THIRD-PARTY LIFECYCLE MANAGEMENT

Guidance

July 2023 | TLP Clear

CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

The Third Party Lifecycle Management Guidance is part of wider suite of third party capabilities across CMORG. Should you wish to access others, please email **enquiries@cmorg.org.uk**.

CMORG-endorsed capabilities (including good practice guidance, response frameworks and contingency tools) have been developed collectively by industry to support the operational resilience of the UK financial sector. The financial authorities support the development of these capabilities and collective efforts to improve sector resilience. However, their use is voluntary and they do not constitute regulatory rules or supervisory expectations; as such, they may not necessarily represent formal endorsement by the authorities.

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

Introduction/Aims/Objectives of Guidance Notes

- Third parties play a critical role in delivering services to firms customers and so throughout the lifecycle of the engagement so it is vital that engagement is robust and complies with regulatory requirements. This guidance looks at each step in the lifecycle of the third party, identifying the key areas of consideration and risks that that financial institutions should consider to support effective and compliant relationships. In addition, the guidance will make reference to Supervisory Statement SS2/21 on third party risk management, and the Operational Resilience requirements of both the PRA and the FCA.
- Delivery will be a publishable document with sections for each stage of engagement from supplier selection and due diligence, classification to support supplier management approach, governance and assurance through to exit.
- In addition, the guidance will propose metrics which will provide key insights into supplier performance and aid decision making.
- Third-party guidance will be applicable to all types of financial institutions.
- CMORG is not a regulatory body, and therefore all CMORG-endorsed capabilities (including good practice guidance, response frameworks and contingency tools) have been developed collectively by industry to support the operational resilience of the UK Financial Sector. The Financial Authorities support the development of these capabilities and collective efforts to improve sector resilience. However, their use is voluntary, and they do not constitute regulatory rules or supervisory expectations; as such, they may not necessarily represent formal endorsement by the authorities.

CONTENTS

VERSION CONTROL

Version Number	Description	Date
Version 1.	Draft Template initial completion (RJ)	24.08.2021
Version 2.	Updated version (DF)	25.05.2023

USEFUL LINKS

Regulator	Link (right-click to open hyperlink)
SS1/21 Operational Resilience Impact Tolerances for important business services	Link to Supervisory Statement
SS2/21 Outsourcing and third party risk management	Link to Supervisory Statement
Glossary of terms - Bank of England	Glossary | Bank of England
Glossary of terms - FCA	Glossary Terms - FCA Handbook

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

Document Title	Identification and Classification
Objective of guidance	As part of the mapping stage of operational resilience it is important to understand which third parties are used to deliver the business service and to guide appropriate management strategies for the criticality of that supplier's services to the overall business service. This section aims to provide suggested areas of consideration when identifying and classifying a third party.
Regulatory Clauses addressed	SS1/21 – Chapter 5 (Mapping) SS1/21 – Section 5.11 (Threshold Conditions) SYSC 15A.4

AREAS OF CONSIDERATION

1. Will the supplier support any Important Business Services ?
   If yes: how many services and which ones?
2. What is the operational resilience pillar the third party supports (e.g. People, Technology, Data)
3. Does this third party provide a critical service to any Important Business Services (i.e. fundamental to the delivery of the Important Business Service)?
4. Will disruption of the third party services impact provision of any of the Important Business Services or critical shared services i.e. potentially cause customer harm, affect policyholder protection or present risks to market instability and/or our own financial instability?
5. What is the impact of third party failure? Will the disruption cause customer harm if not recovered within the impact tolerance for the IBS it supports?
6. Is the arrangement classified as outsourcing as defined by the FCA (Material/Critical/Important) outsourcing?
7. Is the third party classified as automatically material as it is required for the firm to meet threshold conditions or compliance to fundamental rules?
8. What types and classification of data are stored/processed?
9. What (if any) third parties are needed to recover the business service, its supporting processes or operational assets?

