Disaster Recovery Policy Exceptions

QUICK REFERENCE GUIDE

For:	Area Risk Reviewers and Service Quality Leads
Type:	Support Decisioning

May 24, 2022

Contents

Purpose and Objective

The objective is to publish an enhanced Business Continuity Policy exception process that includes risk leader inputs into the granting of policy exceptions when business teams wish to defer developing disaster recovery strategies and plans for their critical applications.

The purpose of this quick reference guide is to provide Area Risk Leaders and Service Line Quality executives with critical background information that will equip them to make informed risk-based business decisions on whether to approve disaster recovery policy exceptions or to recommend disaster recovery to the Application owner.

The Problem with Business Continuity Policy Exceptions

EY's Code of Connection and Business Continuity Policy require that business teams develop recovery strategies and Disaster Recovery plans (DR plans) for all "critical" applications (i.e. applications requiring less than 48 hours to recover from a business disruption). There continue to be many situations where the Application owner has declined to implement the recovery strategy and corresponding DR Plan and has instead sought a policy exception. Three primary root causes for failing to invest in DR solutions include:

- Investing in recovery strategies is not considered a part of "total cost of ownership" of the Application, and is therefore not planned nor budgeted for
- Time required to complete the DR planning conflicts with business priorities
- Historically, the policy exception process required only business application owner approval without additional awareness of senior risk and service line leadership

Potential impacts of a Business Continuity Policy Exception

In situations where critical application owners decline to develop a DR strategy or DR plan, these critical applications will only be recovered on a "best effort" basis. Given that Enterprise Technology (ET) or Client Technology (CT) would need to acquire infrastructure to support these critical applications **before** recovery actions could commence, the applications could be down for as long as 30 days, or longer.

Given the potential for ransomware attacks and the constantly evolving geo-political climate in countries where we do business, our ability to serve clients, and ultimately the Firm's revenue and public image could be severely compromised if a critical application cannot be timely recovered due to a business decision not to invest in a disaster recovery strategy.

Due to the potentially "high" risk to the Firm resulting from policy exceptions of critical applications, IT Risk Management has revised the policy exception process to include discussion with risk leadership and service line quality team members for all policy exception applications.

Considerations by Area Risk Leads and Service Line Quality Reviewers

Upon being routed the Application owner's request for a policy exception, the reviewer should consider the following when evaluating whether an exception request should be approved:

1. The Recovery Time Objective (RTO) and Recovery Point Objective (RPO) established during the Business Impact Assessment (BIA)
2. The financial impact estimated for a 30-day business function outage vs. the costs of implementing DR
3. Whether the business has defined a near-term workaround for performing the function without the business application
4. Whether the business/application owner has committed to developing an Application Recovery plan, which is a requirement of being granted exception, and the targeted timeline for completion

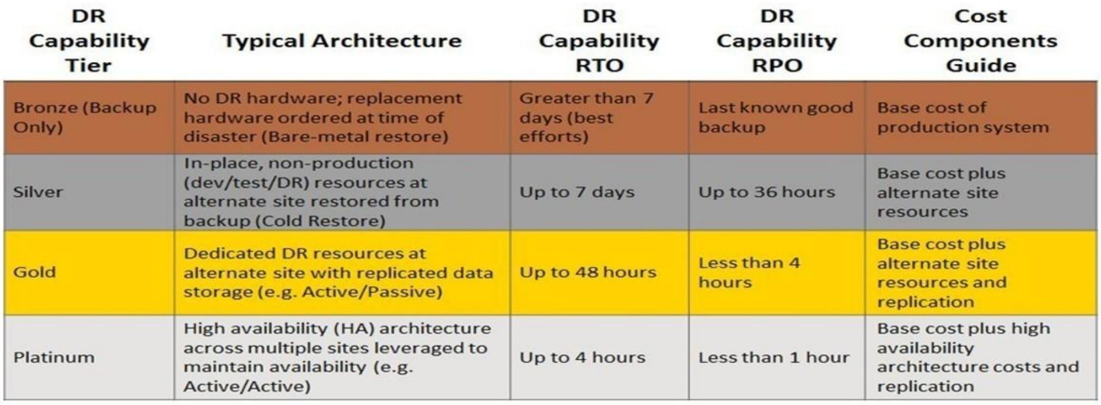
Each of these considerations is discussed in the sections that follow.

The Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are established during the application's Business Impact Assessment (BIA)

What is a BIA?

- A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption.
- It quantifies -- as well as qualifies -- the vulnerabilities and the impacts to applications and/or business processes resulting from a major event which would cause a disruption of the daily work activities.
- Business Impacts to consider include:
    - Lost or delayed sales and income, Regulatory fines,
    - Contractual penalties or loss of contractual bonuses,
    - Customer dissatisfaction or defection, Delay of new business plans, Increased expenses

- The BIA identifies time-critical processes and their recovery priorities and interdependencies based on approved recovery timelines known as the RTO and RPO:
    - RTO = The maximum amount of time that a function or an application can be unavailable before an unacceptable financial or operational business impact would result
    - RPO = The maximum amount of data loss that can be absorbed before an unacceptable business impact would occur
- All applications sent reviewers have been deemed “critical applications by the BIA process given the critical business processes they support.
- Critical applications have RTOs less than or equal to 48 hours and RPOs less than or equal to 4 hours and are required by policy to have DR solutions unless a policy exception is granted.
- The RTOs and RPOs of critical applications will only be achievable if a DR strategy and DR plan is implemented. If a policy exception is approved, the actual recovery time could be greater than 30 days.



DR Capability Tier	Typical Architecture	DR Capability RTO	DR Capability RPO	Cost Components Guide
Bronze (Backup Only)	No DR hardware; replacement hardware ordered at time of disaster (Bare-metal restore)	Greater than 7 days (best efforts)	Last known good backup	Base cost of production system
Silver	In-place, non-production (dev/test/DR) resources at alternate site restored from backup (Cold Restore)	Up to 7 days	Up to 36 hours	Base cost plus alternate site resources
Gold	Dedicated DR resources at alternate site with replicated data storage (e.g. Active/Passive)	Up to 48 hours	Less than 4 hours	Base cost plus alternate site resources and replication
Platinum	High availability (HA) architecture across multiple sites leveraged to maintain availability (e.g. Active/Active)	Up to 4 hours	Less than 1 hour	Base cost plus high availability architecture costs and replication

Critical Applications – DR Required

- The BIA will prioritize applications into 4 categories:
  - Platinum- RTOs of 4 hours or less, RPO of 1 hour or less
  - Gold- RTOs of 48 hours or less, RPOs of 4 hours or less
  - Silver – RTOs of up to 7 days, RPOs up to 36 hours
  - Bronze – RTOs greater than 7 Days, RPO= Last good backup
- Gold and Platinum Applications are considered "Critical" and will be the source of all DR policy exception requests
- The reviewer should exceptionally scrutinize Platinum applications that are seeking policy exception. Platinum applications would have the most serious consequences to the Firm if they were lost and such policy exception requests should be closely scrutinized before being approved.

The Financial Impact estimated for a 30-day business function outage vs. the costs of implementing disaster recovery solution

What is Financial Impact?

- ➢ The BIA asks application/business owners to estimate the potential lost or delayed revenue, contractual penalties or regulatory fines that could occur if there were an outage of the critical business application or process.
- ➢ A potential financial impact of $250 million or more would be considered "major".
- ➢ Major financial impacts can be a driver of shorter RTOs for the critical business applications.

