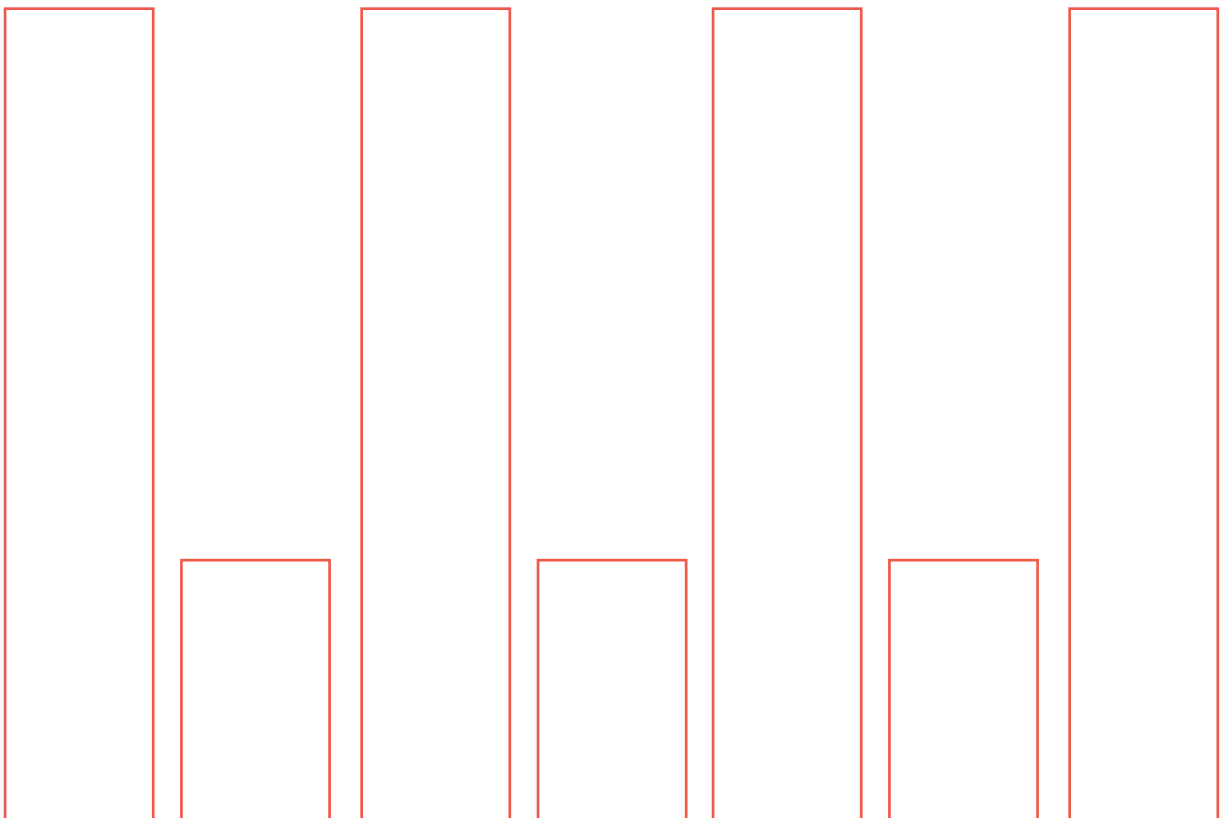
CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

Third Party Exit Plan Template

Joint Initiative Between TPRG and TPOC

VERSION 1.0 | FEBRUARY 2025 | TLP: CLEAR



CONTENTS

1 INTRODUCTION & AIMS

The purpose of this document is to establish a standardised template and associated guidance for exit strategies concerning material and high-impact suppliers as part of an organisation's (further referred to as 'Firm') Third Party Risk Management (TPRM) framework and associated Business Continuity and Disaster Recovery measures.

This template provides a structured approach to managing supplier exits, ensuring continuity of operations and mitigating risks associated with service termination or provider withdrawal. Effective exit planning helps to maintain operational resilience and aligns with regulatory expectations, particularly within the UK and EU financial sectors, where supplier dependencies are scrutinised to safeguard against potential disruptions to core services.

This document, produced as a joint venture between UK Finance's Third Party & Outsourcing Committee (TPOC) and the Cross Market Operational Resilience Group (CMORG's) Third Party Resilience Group (TPRG), primarily caters for the operational necessity of effective exit planning, but also the UK's regulatory imperatives. Due consideration has also been given to the EU's Digital Operational Resilience Act (DORA) and the Financial Services Board (FSB's) "*Toolkit for enhancing third-party risk management and oversight*"; this template addresses key operational and regulatory expectations for disengagement. Regulators emphasise the need for financial institutions to have robust exit strategies for material suppliers, especially those supporting core banking functions, data processing, or customer-facing services. Under these guidelines, the inability to transition smoothly from an essential supplier could be seen as a compliance risk, emphasising the need for well-documented, actionable exit plans.

The document is structured to cover the following sections, each intended to support a comprehensive, regulatory-aligned exit strategy:

- Service Information and Alternative Service Providers - This section includes a curated list of potential alternative suppliers with relevant contact information and a summary of the services each alternative provider offers. It also specifies the minimum service and security requirements an alternative provider must meet to ensure seamless transition and compliance. Additionally, guidance is included on pre-evaluating these providers, especially in cases where rapid substitution may be required under regulatory demands for operational resilience.
- Exit Approach - This section provides a high-level approach to supplier exit planning, covering the overall strategy, objectives, and compliance criteria that a successful exit plan should fulfil. It includes references to applicable UK and EU regulations, such as PRA SS2/21 on operational resilience and DORA, to ensure regulatory alignment and mitigate compliance risk. Objectives include ensuring minimal disruption to key operations, protecting customer interests, and upholding financial stability by addressing dependencies on specific suppliers.
- Roles & Responsibilities - Defines the governance structure for managing the supplier exit process, outlining specific roles, accountabilities, and responsibilities of all parties involved. This ensures that all individuals understand their role in implementing the exit plan and in aligning with regulatory expectations. The section covers responsibilities across legal, compliance, IT, and operational areas to ensure cross-functional accountability and streamlined coordination.
- Risk/Impact Assessment - A structured approach to assessing the potential operational, financial, and compliance impacts of disengaging from a supplier. This includes identifying and evaluating

key risk indicators (KRIs) and establishing an exit risk matrix to gauge various scenarios. Consideration is given to financial and operational impacts, such as exit costs, transition expenses, and risk to customer data. A robust impact assessment helps prioritise mitigating actions and informs the timeline for a safe, compliant exit.

- Exit Initiation Approval - Outlines the governance and approvals needed to initiate the exit process, including specific committee reviews and executive clearances. Guidance includes timelines and criteria for obtaining approvals in line with regulatory expectations, ensuring that senior management and, where necessary, the board, are informed of material risks associated with supplier disengagement.
- Data Management - A comprehensive review of data management practices to be followed in the event of an exit, covering data retention, deletion protocols, and restoration processes. This section emphasises the importance of maintaining data integrity and security, aligning with GDPR requirements for data privacy, and addressing potential risks associated with data migration or destruction. A clear data inventory and emergency data protocols will be maintained to ensure that all data assets are appropriately managed and preserved during the transition.
- Exit Action Plan – This section contains an overview of specific steps to be taken in the event of either stressed or planned exit from a third-party service provider. It provides a detailed roadmap for the actions discussed previously, as well as for subsequent actions. This plan serves as a guide for implementing the considerations outlined in this document.
- Communications - This section details the communication plan for managing supplier exits, including regulatory notifications, customer and stakeholder updates, and media statements. Compliance with notification requirements, such as those outlined by DORA for major incidents, is considered, along with customer communications to maintain trust and clarity throughout the transition. Guidance on coordinating with industry bodies and trade associations where relevant is also provided.
- Testing & Documentation – This section outlines requirements for testing and documenting exit plans for outsourced services.

Scope

This template is designed to accommodate a range of material and essential suppliers, providing a foundational framework for supplier exits across varied contexts. However, for highly integrated services, such as major cloud providers, the complexity of transitioning data, maintaining compliance, and ensuring data integrity may require more detailed, bespoke exit planning beyond the scope of this document.

