# Disaster Recovery Standard

## Table of Contents

[Related Policy 3](#_Toc488216562)

[Purpose 3](#_Toc488216563)

[Introduction 3](#_Toc488216564)

[Standard Statements 4](#_Toc488216565)

[1. Roles and Responsibilities 4](#_Toc488216566)

[2. The DR environment 5](#_Toc488216567)

[3. General Recovery Terminology 5](#_Toc488216568)

[4. General Recovery Terminology 7](#_Toc488216569)

[5. Application Criticality 8](#_Toc488216570)

[6. Global DR Planning Requirements 10](#_Toc488216571)

[7. Global DR Exercising Requirements 11](#_Toc488216572)

[8. Change Management 14](#_Toc488216573)

[9. Training and Awareness 14](#_Toc488216574)

[10. Maintenance and Management Reporting 15](#_Toc488216575)

[11. Business Partners 15](#_Toc488216576)

[Legal Conflicts 15](#_Toc488216577)

[Exceptions 16](#_Toc488216578)

[Comments 16](#_Toc488216579)

[Related Documents 16](#_Toc488216580)

[References and Mandates 16](#_Toc488216581)

[Document Control Information 16](#_Toc488216582)

[Revision History 17](#_Toc488216583)

[Appendix A: Global DR Approach: Criticality, RTO/RPO and Exercising Requirements 1](#_Toc488216584)

## Related Policy

* 401.00 Disaster Recovery Policy

## Purpose

The Alight Global Disaster Recovery Standard (“Standard”) establishes Alight’s Global Disaster Recovery (“DR”) definitions and requirements. The detailed definitions of key DR terms used to communicate and discuss DR related issues globally provide Alight’s global DR community with a common language. Additionally, this document discusses, in detail, the global DR requirements for planning, exercising and reporting.

To achieve the vision of Alight’s global DR program, the global DR organization should consistently:

* Provide well planned, exercised and documented disaster recovery for internal and client facing business critical systems;
* Provide guidance to the business on defining the right levels of protection and corresponding recovery strategies for their critical applications;
* Identify, qualify and quantify Alight’s DR risks to the appropriate business and IT groups
* Anticipate, guide and accommodate the changes in business requirements for increased/decreased levels of resilience;
* Integrate with Business Continuity (BC) processes where applicable;
* Align DR plans and DR spend with business objectives and priorities;
* Deliver a global DR program in a cost efficient manner.

## Introduction

With the increasing importance of information technology for the continuation of business critical functions, protecting and recovering an organization's data and IT infrastructure in the event of a disruptive situation has become a more visible business priority.

A “disaster” is any event or incident that prevents essential application or data center operations beyond downtime tolerances at a specific location. A “disaster“ forces the move of an individual application or entire data center operations to a different geographic location in order to recover critical operations in a more acceptable timeframe. Alight’s DR plans document and manage the process of recovering applications and/or datacenter operations to a different geographic location.

Incidents that can be resolved within the tolerated downtimes without moving operations to a different geographic location are not considered disasters. These incidents are not covered in Alight’s DR plans, and are not in scope in the global DR program.

Disaster Recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

Disaster Recovery planning includes planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. Since a serious incident can occur at any time, it is vital that the organization takes a proactive approach to the development, exercising and maintenance of disaster recovery plans. Disaster Recovery plans should be well practiced and exercised so that the key players are familiar with the specific actions they will need to take, and so that the recovery strategies are fully validated should a disaster occur. Disaster Recovery plans must also be adaptable and routinely updated to reflect changes in people, process, and/or technology.

## Standard Statements

### Roles and Responsibilities

* 1. Alight Global Business & Technology Resilience Program Office

The Alight Global Business & Technology Resilience Program Office (“BTR Program Office”) is the global governing body for Disaster Recovery Planning. The Global BTR Program Office is responsible for providing guidance and standardized frameworks for disaster recovery plan development, maintenance and exercising and for providing and maintaining a solution for centralized plan retention. The BTR Program Office will provide periodic status reports to senior management on the progression of disaster recovery plan development, maintenance, and exercising.

* 1. Alight Businesses

All businesses within Alight are responsible for developing, maintaining, and exercising disaster recovery plans that adhere to the policy and standards set forth by Alight’s Global BTR Program Office.

Each business unit is responsible for identifying key individuals and succession plans to ensure the following disaster recovery management, delivery, and support roles are filled.

* + 1. C-Level Executive or Country Manager: has overall responsibility for the strategic and operational management of the organization and will serve as the DR Program sponsor, is the ultimate decision maker over budget, and is accountable for all disaster recovery planning within all business units under their authority.
    2. Executive Business Leader: is the executive sponsor within a specific business and is responsible for determining planning/recovery budget, prioritizing critical services/systems, identifying plan owners, and approving recovery strategies. They will also be a decision maker in the execution of disaster recovery plans.
    3. Executive Plan Owner: must be of management level and is responsible for the development and management of disaster recovery plan(s). They are required to participate in annual exercises and plan sign-off and will be responsible for executing recovery strategies in the event of a significant technology disruption.
    4. Plan Coordinator: is responsible for coordinating the development and management of disaster recovery plan(s). They are required to participate in annual exercises and publishing plan documentation. The plan coordinator may also be called upon to assist in the execution of recovery strategies in the event of a significant technology disruption.
    5. All Staff: are responsible for cooperating with the implementation of this policy as part of their normal duties and responsibilities or as assigned within specific disaster recovery plans.