- The application should reference the potential financial impact for up to 30 days as determined during the BIA.
- Global business impact criteria have established that a "major" and unacceptable level of financial impact is $250 million.
- A 30-day outage is realistic for any application that does not have a pre-provisioned disaster recovery solution, Thus, the reviewer should be especially cautious of financial impacts that could approach major within 30 days.
- Given that recovery strategy development is generally based on a cost vs. benefits analysis, the reviewer must also consider the costs of implementing the mitigating DR strategy.
- Where the potential financial impact exceeds the costs of implementing the solution, the reviewer should question whether an exception is appropriate, unless the function owner agrees to implement other

Whether the business has defined a near-term workaround for performing the function without the critical business application

What is a Workaround?

- In some situations, the business function can carry on without the critical business application for a short period of time. In these instances, business teams document workaround procedures that allow them to perform the critical processes manually until the critical system is restored.

- Given that the application is required to support a critical business process, the function owner must design a workaround process to continue the process manually for up to 30 days and document the same in the Application Recovery Plan.
- A key consideration is whether the business has identified a workaround process that could be deployed following a disruption of the critical application.
- The risk reviewer should be especially cautious of any critical application that does not have a workaround process that can be immediately activated. The absence of a workaround is a key driver of why DR needs to be developed and the lack of a workaround exposes the Firm to substantial business risk if a DR strategy/plan is deferred.
- For situations where there is no workaround available, the reviewer should only approve the exception request if the business owner has proposed a comprehensive action plan, with accountabilities and target dates for developing the required Disaster Recovery solution within the next twelve months.

Whether the business/application owner has committed to developing an Application Recovery Plan, which is a requirement of being granted exception, and the targeted timeline for completion

What is an Application Recovery Plan?

- The Business Continuity Policy requires that any application owner supporting a critical business application that seeks a policy exception to defer developing a DR strategy and DR Plan must develop an Application Recovery Plan
- The Application Recovery Plan must include the inventory of infrastructure components that will need to be acquired at time at the time of disruption and the detailed technical procedures describing how to rebuild the application once infrastructure is acquired.

- The final key decision point for the reviewer to consider is whether the application owner has an Application Recovery Plan.
- The Application Recovery Plan is a policy requirement for any critical business application that is seeking a Disaster Recovery exception.
- The plan should be completed using the prescribed template and submitted to the Business Continuity Team for review, approval and publishing no later than 90 days from the date of the approval of the policy exception.
- For the reviewer to approve the policy exception request, it is important that the application owner submits a milestone action plan with task owners, milestones and target dates with his/her request for policy exception.
- Absent the action plan, the request should be redirected back to the Application Owner for revision.