INPUTS FROM OPERATIONAL RESILIENCE PROGRAMME

Input	Why?
Identification of Important Business Services	To provide the scope for the mapping of third parties and focus on business services which will potentially cause customer harm, affect policyholder protection or present risks to market instability and/or our own financial instability
Methodology for mapping an Important Business Service	To enable identification of all third parties
An agreed terminology for the classification of the third party	To help understanding of the materiality of the third party (e.g. Critical/Important/Standard etc)

OUTPUT FROM THIS GUIDANCE STAGE

Output	Benefit
Identification of all third parties associated with an Important Business Service (IBS)	To ensure all possible third parties are known
Identification of those third parties material to the business service	To conduct assessment of materiality to the business service
Classification of third party	To provide focus for management, governance and assurance activities

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

Document Title	Capability Assessments (Onboarding)
Objective of guidance	As part of any sourcing activity due diligence is critical to ensure the third party can adequately meet the needs, requirements and vulnerabilities of the firm. This is true to operational resilience and this section provides guidance as to areas for questioning with any third party as part of the due diligence/onboarding stage.
Regulatory Clauses addressed	SS2/21 – Chapter 3 (Impact Tolerance) / FCA Handbook: SYS 15A.2.5R SS2/21 – Chapter 4 (Actions to remain within Impact Tolerance) SS1/21 – Operational Resilience

AREAS OF CONSIDERATION

1. Does the third party have a documented operational resilience and recovery plans, governance of testing and continuous improvement plans? (or equivalent business continuity, disaster recovery, crisis management or incident management plan)
2. How does the third party manage change to maintain recoverability and or end of life / evergreening third party components
3. Does the third party's plan include Business Impact Assessments (BIA's) for significant but plausible incidents with clearly identified recovery steps?
4. Does the third party's plan include the mapping of operational resilience pillars (and governance of testing)
5. Does the third party's plan have identified owners and escalation paths for incident management
6. Does the third party's plan include Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) or other SLA's which are compatible with your impact tolerances set?
   Is the third party able to meet our recovery requirements including impact tolerances and / or recovery time objectives for the services provided?
7. Does the third party test their plans on an annual basis and are they prepared to share the output of any recent test?
8. What is the methodology for testing their plans (walk through, structured scenario, physical testing etc)
9. How do they record continuous improvement initiatives associated with their plans (e.g. Lessons learnt from their tests?)
10. Are they accredited to ISO 22301 (Business Continuity)?

INPUTS FROM OPERATIONAL RESILIENCE PROGRAMME

Input	Why?
Identification the Supplier is associated with an Important Business Service	To focus due diligence on third parties in scope of the regulations
Classification of the third party	To understand the how material the third party is in delivering the Important Business Service
Impact Tolerance for the Important Business Service	To understand the maximum threshold of disruption the third party must deliver its services within

OUTPUT FROM THIS GUIDANCE STAGE

Output	Benefit
Assessment of the third parties capabilities and maturity of resilience	Understanding of the firms approach to operational resilience
Assessment of whether the third party can meet the impact tolerances expectation for the IBS they support	Ability to decide whether to continue to onboard the third party
Expectations of the third party for service performance	To inform the contract/agreement obligations and SLAs

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

Document Title	Periodic Assessment and Assurance
Objective of guidance	To provide boards and management the ability to approve and attest the firms compliance to the regulation, periodic assessment is required to ensure third parties continued to meet their contracted operational resilience obligations. This guidance provides areas of consideration when undertaking periodic assurance of these obligations and service performance
Regulatory Clauses addressed	SS2/21 – Chapter 7 (Governance) FCA: SYSC 15A.7.1R

AREAS OF CONSIDERATION

1. How can we create an organisation wide assessment framework to identify the key risks for each third party?
2. Can we leverage existing risk categories within the organisation to create the assessment framework?
3. For each risk category, who is the business SME, what type of information do we wish to collect and what are our assessment criteria?
4. What is an appropriate review timescale taking into account more regular assessment of higher risk categories/third parties
5. Do we require a remediation project to improve contracts so that third parties provide the information required?
6. How can we create a central, golden source of data for collaboration across the organisation?
7. Does the organisation wish to report from solely an operational resilience point of view or are all third parties in scope?
8. Is operational resilience reporting aligned to pre-existing third party governance?
9. Where does the responsibility sit for regular sample testing of reported risk metrics and how often is that sample testing carried out?
10. Who is responsible for collecting assessment and assurance information from the third parties and do they require any training in the context of operational resilience requirements?