2 SUPPLIER AND SERVICES INFORMATION

2.1 SUPPLIER DETAILS

Job titles may vary depending on the Firm, please include your own where necessary.

Supplier Details	
Supplier Legal Entity Name	
Supplier location(s)	*Document all locations (specifying countries/cities) that the supplier provides services to the Firm from, along with any data centres from which the Firm's data is hosted.* *Document all relevant locations of the material 4th parties (consider concentration risk, geopolitical risk etc.)*
Lead Supplier Manager	
Senior Supplier Manager (if applicable)	
Termination Costs	• *As set out in the contract. If this is not stipulated, Supplier Managers must work with Sourcing Managers and/or Service Owners to provide estimated costs.* • *The outcomes of the calculations for the Termination costs in both stressed and planned exit scenarios need to be included into the Supplier Information and Alternative Suppliers section for each supplier.* • ***N.B** – from a stressed exit perspective, this may only be applicable in stressed exit scenario, where the Firm is instigating an accelerated exit from a supplier due to complete failure/ prolonged disruption of services, as a result of an external event (e.g., cyber-attack, fire etc.)* These fees are likely to be incurred in the following stressed exit scenarios: • Where the Firm is choosing to terminate the contract and exit the supplier at an accelerated pace due to prolonged disruption caused by an external event (e.g., cyber-attack, fire etc.) • Where the supplier is in administration and is still able to provide services to the Group (in a liquidation scenario however, where the supplier has been 'struck off' from the register at Companies House and ceases to exist, the contract is no longer enforceable). In the scenario where the supplier has gone into liquidation and ceases to exist, the contract is likely to no longer be enforceable (please ensure there has been no novation to another supplier entity prior to

	such liquidation), therefore no charges are enforceable. It is likely however that our firm would have sought to terminate (where it has the contractual right to do so) the contract with the supplier ahead of the company being formally wound up and struck off the register. N.B – In any stressed exit scenario there would also be internal resourcing costs as support from IT teams, Data Centre services, Procurement and Legal would be required if moving to an alternate supplier or bringing the services inhouse.
Exit Contract Provisions	• *Outline any provisions in the contract that may support a stressed exit from the supplier.* *(e.g., Termination, Step-in Rights, ESCROW, TUPE (Transfer of Undertakings, Protection of Employment), Parent Company Guarantees, Audit Rights, Knowledge Management etc.)* • *Please reference clause numbers and titles within contract. For support, please contact the Sourcing Manager.*
Regulatory requirements	Should a stressed exit occur, the Firm's executive board member **(Insert name)** who notified the regulator of the arrangement originally (or their subsequent replacement) must: • Ensure early and full engagement of Accountable Person (insert name) who has Senior Management Function (SMF24) responsibilities, and Chief Procurement Officer take place. • Engage the regulators to provide update on process been undertaken, including, where relevant, view on customer impacts and mitigations. • Agree with the SMF24 (insert name) the appropriate engagement method with the PRA (Prudential Regulatory Authority) & FCA (Financial Conduct Authority). Appropriate Business Unit governance must be put in place and undertaken to ensure full auditability of activity in relation to engagement of the regulators in a stressed exit scenario. ***This is recommended for all super severe and medium resilience suppliers that provide material services.*** ***N.B.- Business Units can engage regulators beyond this scope where they have agreed that this is appropriate and proportionate to the anticipated impact.***

2.2 CONTRACT AND SERVICES

Guidance Notes

To complete this section, Supplier Managers must engage with Business Unit/Platform SME's that consume the supplier's service(s). **Supplier Managers are facilitating the writing of the plan, but SMEs must support in providing the content to ensure the information is correct.**

This section must detail all services provided by the supplier, including those mapped to Important Business Services (IBS) where applicable.

If a supplier provides multiple services to the Group, the table below must be replicated for each individual service line. Where there are multiple 'other services' you can either replicate the table or include as an appendix within this plan.

2.2.1 IMPORTANT BUSINESS SERVICE (IBS) MAPPED SERVICES

Insert Service Name	
Service Name/ Description:	• *Utilise description from SMRF and additional information that may be included within contract.*
Contract Reference	• *Include all relevant contracts.*
Contract End Date(s)	
Has the service been identified as material?	
Provide an outline of what makes this service material	
All Business Units/ Platforms consuming the services, including relevant Key Stakeholder name(s)	• *Where services are being consumed by multiple areas or entities, Supplier Managers must list key stakeholders (where relevant) alongside which service they use.*
Business Service Owner(s)	• *May be the same as the Accountable Person / or delegate. This may also be Product Owners.*
List of our Important Business Service (IBS) that the supplier's service(s) have been mapped to	
Impact Tolerances (ITOL) for all IBS supported by the supplier's service(s)	• *The supplier may have their own ITOL's, however the IBS information documented here must be those defined by the Firm.* *Supplier Managers must engage with IBS Owners to confirm ITOLs for all IBS that the supplier's service(s) have been mapped to.*

Number of customers that would be impacted by a disruption to/ complete failure of the supplier's service(s)	• *Please include obtain any granular customer information from the Firm's SMEs, highlighting whether any of these customers will be classed as vulnerable.*
Describe how customers would be impacted by a disruption to/ complete failure of the supplier's service(s)	• *e.g., If the ATM service were to fail, the customer would not be able to use their debit card(s) to withdraw cash.* • *Please ensure to highlight any impacts to vulnerable customers.*

2.2.2 ALL OTHER SERVICES

Insert Service Name	
Service Name/ Description:	
Contract Ref	• *Include all relevant contracts.*
Contract End Date(s)	
All Business Units/ Platforms consuming the services, including relevant Key Stakeholder name(s)	• *Where services are being consumed by multiple areas or entities, Supplier Managers must list key stakeholders (where relevant) alongside which service they use.*
Business Service Owner(s)	• *May be the same as the Accountable Person/ or delegate. This may also be Product Owners.*
Accountable Person	• *May be the same as the Business Service Owner/ or delegate. This may also be Product Owners.*
Number of our customers that would be impacted by a disruption to/ complete failure of the supplier's service(s)	• *Please include obtain any granular customer information from the Firm's SMEs.*
Describe how customers would be impacted by a disruption to/ complete failure of the supplier's service(s)	• *e.g., If the ATM service were to fail, the customer would not be able to use their debit card(s) to withdraw cash.*

2.3 END TO END PROCESSES AND DEPENDENCIES

Guidance Notes

To complete this section, Supplier Managers must engage with Business Unit SME's that consume the supplier's service(s).

N.B – Tables below must be replicated for each Business Unit that the supplier provides services to.
The tables below provide an outline of how the suppliers services integrate/ support.

1. [INSERT BUSINESS UNIT NAME]

Name of internal process	How supplier services enable this process	Supporting Documentation
	This section of the table must include: • *A high-level summary of how the supplier service(s) fit into the Firm's end-to-end internal processes.* • *Identification of any touchpoints with/dependencies on any of the Firm's other suppliers to deliver the services within the end-to-end process. (N.B – this is not fourth parties that the supplier has contracted with, these are the Firm's contracted suppliers).* • *Identification of any of the Firm's other suppliers that have a dependency on the supplier to deliver their services to the Firm. (N.B – as per above, this is different to Nth parties)*	*e.g. process documents or architectural diagrams, or link to any SharePoint/ other repositories that hold relevant process documents and architectural diagrams, etc.*

2. [INSERT BUSINESS UNIT NAME]

Name of internal process	How supplier services enable this process	Supporting Documentation

3. [INSERT BUSINESS UNIT NAME]

Name of internal process	How supplier services enable this process	Supporting Documentation

2.4 END TO END PROCESSES AND DEPENDENCIES

Alternative Suppliers

- For the service being consumed, is it possible to consume all or part of the service from an alternative supplier?
    - If No, then explain why and what the alternative options for maintaining the service in the event of a loss of primary supplier is –
    - If yes, then identify what the alternative suppliers are in conjunction with the below matrix – identify what your top 3 options are.