### The DR environment

* 1. The intent of the approach to DR is to keep the DR and production environments in sync.
  2. The DR environment is comprised of all the hardware, software, networking components and all of the associated services that ensure connectivity, functionality and production that are required for applications, systems, and infrastructure, which enables DR to function properly at an alternate site.
  3. The DR environment is considered production. Change Management, Configuration Management, and Release Management processes should reflect and account for the impact on DR environments whenever changes are introduced to production environments.
  4. DR environments are subject to the same QA/UAT requirements established for their respective production environments. In a DR exercise or a real life recovery, all pre-production validations should be executed on a DR environment before the DR environment is made available to assume production operations. The time to execute all pre-production validations must be factored in when assessing the ability to meet an application’s Recovery Time Objective.

### General Recovery Terminology

* 1. Recovery Time Objective (“RTO”): The RTO is the maximum downtime tolerated for an application, stated in hours. The RTO should be thought of as a “must have” and not a “nice-to-have”. Properly calculated RTOs with a “must have” approach (through a DR Criticality Analysis, Business Impact Analysis, or other analysis), can help right-size the investment in the application’s DR strategy and infrastructure.
     1. The RTO of an application is provided by the business to set the expectation with the Information Technology team, and should be reflective of the investment the business is willing to make in a DR strategy and infrastructure.
     2. DR investments, recovery strategies, and infrastructure will ensure that RTOs are met. When an RTO cannot be met (as a result of exercising or an actual disaster recovery), the DR investments, recovery strategies, and infrastructure or RTO should be re-evaluated.
  2. Recovery Point Objective (“RPO”): An RPO is the maximum amount of data loss tolerated for an application, stated in hours. The RPO also defines the tolerated delay for replicating all changes (system, application, database, security, network, etc.) from the production environment to the DR environment.
  3. The RPO should be thought of as a “must have” and not a “nice-to-have”. Properly calculated RPOs with a “must have” approach (through a CR Criticality Analysis, a Business Impact Analysis, or other analysis) can help right-size the investment in the application’s DR strategy and infrastructure.
     1. The RPO of an application is provided by the business to set the expectation with IT, and should be reflective of the investment the business is willing to make in a DR strategy and infrastructure.
     2. DR investments, recovery strategies, and infrastructure should ensure that RPOs are met. When an RPO cannot be met (as a result of DR exercising or an actual disaster recovery), the DR investments, recovery strategies, and infrastructure should be re-evaluated with the business.
  4. Recovery Scope and Scale Objectives: The Recovery Scope and Scale Objective lists, in detail, the application functionality that should be restored in case of a disaster.
     1. The Recovery Scope Objective allows IT and the business to break down an application’s functionality, or modules, and decide, where technically possible, to selectively recover specific application functionality or modules and exclude others. It also allows the business to set different RTOs for different modules/functionality. When technically achievable, defining the Recovery Scope Objective of an application allows IT and the business to prioritize the chronology of the recovery process of an application.
     2. The Recovery Scale Objective lists the relative performance required and expected from the DR environment compared with the level of performance provisioned for the production environment. The Recovery Scale Objective is expressed as a percentage. The Recovery Scale Objective allows the business to potentially reduce the cost of the DR equipment if it is willing to accept DR performance levels lower than what the production environment provides. The Recovery Scale Objective of an application is provided by the business to set the expectation with IT.
        1. Recovery Scale Objectives lower than 100% indicate that the business is accepting DR performance levels that are lower than those of the production environment.
        2. The DR plans for applications with Recovery Scale Objectives lower than 100% will include plans and logistics of provisioning additional resources (system, network, etc.) to the DR environment when the performance is deemed unacceptable.
  5. Recovery Time Achievable (“RTA”): The RTA of an application is obtained and documented after a successful DR exercise at the highest applicable maturity level. Only successful DR exercises can provide meaningful RTAs.
  6. The RTA for an application will meet or exceed the RTO for the same application. An RTA that does not meet the RTO indicates that although the DR exercise was completed, the DR readiness of the application is not at an acceptable level and the recovery strategy and/or procedures should be re-evaluated with the business.
  7. Failover (or Failover Operations) refers to the actions related to “failing over” applications, systems and infrastructure, a group of applications, or entire data center operations from the Production Site to the DR Site in case of a disaster.
  8. Failback or (Failback Operations) refers to the actions related to “failing back” an application, a group of applications, or entire data center operations from the DR Site to the Production Site when the decision is made to switch operation back to the Production Site.
  9. Recovery Site / DR Site: the facility hosting the DR environment.
     1. The DR Site should not be subject to the same local disaster or business disruption as the Production Site. In order to achieve that, country/regional best practices combined with, when possible, local threat assessments to determine the appropriate distance between the DR Site and the Production Site. Country and regional best practices for appropriate distances between production and DR Sites are mainly shaped by the geography, power grid layout, and local susceptibility to natural and man-made disasters.