INPUTS FROM OPERATIONAL RESILIENCE PROGRAMME

Input	Why?
A list of those third parties that provide critical elements within an Important Business Service	To focus activity on the third parties in scope of the regulations
A process for adding and removing third parties from scope	So that new third party arrangements can be assessed prior to contract signature

OUTPUT FROM THIS GUIDANCE STAGE

Output	Benefit
Accurate risk assessments	Ensuring that changes in services or the organisations risk framework are visible and reviewed with the third party
Centralised report on the performance of third parties aligned to Important Business Services	Early visibility of key risk areas and trends in performance they may impact important business services
Up to date assurance reviews	Ensure that a third party's control framework continues to align with the organisations requirements

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

Document Title	Testing (Structured Scenario Assessments)
Objective of guidance	To identify the vulnerabilities of using a third party or third party service that will need to be remediated to ensure that we can recover our Important Business Services within the impact tolerances set.
Regulatory Clauses addressed	SS1/21 – Chapter 6 (Scenario Testing) SS2/21 – Chapter 3 (Proportionality) SS2/21 – Chapter 10 (Business Continuity & Exit Plans) FCA: SYSC 15A.5.5G / SYSC 15A.5.3R

AREAS OF CONSIDERATION

1. Does the third party operate the full Important Business Service or part of the process to deliver an Important Business Service?
2. If the third party is providing part of the process what pillar will be they be involved in testing?
3. If the supplier is providing the full Important Business Service have the scenarios been reviewed and agreed (include any intragroup internal outsourcing arrangements as well as external outsourcing arrangements)
4. Is the third party conducting the testing independently or will it be combined testing?
5. Does the third party have a test plan in place showing when testing will be conducted, type of testing and scenarios?
6. Have you reviewed the third parties business continuity and disaster recovery plans
7. What testing is the supplier doing with their third parties / the extended supply chain

INPUTS FROM OPERATIONAL RESILIENCE PROGRAMME

Input	Why?
Impact Tolerances	So we can understand how our Impact tolerances would be breached.
SLAs	To understand our recovery against our contracts
Mapping	Used as the basis of the scenario testing

OUTPUT FROM THIS GUIDANCE STAGE

Output	Benefit
Test Report	An understanding of recovery capability and where there are vulnerabilities
Lessons Learned	Actions produced to improve / mature the process

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

1. Identification and Classification
2. Capability Assessment (Onboarding)
3. Periodic Assessment and Assurance
4. Testing (Structured Scenario Assessments)
5. Contracts and Agreement
6. Contingency and Exit Planning
7. Governance and Framework
8. Supply Chain
9. Reporting

Document Title	Contracts and Agreements
Objective of guidance	To ensure that appropriate contractual provisions are in place in MSAs/statements of work as appropriate with third parties. This is important to ensure that effective oversight requirements (as set out in the other section of this guidance) are founded in contractual provisions and therefore actionable.
Regulatory Clauses addressed	SS1/21 – Chapter 4 (Actions to remain within Impact Tolerance) SS2/21 – Chapter 10 (Business Continuity and Exit plans) EU DORA – ICT Third Party (Article 30)

AREAS OF CONSIDERATION

1. Are the existing schedule(s) or language relating to resilience provisions compliant with SS2/21 and DORA requirements for critical arrangements?
2. Do existing schedule(s) or language relating to resilience align to the requirements of the Important Business Services or critical internal functions for example requiring recovery/maintenance of service within appropriate timeframes? Would it be prudent to have 'standard' and 'enhanced' terms aligned to requirements for different risk profiles of third parties?
3. Are standard clauses that will be required for overseeing resilience capabilities, risks and performance at third parties in place e.g. right to audit (including PEN Testing), transparency of reporting etc?
4. Are relevant resilience requirements passed through to extended supply chain (including requirement for the third party to agree material extended supply chain with customer(s)) and effective oversight arrangements in place at the third party on their supply chain?
5. Are there service level agreements and key metrics that are aligned to service credits / performance-based metrics such as availability, response times for incidents etc. that align to business requirements?
6. Are appropriate information sharing and collaboration (such as joint or third party facilitated testing) on resilience outcomes agreed within arrangements? Are collaboration in planning for exit (including standard exit clauses) and disorderly/stressed exit planning baked into contractual provisions (e.g. Code of Escrow)?
7. Have historical contracts been reviewed against new or updated requirements / regulatory expectations? Are gaps identified and prioritised?
8. Are 'rules of the road' agreed up front for deviation from the standard contractual requirements and what contingencies/mitigants might be required internally for agreeing these changes e.g. where there is no right to directly audit but access to third party audit reports.