Question	Alternative 1	Alternative 2	Alternative 3
1. List alternative third-party suppliers that could provide this service: 2. Can this supplier provide all the services required for like for like continuation of the service currently provided?			
2a. If no, then list what services cannot be provided?			
2b. Can the services not being provided be provided by another alternative? If so, please list, or can they be mitigated through an alternative route such as insourcing?			
3. What is the current expected onboarding time for this supplier?			
3a. Does this timescale meet the requirements for a stressed exit?			
3b. Are there steps that can be taken to reduce that timescale for onboarding to meet the requirements?			
3c. If yes, what are these?			
3d. Based upon the answer to 3c, what are the recommended actions to be taken now to secure the effectiveness of any future requirement to onboard this supplier?			
3e. What is the cost/risk considerations linked to the implementation of these?			
3f. For each of these options, what is the business decision regarding the implementation of them?			
4. Does the consuming entity have an existing relationship with the alternative supplier?			
4a. Does the existing relationship cover the same services as those which will be required to be replaced?			
4b If yes, what steps will be required to ensure the supplier has the relevant capacity/relationship to undertake the activity when required?			
4c. If No, then what needs to be done to ensure we have the relevant relationship with the supplier to	Consider Cyber, IT, Data connections		

ensure we can utilise the relationship within timescales when required?	and time to set up. Consider how/what needs to be done to ensure we are a preferred client particularly in a circumstance where multiple Section members of the financial community rely upon the same incumbents.		
Estimated timeline to onboard alternative third party and/or service.	Estimated number of months required to bring onboard		
Are there any proactive actions we can take to bring that period to onboard down?			
What is our current Concentration Risk Score with this supplier?			
What is the current Stability Score for this supplier?			
When were the alternative suppliers' scope and availability last reviewed?			
At this review point, was this supplier a viable option as a contingency?			
Provide additional rationale as to why this supplier would be a good alternative (where relevant)			

3 EXIT APPROACH

Section 10 of Supervisory Statement 2/21 sets out the regulatory expectations on Exit Planning and Business Continuity. It stresses the "ability of firms to deliver important business services provided or supported by third parties in line with their impact tolerances in the event of disruption. Consequently, notwithstanding the importance of effectively planning for non-stressed exits, the main focus of Section 10 is on business continuity and stressed exits."

Approach to managing stressed exit

Exit management is a strategic exercise and requires careful planning. Mismanagement of exit can have severe financial and non-financial implications on a firm. The approach to managing stressed exits has the following enablers.

Organisation culture

This includes, but is not limited to, levels of hierarchy, organisation's ability to manage a crisis including the ability to take quick decisions.

Risk culture

This includes, but is not limited to, investing in the overall capability of supplier relationship managers, constant sensitisation about risk from third party engagements, upgrading risk intelligence gathering via ongoing monitoring. Large, catastrophic events come with forewarnings that were ignored e.g., early signs of financial distress, management change, lawsuits.

Market Intelligence

This includes keeping up with the latest updates in the Market. e.g., the availability of latest capability / technology including new service providers. An important component of Market Intelligence is creating awareness about adverse news (including financial weaknesses within the Supply Chain)

Data Quality

An organisation should have access to data that can reliably predict the impact of Supplier's exit. Data points such as Supplier concentration, sub-contractors, criticality of an arrangement including its impact to the organisation and linkage to Important Business Services enable the organisation to determine the approach that may need to be adopted.

Exit Approaches available

The Exit approach is deeply connected with the nature and complexity of services and the substitutability of the provider.

There are three common approaches available with firms when faced with an exit scenario; 1) Transition out; 2) Partial transition out; 3) In-housing.

1. Transition out

This involves transitioning the services out to an alternate service provider. The alternate service provider may be selected from among the existing service providers, or a new provider may have to

be onboarded. This approach relies on the simplicity of the Firm's overall onboarding process and the ability of the alternate service provider to scale up to meet the demands from the industry.

Transitioning services to an alternate provider that is already providing services to the Firm may be less time-consuming that onboarding a completely new provider. On the other hand, the Firm needs to quickly ascertain that the chosen provider has the proven capability to provide the services.

Transitioning service out to an alternate provider is ideal for arrangements where the services are relatively straight forward with low dependence on sub-contracting. Some examples where transitioning out may work are: cash transportation services, software licensing.

2. Partial Transition out

Where the alternate provider is not previously onboarded or isn't fully capable of providing services, firms may choose to selectively transition services to the chosen provider; either by discontinuing the non-essential services or bringing the remaining services in-house either permanently or temporarily while relying on business continuity measures.

Partial transition out works well for arrangements that relatively more complex, potentially geographically spread out and the underlying arrangement supports an Important Business Service. Partial transition out may work well for Cloud arrangements, payroll processing arrangements, arrangements that support regulatory reporting, for example.

3. In-housing

Bringing the service back in-house is perhaps the easiest approach to consider when faced with a stressed exit. However, the disadvantage of this approach is that the Firm loses the cost, scalability, and other benefits that outsourcing provides. Firms may choose to bring the services back if the alternates in the market do not provide any strategic advantage. The key challenge faced in adopting this approach is the need for potentially rapid internal scalability of resources.

One of the means through which services can be brought in-house is through the exercise "step-in rights". This entails taking over the running of the service using the supplier assets, employees, buildings, sub-contracting chains running into multiple layers etc. These may also be called Transfer of Undertakings (Protection of Employment) or TUPE.

Use of step-in rights is enormously complex, time consuming and difficult to execute because it requires a deep knowledge of the arrangement and support from the service provider to provide the necessary information. It requires meticulous planning and engagement.

Execution of step-in rights or TUPE may be used for extremely complex arrangements such as large a data centre.

Choosing the Firm's approach to stressed exit

Depending on the circumstances, the Firm may choose any of the above approaches that works best. The choice of an approach and its success depends on:

- The time available for execution.
- Cost/benefit among the options available to the Firm.

- Strength of continuity plans to ensure that tolerance limits are maintained during exit.
- Minimal/no disruption of services.
- Ability of the Firm to safeguard its data/intellectual property once the exit is complete.

4 ROLES AND RESPONSIBILITIES

To facilitate a full transition of services the following roles and responsibilities need to be determined to avoid as much disruption to services under an exit scenario.

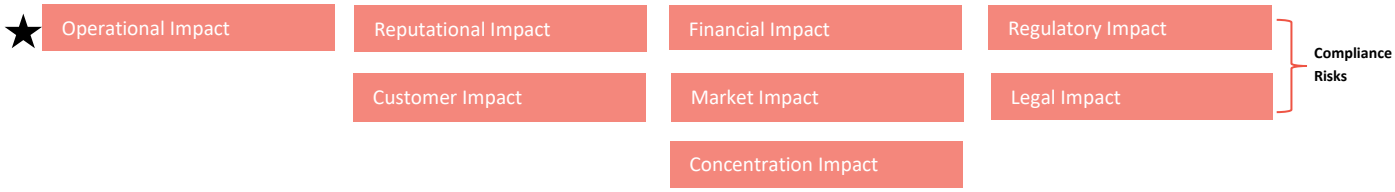
Role	Job Title	Contact Details	Responsibilities
Business / Service Owner			Overall accountability for the stressed exit plan. Will act as deputy if the Exec owner isn't available. Sign off required for stressed exit plan approval.
Business Continuity / Resilience Lead			Contributes to the stressed exit plan, detailing the Business Continuity (BC) approach to maintaining services during a stressed exit.
Executive Owner			Executive responsible for Business / Service owner. Sign off required for stressed exit plan approval.
Important Business Service Owners			Contributes to the stressed exit plan by detailing which Important Business Service (IBS) will be impacted and potential impact on Impact Tolerances. Sign off required for stressed exit plan approval.
Information Security Team			Work as part of a stressed exit project team to ensure all data and controls are in place, and data is safeguarded.
Legal Team			Contribute to the stressed exit plan with any key legal clauses or rights of termination. Sign off required for stressed exit plan approval.
Procurement Lead (if different to Supplier Relationship Manager (SRM)			Contributes to the exit plan detailing alternative suppliers. Act as a deputy to the SRM.