Decisioning

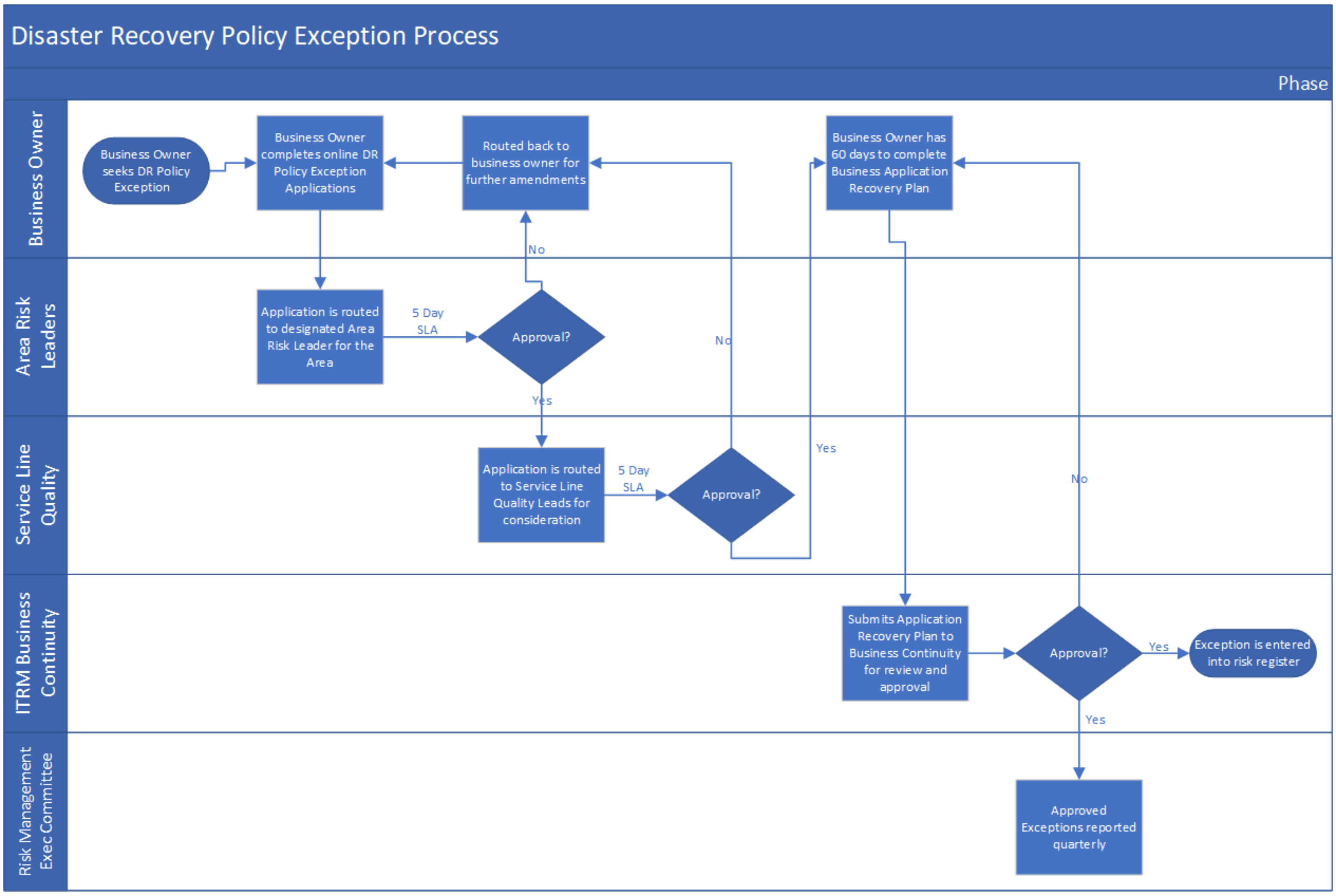
Should the Service Line Quality and/or Area Risk Leaders believe that further support/details are required prior to approving the exception, the exception request can be routed back to the Business/Application owner (with comments) for further actioning by the Business/Application Owner. The decisioning statuses are limited to:

- In Process (review is in process)
- Approved
- Proposed for Further Review

Following an approval of the policy exception by the Service Line Quality and Area Risk Teams, the Business Continuity Team will log the exception as an ongoing risk in the IT Risk Register. The application owner will complete the Application Recovery Plan within the agreed upon target dates and submit to the Business Continuity team to review.

Exceptions are only valid for 365 business days, after which time the exception will expire, triggering another requirement to reapply for the exception.

Appendix – DR Policy Exception Workflow


Disaster Recovery Policy Exception Process
Phase
Business Owner
Area Risk Leaders
Service Line Quality
ITRM Business Continuity
Risk Management Exec Committee
Business Owner seeks DR Policy Exception
Business Owner completes online DR Policy Exception Applications
Routed back to business owner for further amendments
Business Owner has 60 days to complete Business Application Recovery Plan
Application is routed to designated Area Risk Leader for the Area
5 Day SLA
Approval?
No
No
Yes
Application is routed to Service Line Quality Leads for consideration
5 Day SLA
Approval?
Yes
No
Submits Application Recovery Plan to Business Continuity for review and approval
Approval?
Yes
Exception is entered into risk register
Yes
Approved Exceptions reported quarterly