INPUTS FROM OPERATIONAL RESILIENCE PROGRAMME

Input	Why?
Scope of Third Parties critical to Important Business Services / posing a high inherent risk to firm resilience	To ensure that the highest bar is applied to third party relationships and/or third party services that pose the greatest risk and need the most oversight
Data on resilience requirements from Third Parties either derived from Important Business Services analysis or business impact analysis (from BCPs)	To ensure that business requirements are aligned into contractual provisions and standards set with Third Parties such as RTOs, RPOs, contingency requirements

OUTPUT FROM THIS GUIDANCE STAGE

Output	Benefit
Contracts and schedules that are compliant with relevant regulatory requirements and aligned to business requirements based on resilience analysis	Enabling effective oversight of third party relationships aligned to business resilience expectations. Confidence in engagement with existing and new third party providers for relevant oversight of resilience capabilities.
Gaps identified in existing contracts that require mitigation or acceptance (if possible)	Enabling effective risk assessment of third party relationships and alignment to the firm's requirement, resilience expectations and risk appetite
	Actions identified to be driven to completion to address risk(s) / issue(s)

INDICATIVE SECTIONS / KEY EXPECTATIONS RELATING TO RESILIENCE IN THIRD PARTY CONTRACTS

Business Continuity Planning	Testing and Exercising	Incident management
Operational Resilience (IB Services)	Subcontractor/Fourth party resilience	Integration/Alignment of standards
IT Disaster Recovery	Declaration of an incident	Governance and reporting/key metrics

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

1 Identification and Classification
2 Capability Assessment (Onboarding)
3 Periodic Assessment and Assurance
4 Testing (Structured Scenario Assessments)
5 Contracts and Agreement
6 Contingency and Exit Planning
7 Governance and Framework
8 Supply Chain
9 Reporting

Document Title	Contingency and Exit Planning
Objective of guidance	To enable user firms to effectively plan for third party disruption or failure, as well as effective transition at the end of a third party relationship.
Regulatory Clauses addressed	SS1/21 – Chapter 4 (Actions to remain within Impact Tolerance) SS2/21 – Chapter 10 (Business continuity and exit plans)

AREAS OF CONSIDERATION

1. Have we clearly documented how we depend on the third party and how we would be impacted should they be disrupted or fail?
2. Have we understood how easy it would be to substitute the third party either internally or externally, both in the short-term through work transfer as well as transition of services on exit?
3. Have internal business continuity plans been updated to reflect what steps we can take as a business should the third party service be disrupted? Does it include key points of contact, escalation paths and SLAs for third party response and recovery?
4. Have RTOs (and RTOs where relevant) been aligned between the third party (both contractual and tested capability) and the processes / services that rely on the third party service(s) internally? Are any gaps or workarounds documented in continuity and/or recovery plans?
5. Is the response and /or recovery of services by the third party dependent on our resources (e.g. applications housed in our data centres, staff housed in our buildings etc.)? Are they understood/documented?
6. Are the proposed products and services supplied to multiple clients (i.e. are we one of many clients to be recovered in the event of disruption?) Have we discussed how this might impact on us during a significant
7. Is co-operation on exit planning enabled through contractual clauses? Has an exit plan been documented for the service to identify the key steps required, key risks and mitigants required to enable orderly transition of service?
8. Are key clauses (such as escrow) in place to support exit strategies should the third party have a severe (irrecoverable) disruption or fail financially? Are steps required to enable continuity and transition of services documented as part of a stressed exit plan?
9. Are we engaged with peers who use the same critical third parties to plan for either disruption or failure of these third parties?
10. Have we tested (table-top, discussion-based, through to actual work transfer/live type testing) our continuity, exit and disorderly exit plans to identify gaps, limitations, opportunities to enhance?

INPUTS FROM OPERATIONAL RESILIENCE PROGRAMME

Input	Why?
Mapping	To understand relationship between third parties and our Important Business Services.
Impact Tolerances	To support alignment of RTOs/RPOs and continuity arrangements throughout contingency, recovery and exit plans.
Communications	To understand where third party relationships require internal/external communications planning, effective channels and testing to prove this out.
Business Continuity Plans	To ensure that third party dependencies and contingencies/workarounds are documented within BCPs.