			Sign off required for stressed exit plan approval.
Project / Program Manager			Involved to co-ordinate the exit plan and ensure governance is adhered to.
SMF24			Overall accountability for Outsourcing and Third-party risk management in the Firm, to be informed of any potential stressed exit invocation. Sign off required for stressed exit plan approval.
Subject Matter Experts (Business and Technical SME's)	[May be multiple]		Contributes specialist knowledge and feedback to the exit plan i.e. architectural impact, service transition requirements, technical requirements).
People Team			Work as part of a stressed exit project team to ensure all people queries are resolved, this may also involve the TUPE'ing of staff (Transfer of Undertaking, Protection of Employment).
Supplier Relationship Manager (SRM)			Coordinates with all Firm stakeholders to ensure the exit plan is up to date and reflects the current position i.e. annual reviews. Sign off required for stressed exit plan approval.
Communications Head/Team			Coordinates with the BC/Resilience Lead as part of a stressed exit, drafts and issues both internal and (if required) external comms.

5 RISK / IMPACT ASSESSMENT

Note: Company / Financial Institution should align Risks according to their Risk Management Department / Risk Governance Framework

Purpose/Directions: Identify immediate impacts to services as a result of permanent loss of Third-Party. Select all relevant impacts and describe how the permanent loss of Third-Party services affects each. *Other Considerations/Best Practices: Impact of 'Other' should only be selected to provide more details and/or to include impact(s)*



Identify immediate **Operational Impact(s)** to services as a result of permanent loss of Third-Party and describe how the permanent loss of Third-Party services affects each**.** By describing these operational impacts Line of Business can gain a comprehensive understanding of the challenges posed by the loss of a material third-party service and can work towards mitigating these impacts through an effective exit strategy.

Risk/Impact of loss resulting from inadequate or failed internal processes or systems, people or external events. The primary risk associated with third parties is operational risk; however, third-party risk can also manifest in strategic, reputational and compliance risks.

Operational	Yes/No	Comment/Details:

Other Considerations/Examples

The operational impacts of a line of business losing a material service(s) provided by a third party/suppler can be significant and multifaceted, impacting various aspects of the companies' operations.

- Operational – Key Service Loss: Example: Loss of key service would impact transaction processing, impacts to data storage, or impacts to customer account management, leading to delays, errors, or unavailability of key services.
- Operational - Customer Service Challenges: Customer-facing operations, including online banking, ATM access, and customer support systems, may be affected, potentially leading to customer dissatisfaction and service complaints. Increased operational impacts due to customers wanting answers and/or complaints.
- Operational - Risk and Compliance: The loss of the material third-party service can impact the Firm's risk management and compliance functions, potentially leading to challenges in monitoring transactions, regulatory reporting, or adherence to security standards.

- Operational - Financial Implications: The operational impacts can have financial ramifications, such as increased operational costs, potential revenue losses, and the need to allocate resources to mitigate the effects of the service loss.

Customer Impacts

Note: Company / Financial Institution should consider the types of businesses and services they provide and the needs of the following types of customers. Determine your customers.

Example: People, Companies, Institutions

Other Considerations

When a material service supported by a third-party vendor is lost, the customer impact refers to the effects of this loss on the customers who rely on the Line of Business-Critical Service(s) and or Prioritized Material Service(s) (PCS). This impact can vary depending on the nature of the service and the extent to which it is critical to the customers' operations. Some potential aspects of customer impact in this context include, but not limited to:

1. Material Service Downtime: Customers may experience disruptions / downtime depending on the Line of Businesses material service(s) supported by a Third Party are unavailable (in consideration of any Application Enablers such as Externally Hosted / Managed Applications) affecting Line of Business productivity and ability to serve their customers.

2. Customer Financial Impact: The loss of a material service can have financial implications for customers, such as lost revenue, increased costs to mitigate the impact, or potential contractual penalties.

3. Customer Reputation/Experience: If the loss of the material service leads to customer-facing issues, it can damage the reputation of both the third-party vendor and the impacted customers, potentially leading to customer dissatisfaction and loss of trust. Customers may experience a decline in the quality of service, impacting their overall experience and satisfaction of the Firm.

Customer	Yes/No	Comment/Details:

Financial

The financial impact of the loss of a material service (in consideration of any Application Enablers) supported by a third-party vendor refers to the effects on the financial aspects of the Lines of Business operations. This impact can encompass various elements, including but not limited to:

1. Revenue Loss: The unavailability of the material service may directly impact the Lines of business ability to generate revenue, especially if the service is integral to their product or service offerings.

2. Cost of Downtime: Lines of business and or Customers may incur additional costs to address the consequences of the service loss, such as implementing the perm/interim strategy (aka workarounds), overtime pay for staff or hiring resources or acquiring/contracting an alternative third party's services.

3. Contractual Penalties: Service level agreements (SLAs) and contracts with other Third Parties or regulatory bodies may impose penalties or fines for service disruptions, further impacting the Line of businesses financial position.

4. Legal and Compliance Costs: The loss of a material service might lead to legal and compliance-related costs, such as addressing customer claims, regulatory fines, or legal actions resulting from the service outage.

5. Customer Churn and Loss of Future Revenue: Prolonged or severe service disruptions can lead to customer dissatisfaction, potentially resulting in customer churn and the loss of future revenue streams.

6. Understanding the financial impact is important for both the third-party vendor and the affected Lines of business, as it can influence the prioritization of efforts to fully exit the service, the negotiation of compensation or penalties, and the assessment of the overall cost of the service disruption. It also plays a crucial role in determining the permanent exit strategy & interim strategies required to mitigate the financial impact.

Financial	Yes/No	Comment/Details:

Identify immediate **Market Impact(s)** to services as a result of permanent loss of Third-Party and describe how the permanent loss of Third-Party services affects each.

Definitions of Key Market Risk Component

- General Market Risk: According to the Market Risk Capital Rule[1], General Market Risk may be defined as **risk of loss in the market value of positions resulting from broad market movements,** such as changes in the general level of interest rates, credit spreads, equity prices, foreign exchange rates, or commodity prices.
- Specific Market Risk: Specific Risk is defined as changes in the risk of loss on a position due to factors other than broad market movements and includes event and default risk, as well as idiosyncratic risk. **Specific Risk is associated with equity and debt positions**.

Market	Yes/No	Comment/Details:

Identify immediate **Reputational Impact(s)** to services because of permanent loss of Third-Party and describe how the permanent loss of Third-Party services affects each**.**

Other Considerations: When a company experiences the loss of material services due to a third-party provider failure, the reputational impact can be significant. Here are some potential factors to consider and guidance on managing the reputational impacts, include but not limited to:

1. Transparency and Communication: It's crucial for the company to communicate transparently with its customers and stakeholders about the situation. Clear and timely communication can help **manage**

expectations and mitigate reputational damage. Providing regular updates on the situation and the steps being taken to resolve it can demonstrate the companies' commitment to addressing the issue.

2. Customer Impact: Assess the impact of the third-party service loss on customers. If their ability to access their accounts, make transactions, or receive services is affected, it's important to proactively reach out to affected customers, offer support, and provide alternative solutions if possible. Customer satisfaction and loyalty are closely tied to the **Firm's reputation**.

3. Regulatory Compliance: Depending on the nature of the services lost and the regulatory environment, the Firm may need to report the incident to relevant regulators and authorities. Demonstrating compliance with regulatory requirements and cooperation with oversight bodies can help **maintain the companies' reputation for integrity and responsibility**.

4. Brand Perception: Consider the potential impact on the companies' brand perception. **Reputational damage may occur if the incident is perceived as a reflection of the company's inability to ensure the reliability and security of its services**. Communicating the Firms' commitment to security, risk management, and position during the exit can help **mitigate these concerns**.

5. Long-Term Rebuilding: If the incident has caused reputational damage, the line of business should also focus on rebuilding trust and confidence over the long term. This may involve targeted marketing and communications efforts to emphasize the Firm's strengths, reliability, and commitment to customer service. **These may be specific items to highlight within your long-term strategy.**

In summary, when a company experiences the loss of material services due to a third-party provider, managing the reputational impacts requires a proactive and transparent approach. By prioritizing customer communication, compliance, risk management, and long-term rebuilding efforts, the company can mitigate reputational damage and maintain trust among its stakeholders.

