REPLY
GLUE

A PARADIGM SHIFT IN FINANCIAL SERVICE'S OPERATIONAL RESILIENCE: AN ARCHITECTURE LENS

Application Portfolio Management (APM) is a governance process for the effective management of IT application and technology landscape which has been adopted across industry and sector. Pragmatic implementation of APM with proactive and periodic portfolio assessment helps to identify IT portfolio health issues and opportunities to mitigate portfolio risk. In typical application governance process, applications are classified based on business criticality which is one of the key parameter to prioritise and direct IT investment to address any remediation or modernisation initiatives whether it is related to technology enhancement or business functional enhancement or enhancing non-functional requirements. APM and associated optimisation or rationalisation has evolved over the period of time with more focus on where the boundary is set in terms of its operational resilience and support, technology, infrastructure and integration points.

This whitepaper focused on financial services organisations to highlight the upcoming Prudential Regulation Authority (PRA) policy which fundamentally shifts operational resilience from application centric to service centric and at the same time broadens governance responsibility to Board and Senior Management Function of the organisation.

WHAT IS CHANGING IN FINANCIAL SERVICES?

To improve the operational resilience of PRA regulated firms and to protect wider UK financial sector and UK economy from the impact of operational disruptions, Prudential Regulation Authority (PRA) jointly with Bank of England (BoE) and Financial Conduct Authority (FCA), defined a draft policy in July 2018 to embed Operational Resilience into PRA's prudential framework through the Discussion Paper 1/18 - 'Building the UK financial sector's operational resilience' and subsequently made amendments to the proposed policy through Consultation Paper CP 29/19 Building operational resilience: Impact tolerances for important business services.

Operational resilience of financial sector becomes important considering dynamic and complex nature of the sector where it reliant on technologies and third parties, and especially leveraging cloud platform solutions where the cloud provider operates in number of different countries to deliver the business service. PRA expects the firms to be operationally resilient by preventing disruption, adapt systems and processes to provide service in the event of incident and, learn and evolve both from incidents and near misses. PRA's proposed operational resilience policy expects the firm to deliver improvements in three (3) key areas.

1. **Prioritising the things that matter**: Boards and Senior Management should prioritise activities that would pose risk to
    a. the stability of the UK financial sector,
    b. a firm's safety and soundness or
    c. appropriate degree of policyholder protection (in case of insurers)
2. **Setting clear standards for operational resilience**: Articulation of maximum level of disruption with time limit to recover from severe and plausible disruptions.
3. **Investing to build resilience**: Contingency arrangements to enable firms to resume the delivery of important business services.

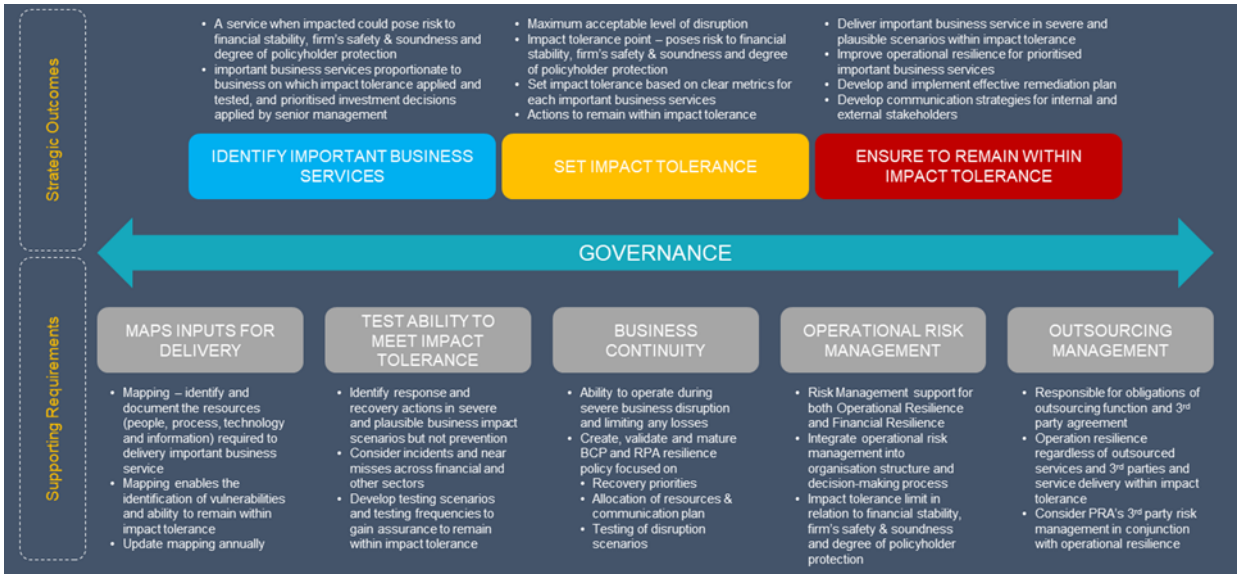
Considering this policy, operational resilience is no longer focused on individual business critical applications and resources but the wider business services provided to the user where a group of applications leveraged to deliver the service. This policy not only expects firms to identify important business services and associated impact tolerance limits but also to identify severe business disruption scenarios and the ability to test the scenarios to identify vulnerabilities to take remediation actions.

