

Through governance frameworks, documented controls, risk management processes and assurance activities.

Why This Matters

Organisations are increasingly judged not only by their own controls, but also by the controls of the suppliers they engage.

Strong supplier assurance helps organisations:

- Reduce third-party risk
- Meet regulatory expectations
- Improve governance oversight
- Support operational resilience
- Enhance stakeholder confidence

A well-governed supplier relationship ultimately benefits both parties by reducing uncertainty and improving transparency.

Conclusion

> *Enterprise organisations require more than products and services from their suppliers. They require confidence.*

Through governance, compliance oversight, privacy management, security controls and structured assurance processes, 1datapipe seeks to provide customers with the transparency and accountability needed to support informed supplier risk management decisions.

As regulatory expectations continue to evolve, we remain committed to supporting customers through robust governance, effective controls and a culture of continuous improvement.