Reputational	Yes/No	Comment/Details:

Compliance	Yes/No	Comment/Details:

Identify immediate **Legal Impact(s)** to services as a result of permanent loss of Third-Party and describe how the permanent loss of Third-Party services affects each**.**

1. Liability and Indemnification: Assess the legal implications of the service loss in terms of liability and indemnification. Depending on the circumstances of the service disruption, the Firm may have grounds to seek compensation or indemnification for losses incurred as a result of the third-party's failure to deliver material services.

2. Customer Contracts and Obligations: Evaluate the legal implications for customer contracts and obligations. If the service loss impacts the Firm's ability to fulfill its commitments to customers, such

as processing transactions or providing access to accounts, there may be legal implications related to breach of contract or fiduciary responsibilities to customers.

3. Data Protection and Privacy: Consider any legal implications related to data protection and privacy. If the service loss affects the security or privacy of customer data, the Firm may need to assess its obligations under data protection laws, including notification requirements in the event of a data breach.

In summary, the legal impacts of a loss of material services from a third-party provider require a comprehensive assessment of regulatory, customer, and risk management considerations. By proactively addressing legal obligations, contractual rights, and risk mitigation strategies, the Firm can navigate the legal implications and seek to minimize potential liabilities arising from the service loss. It's important for the Firm to engage legal counsel and relevant stakeholders to ensure a comprehensive approach to addressing the legal impacts of the situation.

Legal	Yes/No	Comment/Details:

Identify immediate **Regulatory Impact(s)** to services as a result of permanent loss of Third-Party and describe how the permanent loss of Third-Party services affects each**.**

- The loss of material services from a third-party provider can have significant and specific regulatory implications for a Firm. Here is some guidance on the potential regulatory impact and how the Firm can navigate:
- Regulatory Compliance:
- Consider the regulatory implications of the service loss.
- Depending on the nature of the affected services, the Firm may have obligations to report the incident to relevant regulatory authorities.

Compliance with reporting requirements and cooperation with regulatory inquiries is essential to mitigate potential regulatory/government repercussions.

Regulatory	Yes/No	Comment/Details:

- Identify immediate **Concentration Impact(s)** to services as a result of permanent loss of Third-Party and describe how the permanent loss of Third-Party services affects each concentration" as pools of exposures that may perform similarly because of a common characteristic or common sensitivity to economic, financial, or business developments. Concentrations can arise with respect to individuals, geographic locations, industries, products/services, asset classes, and any other category reflecting a common pool of exposure.
- Not all concentrations represent the same level of risk or necessitate the same level of supervision. "Concentration risk" refers to any single exposure or group of similar, correlated

exposures that exceed risk tolerance levels and/or have the potential to produce losses large enough to threaten the Company's performance, condition, or reputation.

Concentration	Yes/No	Comment/Details:

Technology	Yes/No	Comment/Details:

Data*	Yes/No	Comment/Details:

**Future Consideration*

Cloud Technologies*	Yes/No	Comment/Details:

**Future Consideration*

Subcontractor*	Yes/No	Comment/Details:

**Future Consideration*

Other	Yes/No	Comment/Details:

How long can the service be unavailable before there are significant impacts to the Company, Business or Clients/Customers?

- *State the timeframe of the service being unavailable and the specific service / activity it would have an impact to.*
- *State the level of impact (low, medium, or high) for each impacted service / activity.*
- *When deciding the timeframe, choose the worst possible scenario so you do not overestimate the length the service might be unavailable.*
    - *For example, if you are deciding between one week or two weeks for how long the service can be unavailable without significant impacts, choose one week. If it is unknown how long your service can be unavailable, choose 0 days as this is the worst possible case.*

Residual / Potential Impacts:

- *When developing an exit strategy plan, it is important to capture the residual/potential impacts that may reside/remain once the permanent strategy is implemented. *For None Strategy's (No Strategies) this is even more important to document*
- *Residual impacts are, in the simplest sense, the consequences of any action. In an exit strategy context, residual impacts are the impacts that may reside/remain once the permanent strategy is implemented. (Or if there is a 'None/No Strategy).*
- *An easy example, such as building a new highway, can have both positive residual impacts to the public (road noise) and lasting environmental consequences (increased rain run off).*
- *Residual/Potential Impacts are often not same as the impacts section in the plan which are capturing the impacts due to the loss of the services, as the goal of the exit strategy plan is to reduce/mitigate the loss of services from the Third Party. If there is a non-strategy (no strategy) then this may be similar.*
- *Requirements: Summary of expected residual/potential impacts are listed; if none are expected, state why they are not expected.*
- *Responses such as "N/A" or "None" may be not accepted/sufficient.*
- *Common residual impacts that can occur, but are not limited to:*
    - *Financial impacts (cost of implementing exit strategy plan; legal fees)*
    - *Operational impacts (example: significant disruptions to business operations which can impact employee morale and productivity – this can be mitigated by effectively planning and communicating with employees, loss of domain knowledge)*
    - *Market impacts (SEC Filings, Stakeholder impact due to inability to receive timely materials, information, communications)*
    - *Reputational impacts (impact to the Firm's business reputation including customer/industry reputation, customer trust)*
    - *Legal impacts (involving legal requirements such as complying with regulatory requirements or fulfilling contractual obligations)*
    - *Technology impacts (Data loss associated with an externally hosted application)*
    - *Strategic impacts (long term strategic impacts on the business including loss of key personnel and expertise, as well as the impact on the company's brand and market position.)*

6 EXIT INITIATION APPROVAL

Guidance: This section is designed to ensure that appropriate governance structures are in place to approve a decision to exit and subsequent initiation of the exit plan.

It is expected that the exit initiation approval process and management of the exit plan will be owned by those who are responsible for the management of the service / relationship, however it will be necessary to obtain certain senior stakeholder and committee approvals prior to initiating any of the steps outlined in the plan.

Exit Initiation Approval Flow: Initiation approval process flow is outlined in the table below and expected to be considered as appropriate for the type of exit, i.e. stressed and non-stressed.

- When to apply the process.
  - Exit initiation considerations will only become relevant at the point when the service / relationship is disrupted to a level where service level requirements and operational resiliency can no longer be maintained.
- How to apply the process.
  - Initial stages of exit initiation approval will be triggered by the service stakeholder group. This group will lead escalation to senior stakeholders and committees as required.
  - Non-Stressed Exit – Application of the full approval flow will be required prior to initiation of the exit plan.
  - Stressed Exit – SMR approval (within relevant committee structures) is required as a minimum prior to exit initiation in a stressed exit scenario. Further risk committee and regulatory approval must be sought at the earlier opportunity within the committee structure schedules.

*NB: Table can be adapted according to individual Firm's structures, however, should carry 4 distinct phases.

1) Stakeholder / service user alignment that services have been disrupted to a level that is irreparable.
2) SMR alignment
3) Committee approval
4) Regulatory approval – where relevant

Exit Initiation Stage	Description	Stakeholder (Name and Title)	Committee	Regulatory Authority
1) Stakeholder Triage	List the names / details of staff who will be responsible for raising the initial consideration for exit initiation			
2) SMR Approval	List the names / details of staff with SMR responsibility for the service / relationship. These individuals will hold responsibility for raising the initial approval request at			

	subsequent committees as required			
3) Risk Committee Approval	List of risk committees required to approve a decision to exit			
4) Regulatory Approval	List of regulatory approvals required to approve a decision to exit			

7 DATA MANAGEMENT

The content in light grey (and italics in the table) are guidance notes outlining the type of information/questions which should be included/considered when completing this section.

Data Management

Outline what data will need to be transitioned, accessed, retrieved and/or confirmed destroyed in a stressed and planned exit scenario. Identify who is Data Controller, who is Data Processor. Identify any retention periods needed. Identify where data is stored and how it will be destroyed/conformed if it is destroyed. Also, identify where the data currently resides within the supplier. The Exit Plan should also outline how we would expect to bring the data in house/on premise, transfer the data to an alternative provider and confirm data is deleted destroyed in accordance with the contract and Firm policies for data management e.g. **Data Privacy and Data Governance**. **Always check the current policy version and requirements for Data**.