The proposed policy expected to be effective by second half of 2021 where the firms have 3 years to comply with this policy. PRA expects the firms to document self-assessment of their compliance with the policy where the accountability resides with firm's board and senior management team. Self-assessment expected to cover group-level where applicable and the outcome needs to be shared with PRA on request which broadly should cover the following.

- Methodology used for self-assessment
- Process and criteria followed to identify important business service
- Define impact tolerance limit for important business service with rationale
- Strategy to test the ability to deliver important business service within impact tolerance limit

- Scenario testing performed to identify vulnerabilities and identified actions plan to improve firm's ability to remain within impact tolerance

The below diagram summaries key elements in the PRA's proposed approach for the operational resilience policy covering two broad categories Strategic Outcomes and Supporting Requirements



1. STRATEGIC OUTCOMES

Firm's operational resilience needs active involvement of boards and senior management to make strategic decisions to comply with this policy and enable the firm to deliver important business service in severe disruption within impact tolerance. PRA framework approaches this in three (3) key steps.

Identify important business services:

PRA defines important business services as *"a business service is important if its disruption could pose risk to the firm's safety and soundness or financial stability, or in the case of insurers, the appropriate degree of policyholder protection"*.

This plays a key role in the overall approach because a business service delivery requires an end to end orchestration between mix of business critical and non-critical systems, which could potentailly include internal or group systems, 3rd party systems, outsourced systems and cloud based systems, and associated business processes. Through the business service approach, it would effectively guide to identify areas of risk – technical and non-technical, mitigation actions to overcome the risk and focused investments required to implement the mitigation action.

PRA recommends that while defining the criteria to identify important business services, firm need to consider various risk factors like

- Risk posed to financial stability of the firm
- Risk posed to safety and soundness of the firm and

- Risk posed to policyholder protection (in case of insurer)

Also, need to consider the granularity of the important business service where an impact tolerance can be applied and tested, and prioritisation could be made for investment decisions. PRA does not propose a definitive list of taxonomies of important business services as it differs from one firm to another. Example of important business services could be – a bank's payment service, a life insurer's payment of annuities or a retail bank's provision of ATM cash withdrawals to customers.

Set impact tolerance:

Per PRA's framework approach, the next logical step is to set impact tolerance for the identified important business services. Impact tolerance defined as maximum acceptable level of disruption to an important business service a firm can tolerate disruption. While defining impact tolerance, it needs to be assumed that the disruption will occur and it should not be based on cause, probability and frequency of disruption. This makes impact tolerance fundamentally different from firm's risk appetite.

Impact tolerance needs to be set at a point where it can be applied and tested, and it enables firms to set resilient requirements in terms of people, processes, technology, facilities and information for the delivery of important business service irrespective of who delivers the business service - internal, external and another entity within the group.

To remain within impact tolerance:

Final stage of strategic outcomes in PRA's approach is to delivery important business services within the identified impact tolerance limits. This could be achieved by performing mapping resources and testing the delivery of important business services during the identified disruption scenarios which will prepare firm to identify vulnerabilities and remediation actions to remain within impact tolerance irrespective whether the service been provided by its own group or through external third parties. After the new policy comes into effect, firms will have up to 3 years to take action to be compliant with this policy. Within this time, firm can develop and implement effective remediation plan for important business services which is unlikely to remain within defined impact tolerance limit. While developing plans to improve operational resilience and prioritising associate activities, the following needs to be considered

- Nature and scale of the risk that disruption to the important business service
- Time-criticality of the important business service and
- Prioritisation of important business service based on scale of necessary improvements

2. SUPPORTING DOCUMENT

To support the strategical delivery of important business services within impact tolerance limit needs set of documents - identified list of resources, processes and facilities related to important business service, test plan related to disruption scenario testing, business continuity plan, outsourcing plan and risk management plan. Here, we briefly touch on PRA's policy on supporting documents that aid to achieve strategic outcomes.

Maps input for delivery of important business service:

The process of identifying and documenting necessary people, process, technology, facilities and information required to deliver each of the important business service is called “mapping”. This process helps to identify vulnerabilities in terms of critical resources for the delivery of important business service.