OUTPUT FROM THIS GUIDANCE STAGE

Output	Benefit
Documented and tested business continuity plans	Confidence in our ability to respond, adapt and communicate should a third party be disrupted.
Documented and tested exit (incl. disorderly) plans	Confidence in our ability to respond, adapt and communicate if a third party fails completely at short notice. Confidence in our ability to transition service(s).
Assurance and oversight of third party contingency and exit planning discipline	Confidence in third party resilience and their ability to support us through internal/external disruption.
Engagement with peers and the industry on common opportunities to enhance resilience around critical third parties	Efficiency from harnessing common challenges/opportunities and lessons learned from peers. Using, where possible, industry standard mechanisms e.g. for payments re-routing. Consistent external communications where peer firms disrupted.

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

Document Title	Governance and Framework
Objective of guidance	Having an appropriate and fit for purpose framework in place to enable organisations to demonstrate their operational resilience capability is key to achieving the principles of the regulation. Robust governance is required to support the framework's operation and reporting output.
Regulatory Clauses addressed	PRA SS1/21 – Chapter 4 (Actions to remain within Impact Tolerance) PRA SS1/21 – Chapter 7 (Governance) PRA SS1/21 – Chapter 8 (Self Assessment) FCA SYSC – Chapter 15A (Operational Resilience Requirements)

AREAS OF CONSIDERATION

1. Do firms have an appropriately robust framework to a) assess the criticality of third parties to Important Business Services and b) identify, manage and report associated risks via an internal control mechanism?
2. Have firms identified and implemented named role holders to support and enforce the framework? Does a RACI exist to enforce the third party lifecycle, specifically for IBS critical third parties?
3. When a third party's IBS criticality is identified or changed, are all relevant stakeholders engaged?
4. How does a firm's capability to identify a third party's IBS criticality align with pre and post contract activities? Is the distinction between third party types, and how their resilience is determined, documented?
5. Is there a defined governance map in place to review and approve changes to the framework, escalate scenario testing outcomes and operational breaches and remediation activities?
6. Is there an evidencable governance path for items requiring board approval, in line with SS1/21 requirements?
7. Firms should ensure the review and approval of the Self Assessment is a standard agenda item at the Board, at a frequency that meets risk appetite, but no less than annually.
8. Is there a process to ensure that all policies, both internal and externally facing, are reviewed and updated to cater for operational resilience regulatory requirements, including future regulatory horizon scanning ?
9. Does the firm have a process for evidencing regulatory compliance traceability, including but not limited to PRA SS1/21 and FCA SYSC 15?
10. Do firms have an internal framework for notifying the PRA of material outsourcing and non-outsourcing third-party arrangements?

INPUTS FROM OPERATIONAL RESILIENCE PROGRAMME

Input	Why?
Key outputs from preceding stages for consideration and approval (e.g. lists of IBS critical suppliers, outputs of scenario testing)	To enable effective understanding and management of operational resilience issues.
Understanding of accountable role holders (e.g. MRT, SMF 24)	To ensure the most appropriate stakeholders form part of the governance framework

OUTPUT FROM THIS GUIDANCE STAGE

Output	Benefit
Documented operational resilience governance framework with escalation routes	To enable management and escalation of operational resilience issues.
Terms of Reference for key governance meetings	To ensure appropriate attendees are present to review relevant information within structured meetings in order to provide effective oversight and management
Defined and agreed operational resilience roles and responsibilities	To ensure clear accountabilities and responsibilities for the management of third party operational resilience.
Approvals of key stages of third party lifecycle management (e.g. Identification and classification of IBS's, impacts tolerances and assessments)	To ensure all part of the framework remain up to date, in line with evolving regulation and formally approved by appropriate accountable persons.

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

Supply Chain	Supply Chain
Objective of guidance	To ensure that firms have full transparency on any material services that will be subcontracted at the onboarding of a new material outsourced provider and ensures that they relevant notification (and the right to object) of material services being subcontracted during the term of the agreement
Regulatory Clauses addressed	SS2/21 – Section 9 Sub-outsourcing And materiality criteria in Chapter 5

AREAS OF CONSIDERATION

1. Do we have up to date lists of all material subcontracted service providers (names, locations, service) ?
2. Does the service meet materiality criteria which includes the potential impact on the firms ops resilience and provision of IBS
3. Does the subcontractor comply with applicable laws, regulatory requirements and contractual obligations including contractual access, audit and information rights ?
4. Does contracted service provider undertake robust testing, monitoring and control on it sub-contractors ?
5. Does the written agreement outline the criteria the subcontractor must meet and also the obligations that it meets and / or any services that cannot be outsourced including notice period, ability to approve/object and any termination rights for cause if notification has not been given
6. Do we understand who is transferring our data across the entire supply chain (and by location) and does it increase our risk?
7. Does the material outsourced provider allow the firm to /bank or PRA allow equivalent access, audit and information rights - if not do we know this? If so do we need to inform our regulator?
8. Are our termination rights for cause linked to repeatable IBS or insolvency failures ?
9. Does our business continuity exit planning and have scenario testing consider plausible scenarios within the supply chain ?
10. Do we understand the 4th parties availability and recovery requirement and how these align to the contracted 3rd party availability and recovery requirements?