Example wording below to amend as appropriate, also populate the Data Management section below.

To facilitate a full transition of services the following data will need to be accessed, retrieved and transferred to avoid disruption to services under an exit scenario. All Firm data stored by [**SUPPLIER**]

- All information held by [**SUPPLIER**]
- Physical servers within data centres & Branch Servers
- All data related to Backup Data domains & Off site storage
- All related documentation (Operation Handbooks, Service Descriptions, runbooks, playbooks, customer scripts, architectural diagrams, Data Dictionary etc)

The Data Management section below provides detailed requirements:

The following considerations need to be captured as part of the Exit Strategy Planning. Any exit of services needs to be undertaken in accordance with the contract and the Firm policies regarding Data e.g. Data Privacy, Data Governance, Data Destruction etc.

When populating this table, Supplier/Contract Managers must work with relevant Business SMEs/Teams such as Data Privacy Teams, Operational Resilience, CISO, 3rd Party Information Security teams etc to ensure the information is accurate and contains sufficient detail to enable a smooth exit.

Is Personal data processed by the Third Party?	*Yes/No - Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly.*
Does the Third Party have access to any Firm Data?	*Yes/No – If no, the remainder of this section will not be applicable.*
What is the defined data relationship with the contracting party and Firm?	**Data Controller?** A data controller is the entity that determines the purposes and means of processing personal data. Essentially, they decide the "why" and "how" of data processing. **Example wording answer as appropriate to the services:** [SUPPLIER] is classified as the Data Controller under this agreement.

	Data Processor? A data processor is an entity that processes personal data on behalf of the data controller. They act on the instructions of the controller and do not determine the purposes or means of processing. **Example wording answer as appropriate to the services:** [SUPPLIER] is classified as a Data Processor under this agreement. **Joint Controller?** Joint controllers are two or more entities that together determine the purposes and means of processing personal data. They share the responsibility for the processing activities. **Example wording answer as appropriate to the services:** Firm and [SUPPLIER] are classified as Joint Controllers this agreement.
Data Volume	*How many data subjects does the third party process/hold data on?* *How many and what type of data items/documents are processed/stored?*
What is the Third Party Information Security assessment rating?	*Add details of the Third Party Information Security Assessment category used by your Firm. E.g. Tier 1 Material.*
What Data Type does the Supplier have access to or hold/process?	• *What type of data/records/information does the supplier hold/process (e.g. customer/colleague date, processes, manuals, project plans etc.)?* • *List the Data items stored/processed e.g. customer name, DOB, address, Medical etc or embed document with this information.* • *Are any of the Special Categories of data processed? E.g. Health/Medical, Personal Orientation, Criminal convictions & Data related specifically to children.* • *Review contract and include any relevant data information.* • *Ensure information is included on all personal data, including any encrypted or pseudonymised data.* • *Provide any additional context on what this data is.*
What high-risk data items are held by the third party?)	*Financial information, bank and credit card data? Yes/No – If yes, provide details of which are applicable.* *Distinct from categories, we also need to identify 'types' or personal data sufficiently well to understand other (non-GDPR-related) conditions of processing and (GDPR and other) risks of processing. E.g. payment card data is not a legally defined category, it's 'just' personal data but it would need to be managed more strictly than (e.g.) addresses or middle-initials – credit card data is subject to PCIDSS. Retention periods will also vary by type – we may be under legal obligation to retain certain types of data for prescribed periods (financial records, personnel records, latent disease claims records, etc.).*
Is the data transferred processed outside of the EEA?	*In the case of 'yes', we need to know where to and then identify and validate the legal basis on which that data is being transferred (adequacy, SCCs).* *Non-EEA Country - State all countries and jurisdictions that data is processed and stored.* *Are any considered to have adequate data privacy laws e.g. Guernsey, Isle of Man, Jersey Andorra, Argentina, Canada, Faroe Islands, Israel, New Zealand, Switzerland, Uruguay – Check current guidance*

Is any data processed or stored outside the Third Party, such as a 4th party provider(s)/cloud?	*Yes/No* *If yes, provide details of sub-processors where data held/processed by 4th Parties.*
Identify all data that needs to be returned to Firm or migrated / transitioned to a new provider	*All Data (including the database schema) must be accessible to Firm and to the new Outsourced Provider chosen by Firm in a format agreed by the parties, including data that may be held by the primary outsourcer or its subcontractors.* *Things to consider:* *Consider and identify where possible, how we would prioritise data that would need to be accessed, recovered or transferred as a priority in a disruption or stressed exit.* *Ensuring the integrity of the data performance on the old v new systems.* *Consider what data schema details are required? E.g. embed Data Dictionary, System Architecture Diagram(s) showing Data Flows, Data Maps etc which would be required in the event of a stressed exit scenario.*
How should the data be returned, stored, or transferred to either Firm or a replacement supplier?	*Provide the details and process on how the data held and/or processed by the Third Party (or 4th Party) will be recovered, accessed and/or transferred apart of this Exit Strategy Plan?* *For data recovery and transfer consider how easy or difficult it will be to transfer data from one provider to another. Is data shared in a standard format? If not, should it be? Or can it be backed up in a standard format?* *Consider secure asset transfer back to Firm or to a replacement supplier (e.g. securing data in transit, use of secure carrier, etc.).*
Are there any documented recovery plans, or any other documented plans (entitlements, rights, capabilities) to have access to the third party data?	*Add details of any documented recovery plans which would be used in the event of a stressed exit scenario to access and return/transfer the data as necessary.* *Consider:* *If no plans exist, do they need to be developed?* *Have these plans been tested? What were the findings (if any)? What remediation actions (if any) are required?*
Are there any Third Party Supplier Data Retention Considerations Post Exit?	*Where data is not being returned to Firm or transferred to an alternative provider, does the Third Party Supplier need to retain Firm data for a period of time to meet Regulatory Data Retention requirements? Yes/No?* *If Yes, document/consider:* *a. the reason for retention? E.g. GDPR requirement* *b. the length of time the data/records would be retained for? E.g. 7 years* *c. Is there a contractual obligation for the TPSP to comply with the required retrieval timeframes (e.g. within a 48hrs)?* *d. Has there been legal review of the contract and data transfer agreement (where required)?* *e. What are the contractual terms that survive post termination of the contract in the context of the data/records that need to be retained by the Third Party? E.g. do data confidentiality agreements and audit rights (such as Information Security Assessments) survive the termination of the contract?*

Consider technology solutions and tools to facilitate the switching and portability of data and applications and industry codes and standards	*As part of the regular (minimum Annual) review process, consideration should be given to whether there have been any changes/advancements in technology solutions and tools which could support/facilitate the switching and portability of data and applications and industry codes and standards.* *List details of any such tools which Firm would use in the event of an exit (particularly a stressed exit) to support/facilitate the switching and portability of data and applications and industry codes and standards.* *Include details of any testing completed/undertaken to validate the operational effectiveness of the tool/solution.*
How should the data be destroyed (if applicable)?	*Outline the process for data destruction in accordance with Firm contract and Data policies.* *Describe the steps that will be needed to ensure data destruction.* *Consider – has the destruction capability for all sources of data been tested?*
Conclusion	*All the above should be completed & assessed to form an understanding of the data relationship with the party. In the event of an exit please work with CISO to plan accordingly the post contracted data relationship that will remain with the party.* *Things to consider: Storage Limitation: Data Deletion and Data Retention, Data Transfers.* *Data security, including Data Subject Access Request (DSARS), Data Location Requirements.*

Where is the Data Processed or Stored?

Consider and identify where possible, how we would prioritise data that would need to be accessed, recovered or transferred as a priority in a disruption or stressed exit.