Test ability to meet impact tolerance:

Defining impact tolerance alone would not make a firm compliance with this policy but it is essential to test firm’s ability to deliver important business service within impact tolerance where the focus should be on response and recovery actions but not on preventing incidents by designing and developing a testing plan which covers

- type of scenario testing
- range of scenarios where the firm exceeds impact tolerance
- frequency of scenario testing
- number of important business services tested and
- testing the availability and integrity of resources

Business Continuity:

Business continuity plan (BCP) aimed at the firm to be able to operate on an ongoing basis with limited losses while PRA’s Operational Resilience policy focuses on firm’s ability to deliver important business services and both these policies are closely linked and complement each other. For example

- Recovery prioritises the delivery of important business services within impact tolerance
- Business continuity planning focuses on the delivery of important business service with required resource allocation and communication planning
- Business continuity plans complement the testing of disruption scenario and related impact tolerance

Operational Risk Management:

Operational risk management supports both operational resilience and financial resilience, and effective operational risk management policy

- Have reduces the likelihood of operational incidents occurring
- Limit the losses in the event of severe business disruption and
- Sufficient capital to mitigate the impact when operational risk materialises

PRA approaches Operational risk in two ways and it does not have associated capital requirement or affect operational risk capital policy or adding considerations to capital calculations

- Firm’s ability to respond to and recover from disruptions, assuming failures will occur.
- Take action to provide important business services within impact tolerances through severe disruption

Outsourcing Management:

PRA’s policy on outsourcing and third-party risk management complements operational resilience policy where PRA’s approach is to consider both these policies in combination. PRA expects firms to be operationally resilient

regardless of any outsourcing arrangements or use of third parties and it should not undermine firm's ability to delivery important business services within their impact tolerances irrespective of the service been delivered wholly or in part by third parties - other entities within their group or external providers.

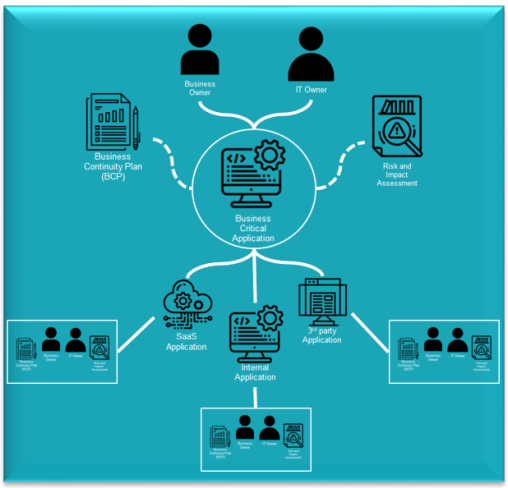
3. GOVERNANCE

From governance point of view, boards and senior management plays a vital role as they have the overall accountability of for policy compliance and have to approve the identified business services and defined impact tolerance limits. The self-assessment related to PRA's operational resilience policy is a periodic activity where board has the responsibility to review and approve regularly, and with sufficient skills and knowledge then can challenge senior management constructively to meet is responsibility.

IMPACT OF PRA'S OPERATIONAL RESILIENCE ON APPLICATION GOVERNANCE

In a typical application portfolio management / governance, irrespective of sector / industry, for better management of applications, they are classified into different tiers for the identification and allocation of application ownership, support resource requirements and associated process documentations. Based on the maturity of the organisation, application portfolio managed through an APM tool or a combination of Enterprise Architecture (EA) tools for capturing and managing a wide variety of application parameters including but not limited to

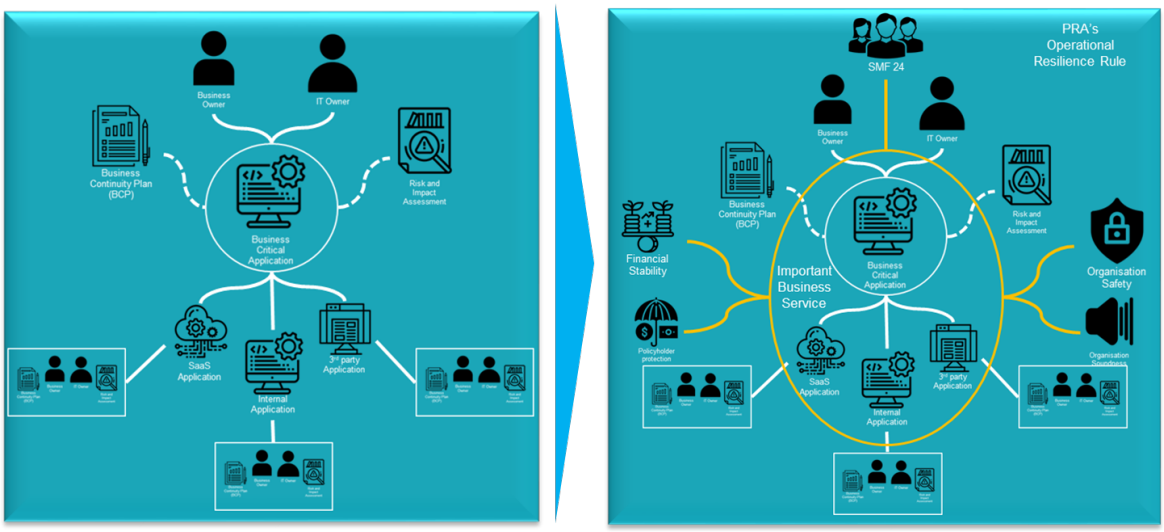
- Application ownership - Technical and Business ownership, supporting business function / vertical, Business criticality
- Application configuration management (Configurable Items) - Technology and infrastructure components, Software and technology currency
- Application integrations - internal and external
- Operational support - Service Level Agreement (SLAs), Recovery Parameters (RTO, RPO)