INPUTS FROM OPERATIONAL RESILIENCE PROGRAMME

Input	Why?
Potential impact of large complex sub-outsourcing chains	Ability to oversee and monitor impact tolerances during operational disruption
Termination rights with the material outsourcer	A significant incident at a subcontractor could cause extensive and unmanageable operational disruption and could no longer stay within it impact tolerances (failure of KPI's, insolvency, repeatable non performance)

OUTPUT FROM THIS GUIDANCE STAGE

Output	Benefit
Identification of all end to end supply chain associated with delivering Important Business Service (IBS)	To ensure all possible material subcontractors are known at the onboarding and ability to object or terminate contract if a proposed subcontractor propose an increased risk
Written material outsourcing agreement to be clear on whether subcontracting is permitted and specific on authorisation especially when transferring data	Outline any services that we cannot subcontractor and any conditions for permissible subcontracting with the right oversight to ensure contract obligations are met to make sure no increased risks in the service
Notification on any material change to service	Notification period to accept or reject subcontractor

THIRD PARTY LIFECYCLE MANAGEMENT | GUIDANCE NOTES FOR ENABLING OPERATIONAL RESILIENCE WITH THIRD PARTIES

Document Title	Reporting
Objective of guidance	To support firms understanding of what ongoing monitoring and periodic reporting should be captured for both internal and regulatory reporting
Regulatory Clauses addressed	SS1/21 – Chapter 7 (Governance) FCA: SYSC 15A.7.1R/ SS1/21 – Chapter 8 (Self Assessment) SYSC 15A.6.1R SS2/21 – Chapter 4 (Governance and Record Keeping) SS2/21 – Chapter 10 (Business Continuity and Exit Plans)

AREAS OF CONSIDERATION

1. What audiences will need to see reporting (e.g. regulator, boards, business service owners)?
2. Are you using technology to support your operational resilience programme to enable automated reporting?
3. How are vulnerabilities across your business units being capture, tracked and formally closed? Third parties should form part of the wider reporting.
4. What information is required for your Important Business Service (IBS) self-assessments regarding third parties?
   - Mapping data – which suppliers support the IBS
   - Testing conducted and third party vulnerabilities identified
   - Plans and timescales for remediation activities
5. Metrics for consideration:
   - % overall supply base classified as critical (positioning metric)
   - % critical suppliers with identified vulnerabilities (tracked metric – aiming for 0%)
   - % critical suppliers completed annual assurance activities (annual metric aiming for 100%)
   - % critical suppliers with approved exit plans (should be 100%)
6. How will outcomes from periodic assessment and assurance (stage 3) be incorporated into existing TPRM monitoring frameworks?
7. What other information is reported on service issues/risks with supplier services e.g. service performance metrics, or incidents and severity

INPUTS FROM OPERATIONAL RESILIENCE PROGRAMME

Input	Why?
Classification of suppliers	To understand the criticality of the supplier to the Important Business Service
Findings from scenario testing as to specific third party vulnerabilities	To understand third party vulnerabilities which may take the business service out of impact tolerance
Contract provision regarding operational resilience obligations	What is expected from the supplier with regarding operational resilience/business continuity
Whether the supplier is themselves regulated	To align impact tolerances for the services and ensure supplier if fulfilling its regulatory obligations
Outcomes from 'Periodic Assessment and Assurance' Lifecycle stage	Ensure awareness and visibility of outcomes from periodic assessment and assurance activity

OUTPUT FROM THIS GUIDANCE STAGE

Output	Benefit
Information regarding capability and maturity of third parties supporting Important Business Services	For board oversight and understanding of ability to remain within impact tolerance
Third party vulnerabilities and remediation activities	For board oversight and understanding of ability to remain within impact tolerance