Data Storage Repository where Firm Data is Stored or Processed (See Guidance below)	3rd Party or 4th Party Supplier Owned? (Add name of 3rd/4th Party)	Data Location – Country	Data Location – Town / Region	Structured or Un-structured Data (See Guidance below)	Hard or Soft Copy Records	Type of Data Stored or Processed	Data Stored 'On-Premise' or Cloud?	Format Data Held and will be transferred/returned e.g. CSV File	Is the Data Processed or Transferred outside of the EEA? (Y/N)

Structured or Un-Structured Data Guidance	**Structured Data** - Structured data is data that uses a predefined and expected format. This can come from many different sources, but the common factor is that the fields are fixed, as is the way that it is stored (hence, structured). This predetermined data model enables easy entry, querying, and analysis. **Un-Structured Data** - Unstructured data is information with no set data model, or data that has not yet been ordered in a predefined way. Though typically text (like an open text field in a form), unstructured data can come in many forms to be stored as objects: images, audio, video, document files, and other file formats.
Hard or Soft Copy Records	Hard copy means paper/fiche etc. Soft copy means any electronic records.
Data Storage Repository where Firm data stored Or Process	List all storage repositories where Firm Data is Processed or Stored **Examples (not exhaustive list):** Core Policy Admin Systems, Downstream Associated Systems/Applications, Standalone Systems/Applications and Tools, Back Up Data Storage, Calls, Emails, Microsoft Office Documents (Drives/SharePoint), User Access and Processes, Intellectual Property (guides/manuals/templates/documents / document and calculation specification)

Where is the Software Stored?

Application Name	3rd Party or 4th Party Supplier Owned? (Add name of 3rd/4th Party)	Application Hosted Location – Country	Application Hosted Location – Town / Region	Application Hosted 'On-Premise' or Cloud?	Where is the source code stored?	Provide details of Source Code Agent if applicable	Has the software source code been tested?	Last Date Tested

Data Destruction Certificate

Always refer to the current data destruction certificate and check with the Data Privacy Team. The current template is embedded for reference however, you must make sure you use the current version.

Current Third Parties – Firm Data Destruction Confirmation Template embedded here which the Data Privacy Team require completion of during an exit scenario. It lists the different types of repositories of where Firm data may be stored and/or processed and tracks the data treatment activity etc**.**

Check with the Data Privacy Team for current version before use.

8 EXIT ACTION PLAN

Action Plan – to be triggered at the event of Exit -based on risk category/exit trigger, action. Owner, timescales.

Definitions for reference:

- Stressed Exit - Withdrawing from a supplier agreement following the failure or insolvency of the service provider. Usually occurs with limited or no notice. Firm has little or control over the exit and its timing, therefore there is a risk to the continuation of the services.
  Plan could be invoked alongside either the Incident Management Framework or Crisis Management Framework, an anticipated or critical failure, geopolitical crisis (trigger event).
- Non-Stressed Exit - A move away from a supplier agreement in a planned and managed way due to strategic, commercial or performance reasons. Usually occurs within agreed timescales. Firm is in full control and able to implement an alternative solution without any disruption to services.

Stressed Scenario			
Action (order may vary depending on exit scenario)	**Responsible** (Name & Job Title)	**Approximate Timeline**	**Guidance**
Access Impact	Individual or Team responsible for incident impact assessment	Immediately	To determine what action needs to be taken, the sequencing and timeline, the impact of a trigger event needs to be assessed.
Decision to Exit	Appropriate individual with authority to make decision, this will be determined by the scenario and service provision	Within first 24-48 hrs	The decision to Exit will be dependent upon the nature of the scenario and the options that are presented. Reference should be made to the Exit Strategy to inform decision making.
Communicate decision	Led by Communication team and appropriate individuals	Within first 24 hrs	Communicate decision to relevant internal and external stakeholders. Notification to the regulator may be required.
Initiate Business Continuity Plan (Interim measure)	Assumption is that responsibility for the invocation of a Business Continuity strategy is already documented	Immediately	It is anticipated that in a stressed scenario there will be a requirement to invoke relevant Business Continuity strategies to continue service within risk appetite.

Initiate Incident Management Team *or* Crisis Management Team	Individual or Team responsible for Incident Management Team or Crisis Management	Immediately **Please note** that the Business Continuity response may have been invoked already.	In a stressed scenario it is anticipated that an Incident/Crisis Management response should run concurrently.
Initiate Project and SteerCo	Relevant Business Owners/Sponsor with appropriate authority	Within first 24-48 hrs	Due to the potential complexity and criticality of the Exit a project will need to be established with key stakeholders to manage the Exit, identify key milestones, resources required, and manage risks and costs. This project should include decision making and appropriate governance and if required provide updates into the Incident/Crisis Management response.
Complete Operational Risk Assessment	Relevant Business Owners/Sponsor with appropriate authority	Within first 24-48 hrs	A risk assessment (Operational, or otherwise, as appropriate) should be completed and then reviewed and maintained during the execution of the Exit Plan, this should help to monitor and manage risks and inform decision making. This may be an activity that was wrapped into one of the above activities. This should be used to help the Firm move at pace.
Integrate preferred strategy	Relevant Business Owners/Sponsor with appropriate authority	Timeline should be informed by sustainability	Outputs from the Incident/Crisis Management response/Risk

		of Business Continuity Plan, Crisis Management outputs and Risk Assessment	Assessment may result in preferred strategy being adapted. The approach taken should be subject to ongoing review as events unfold, in a stressed scenario assumption made may require agility.
Initiate communication strategy	Led by Communication team and appropriate individuals	Within first 72hrs	Communication plan should include both internal and external stakeholders and include frequency. These should be reviewed as the Exit is executed.
If applicable agree data transfer process, capacity and capability	Service Owner/s	Within first week	Consider how data integrity and security is maintained during the transfer of any data, including how this will be tested and any validation completed.
Other non-data asset transfer	Service Owner/s	Within first week	Agree the recovery or destruction of non-data assets where applicable, equipment, artefacts, intellectual property. In addition to this, there may be knowledge and procedural documentation.
Execute Strategy			It is anticipated that in a stressed scenario the preferred strategy will follow an existing process, onboarding a new supplier/technology or operational change, or a hybrid of these. It is assumed that these are established processes that the Exit will leverage.
Serve notice	Service Owner/s	Timeline should be informed by Exit Strategy	Depending upon the nature of the Exit the point at which notice is served may vary/not

			be required. The contract should inform what action needs to be taken and within what circumstances.
If applicable revoke access virtual/physical	Chief Information Security Office	Timeline should be informed by Exit Strategy	As part of the detailed project plan and milestones, the requirement to remove access and other Exit tasks should be identified, monitored and completed.
Invoke hyper care			Following the transition of services to another provider/or bringing a service back in house, it is important to ensure that there is a heightened level of monitoring to ensure that the service is performing as expected and that controls are implemented to identify any weaknesses.
Complete lessons learned review			Following a stressed Exit, a review of the services including a lessons learned review should be completed to ensure that services are operating as intended. It should also identify learnings to ensure there is continuous improvement.

In the scenario of a planned exit, it is assumed that the exit will be managed in accordance with the contract and existing procedures for sourcing will be leveraged, similar steps will have to be taken. However, it is anticipated that the timeline would be extended.

Non-Stressed Scenario

Action (order may vary depending on exit scenario)	Responsible (Name & Job Title)	Approximate Timeline	Guidance
Assess Impact	Individual or Team responsible for incident impact assessment	Immediately	To determine what action needs to be taken, the sequencing and timeline, the impact of a trigger event needs to be assessed.
Decision to Exit	Appropriate individual with authority to make decision, this will be determined by the scenario and service provision	Within first 24-48 hrs	The decision to Exit will be dependent upon the nature of the scenario and the options that are presented. Reference should be made to the Exit Strategy to inform decision making.
Communicate decision	Led by Communication team and appropriate individuals	Within first 24 hrs	Communicate decision to relevant internal and external stakeholders. Notification to the regulator may be required.
Give Notice	Assumption is that responsibility for the invocation of a Business Continuity strategy is already documented	Immediately	It is anticipated that in a non-stressed scenario there will be a requirement to invoke relevant Business Continuity strategies to continue service within risk appetite.
Initiate Business Continuity Plan (Interim Measure)	Individual or Team responsible for Crisis Management	Immediately **Please note** that the Business Continuity response may have been invoked already.	In a non-stressed scenario, it is anticipated that an Incident/Crisis Management response should run concurrently.
Initiate Incident Management Team *or* Crisis Management Team	Relevant Business Owners/Sponsor with appropriate authority	Within first 24-48 hrs	Due to the potential complexity and criticality of the Exit a project will need to be established with key stakeholders to manage the Exit, identify key milestones, resources required, and manage risks and costs. This project should include decision making and appropriate governance and if required provide updates into the Incident/Crisis Management response.