Considering the new policy, the focus for banking and insurance firm is to enable important services operationally more resilient and to be delivered within the impact tolerance level while limiting any wider organisational stability, safety, soundness and policyholder protection which implicitly enforces all the associated application operationally resilient irrespective of application tier.

There are key differences between application centric and service centric way of governance. Some of the key differences are

- **Level of Exposure**: In the current world, if there is an impact to an application, based on the business criticality of the application it might get elevated up to the Business Unit (BU) head and in rare cases it might reach to the CIO. In the new world, delivery of the important service is agreed and approved at senior management level – Board Members and / or CIO and more importantly they are accountable for the delivery important business services.



Governance focus shift from business critical application to business critical service

- **Level of Impact Isolation**: In the application centric world, the purview of the impact is viewed at the application level but in the service centric world, any disruption to the important business viewed at the wider organisation level in terms of financial stability, safety and soundness of the organisation.
- **IT Investment Prioritisation**, as part of the application portfolio management, IT investment is prioritised on application centric opportunities that would yield higher business benefit or to mitigate technology risks or modernise the application however the new policy would prioritise IT investment on the service components that could cause major impact to the delivery of the important service.
- **Operational Support and Business Continuity**: Prior to the new policy, operational support documentation and business continuity plan is more focused around the applications and to comply with this policy, business continuity needs to be viewed holistically at organisational in combination with existing business continuity plan.
- **Level of Architecture Impact Assessment**: From architecture point of view, application architecture impacts are assessed at the application level but going forward architecture impact needs to be assessed at the wider service level.
- **Disruption Avoidance vs Occurrence**: In the current application portfolio, operational resilience is focused on to reduce the liklihood of operational incidents and minimise the loss in the event of disruption occurring however the new policy mandates the firms to plan business continuity to respond and recover from disuption considering that disruptions will occur.
- **Level of Accountability**: For 3rd party or vendor managed applications, vendors are accountable to deliver the application functionality within the SLA however in service centric world, board and senior management function is accountable for the delivery of the important service within impact tolerance irrespective of whether it being delivered by internal IT team or 3rd party vendor or cloud partner or combination of all.

CONCLUSION

In summary, the PRA's Operational Resilience policy is for the betterment of financial or insurance firms where it widens the focus from application to delivery of important business services within the identified tolerance limit. Prior to investing time and effort to comply with the policy and to identify Important Business Services, there are some key areas needs to be focused to avoid any red herring and these areas where Glue Reply has extensive experience in helping clients, like

- **Business Capability Model Development and Alignment**: Need to assess and develop a business capability model for the enterprise and need to assess and identify any capability overlapping or shared services with Group function where applicable. A baselined business capability model is a key aid in multiple areas especially in identifying firm's strategy alignment and map statutory obligations and associated legislations, and at the same time it defines foundation to identify important business services.
- **Compensatory Process Assessment and Automation**: Assess and identify any existing manual process that are in-place as this might be one of key area which would manifest as a key blocker to comply with the new policy. It is essential to identify appropriate process automation for the delivery of important business services.
- **Application Portfolio Rationalisation**: While the new policy focuses on important business service and how it can be delivered during disruption. At the same time, it is paramount to have a "Single Source of Truth" of existing application portfolio and associated risks and opportunities through performing an Application Portfolio Rationalisation exercise which would set a foundation for the identification of important business services and associated Self-assessment mandated by PRA.

For the PRA mandated Self-assessment, it is also recommended to leverage a 3rd party to assess the compliance against PRA's Operational Resilience policy for an unbiased outcome.