Initiate Project and SteerCo	Relevant Business Owners/Sponsor with appropriate authority	Within first 24-48 hrs	A risk assessment (Operational, or otherwise, as appropriate) should be completed and then reviewed and maintained during the execution of the Exit Plan, this should help to monitor and manage risks and inform decision making. This may be an activity that was wrapped into one of the above activities. This should be used to help the Firm move at pace.
Complete Operational Risk Assessment	Relevant Business Owners/Sponsor with appropriate authority	Timeline should be informed by sustainability of Business Continuity Plan, Crisis Management outputs and Risk Assessment	Outputs from the Incident/Crisis Management response/Risk Assessment may result in preferred strategy being adapted. The approach taken should be subject to ongoing review as events unfold, in a non-stressed scenario assumption made may require agility.
Initiate Preferred Strategy	Led by Communication team and appropriate individuals	Within first 72hrs	Communication plan should include both internal and external stakeholders and include frequency. These should be reviewed as the Exit is executed.
Initiate Communication strategy	Service Owner/s	Within first week	Consider how data integrity and security is maintained during the transfer of any data, including how this will be tested and any validation completed.
If applicable agree data transfer process, capacity and capability	Service Owner/s	Within first week	Agree the recovery or destruction of non-data assets where applicable, equipment, artefacts, intellectual property. In addition to this, there may be knowledge and procedural documentation.
Other non-data asset transfer			It is anticipated that in a non-stressed scenario the preferred strategy will follow an existing process, onboarding a new supplier/technology or operational change, or a hybrid of these. It is assumed that these are established processes that the Exit will leverage.

Execute strategy	Service Owner/s	Timeline should be informed by Exit Strategy	Depending upon the nature of the Exit the point at which notice is served may vary/not be required. The contract should inform what action needs to be taken and within what circumstances.
Serve notice	Chief Information Security Office	Timeline should be informed by Exit Strategy	As part of the detailed project plan and milestones, the requirement to remove access and other Exit tasks should be identified, monitored and completed.
If applicable revoke access virtual/physical			Following the transition of services to another provider/or bringing a service back in house, it is important to ensure that there is a heightened level of monitoring to ensure that the service is performing as expected and that controls are implemented to identify any weaknesses.
Invoke hyper care			Following a non-stressed Exit, a review of the services including a lessons learned review should be completed to ensure that services are operating as intended. It should also identify learnings to ensure there is continuous improvement.
Complete lessons learned review	Individual or Team responsible for incident impact assessment	Immediately	To determine what action needs to be taken, the sequencing and timeline, the impact of a trigger event needs to be assessed.

9 COMMUNICATIONS

Stressed Exit: Communication Cascade

Responsibility for delivery of communication cascade must be clearly outlined within exit strategy responsibilities.

Stressed Exit Identification: Notifications

Note: Specific job titles are likely to vary from firm to firm

Job title	Name	E-mail address	Telephone Number	Responsibility Considerations
Supplier Relationship Manager				**Notify colleagues with connected supplier management responsibilities**
Executive @ Supplier Manager Accountability				**Ensure awareness to all executive team**
Executive @ SMF24 Accountability				**Notification to Regulator / Industry Bodies / Trade Associations**
Head of business areas affected by stressed exit				**Invoke BC plan, if applicable**
Head of Operational Resilience				**Invoke Crisis Management Plan *or* Incident Management plan, if applicable**
Head of Procurement				**Commence procurement process to onboard an alternative supplier**

Supplier: Notifications

Job title	Name	Email Address	Telephone Number	Responsibility Considerations
Supplier: Account Manager				**N/a**
Supplier: Relationship Director				**N/a**
Interdependent Suppliers: (name)				**N/a**
4th Party Material Suppliers				**N/a**

Operational: Notifications

Job title	Name	Email Address	Telephone Number	Responsibility Considerations
Head of business area with				**Invoke BC plan, if applicable**

interdependent service/supplier				
Head of Legal Services				**Review contract to protect irm including notice to terminate, step in rights, intellectual property rights etc**
Head of Finance				**Cease making supplier payments if advised by Legal / impact on budgets**
Head of Business Change				**Prepare for transition to a new supplier / bring service in-house**
Head of HR				**Consider TUPE implications, if applicable**
Head of Property				**Remove supplier access to premises**

Technology: Notifications

Job title	Name	Email Address	Telephone Number	Responsibility Considerations
Head of Data				**Consider requirements to protect data/data recovery**
Head of IT / Technology SME				**Consider impact on systems / Escrow arrangement / bring service in-house**

Incident awareness: Notifications

Job title	Name	Email Address	Telephone Number	Responsibility Considerations
Head of Customers Comms				**Issue comms to customers through appropriate channels and maintain regular updates**
Head of External Comms				**Draft Press Release**
Head of Internal Comms				**Issue comms to colleagues and intergroup legal entities through appropriate channels and maintain regular updates**

Stressed Exit: External communications cascade

Responsibility for delivery of external communications cascade must be clearly outlined within exit strategy responsibilities.

If the exit is being conducted from a third-party supplier that is material to any of the Firm's Important Business Services (IBS), the Firm might consider cascading the communications of such third-party exit to its designated authority.

External stakeholder notification: Decision-making framework

Job title	Name	Email Address	Telephone Number	Responsibility Considerations
				Determine whether external stakeholder notification is necessary and/or desirable. If yes, proceed
Regulatory Engagement/ Compliance Lead				**Identify if the Firm is legally required to notify any external stakeholders of an event of a stressed exit from a material third-party supplier. If yes, draft relevant comms**
				Identify the external stakeholder groups the Firm sees the benefit in notifying, e.g., regulatory authorities; trade bodies; media/press; partner firms/independent financial advisers (IFAs); supplier staff
Head of External Comms				**Issue comms to the supplier staff if deemed necessary, contents may vary and can include the following: assurances of job security; notification of actions taken and planned etc.**

External stakeholder notifications: Notifications

Job title	Name	Email Address	Telephone Number	Responsibility Considerations
Head of Customer Comms				**Issue the agreed message to the agreed**

				external stakeholder groups through the appropriate channels and maintain regular updates

10 TESTING AND DOCUMENTATION

Testing and documentation for exit plans demands a structured approach to ensure operational resilience and regulatory compliance. The framework recommends annual testing for Material Outsourced services, with additional testing triggered by material service changes.

At minimum, testing consists of desktop walk-throughs, complemented by scenario testing covering technical, cyber, and operational risks, with third-party provider involvement where feasible.

Documentation standards mandate comprehensive test records, including scenarios, dates, and outcomes, maintained within a lessons learned register that tracks both mock and real disruptions. All documentation requires version control and follows a controlled distribution process, with central storage in appropriate file storage solution.

The governance structure places responsibility with the Supplier Relationship Manager (SRM) for development, supported by relevant stakeholders. A two-stage approval process ensures thorough review: first at the stakeholder level, followed by executive sign-off. The Operational Resilience team provides independent assessment and validation, with findings documented in the risk register. Testing effectiveness is measured through service continuity verification, resource availability confirmation, process documentation currency, implementation risk assessment, and stakeholder readiness validation.

This comprehensive approach ensures exit plans remain current, practical, and aligned with regulatory requirements while maintaining operational resilience throughout the third-party relationship lifecycle.

Below: An example of how a summary of these testing activities might be documented:

Scenario	Date	Key Lessons Learned	Main Action Taken
Capture all scenarios tested and real-life disruptions that have occurred, which have prompted a stressed exit scenario.	Capture the dates of each mock scenario/real life disruption.	List all lessons learned for each of the mock scenarios/real life disruptions. This is crucial in order to improve the resilience of the third-party provider.	List the actions taken from each of the scenarios/disruptions. These should tie back to the key lessons learned.
Mock - Technical Failure			
Mock - Cybersecurity Breach			
Mock - Natural Disaster			
Real disruption 1			
Real disruption 2			