### General Recovery Terminology

* 1. Tier 0: Typically infrastructure components that are relied upon for day-to-day IT operations, typically owned and managed by the global AITS organization, and are expected to provide close to 100% availability across Alight’s global production network. They are also very critical in recovery operations. The RTO is </=12 hrs or as defined by the shortest RTO of the applications(s) or system(s) that depend on this technology/infrastructure. Examples include but are not limited to:
     1. Network
     2. Telecomm
     3. Storage/replication
     4. Naming services (i.e., DNS)
     5. Authentication/authorization
        1. Active Directory
        2. LDAP
  2. Tier 1 Applications: Applications deemed the most critical globally. Based on the application criticality framework section, these applications scored high enough to be included in the Tier 1 application group. These applications are critical in maintaining Alight’s revenue and reputation, as well as Alight’s ability to meet client and/or government deadlines. Tier 1 applications have the highest levels of DR requirements, visibility, and responsibility as follows:
     1. The Recovery Time Objective (RTO) of a Tier 1 application should not exceed 48 hours.
     2. The Recovery Point Objective (RPO) of a Tier 1 application should not exceed 24 hours.
     3. Recovery Scale and Scope Objectives should be reconfirmed as acceptable with the business during the annual DR exercises based on user feedback.
  3. Tier 2 Applications: Applications essential to Alight’s business, but not significantly affecting Alight’s revenue, reputation, or the ability to meet external deadlines (see section 3). These applications are not as critical as Tier 1 applications, but are essential in maintaining Alight’s ability to do business. Below are the global DR program requirements for Tier 2 applications:
     1. The Recovery Time Objective (RTO)of a Tier 2 application should not exceed 72 hours
     2. The Recovery Point Objective (RPO) of a Tier 2 application should not exceed 24 hours.
     3. Recovery Scale and Scope Objectives should be reconfirmed as acceptable with the business during the annual DR exercises based on user feedback.
  4. Tier 3 Applications: Applications that are important to Alight’s business, but negligibly affect Alight’s revenue, reputation, or the ability to meet external deadlines are defined as Tier 3 applications. Below are the global DR program requirements for Tier 3 applications:
     1. The Recovery Time Objective of a Tier 3 application should not exceed 1 week
     2. The Recovery Point Objective of a Tier 3 application should correspond to the last successful backup.
     3. Recovery Scale and Scope Objectives should be reconfirmed as acceptable with the business during the annual DR exercises based on user feedback.

### Application Criticality

The Alight Application Criticality Framework was put together to establish a global standard for tiering applications. It helps the business understand “how” critical an application really is, and can assist in justifying or modifying the DR spends for a particular application. All applications must be put through the Alight Application Criticality Framework to assign an application criticality score and tier.

* 1. Fields to Be Used in Determining Application Criticality
     1. Today, application criticality is determined using three values:
        1. Revenue Impact
        2. Reputation Impact
        3. Timeline Impact
     2. Six additional fields were identified to paint a holistic picture of how critical an application really is. Following is a brief overview of all nine values that will be used to determine application criticality:
        1. Alight Application Category: every application is assigned one category from the list below:
           1. Revenue Generating: Revenue Generating applications can potentially be highly critical.
           2. Mandatory: Mandatory applications can potentially be highly critical.
           3. Business Unit Enabling: BU Enabling applications are viewed by the global DR program office as not as critical as Mandatory applications.
           4. Corporate/Enterprise: These applications can span the “not critical” to the “highly critical” spectrum.
        2. Business Units with Users: The more Business units with users that use an application, the more critical the application is considered.
        3. Internal Users: The higher the internal user count (or a relevant high/medium/low assessment), the more critical the application can potentially be.
        4. External Users: The higher the external user count (or a relevant high/medium/low assessment), the more critical the application can potentially be.
        5. Revenue Generated: The higher the revenue generated (or a relevant high/medium/low assessment), the more critical the application can potentially be.
        6. Revenue Impact: Possible values when the application is down for more than 24 hours in the most critical time of the year:
        7. Reputation Impact: Possible values when the application is down for more than 24 hours in the most critical time of the year:
        8. Timeline Impact: Possible values when the application is down for more than 24 hours in the most critical time of the year:
        9. Degree of Dependency: The higher the degree of coupling/dependency to/from other systems, the more critical the application can potentially be.
  2. Criticality Scoring – Because the four Alight application categories (see section 5.1.2.1 above) are mutually exclusive, an application can only have one Alight application category. As a result, only three Impacts can be applicable to any given application, as illustrated below. The IT and external impacts are common to all applications, whereas either the Revenue Impact or the Internal Impact can be applicable to a single application.
     1. The criticality score of an application is calculated as follows:
        1. For every applicable Impact, add the applicable criteria scores.
        2. Multiply the total points for an Impact by the Impact’s relative weight.
        3. Add up all the impact scores for the application. The resulting total criticality score determines the tier that will be assigned to the application.

### Global DR Planning Requirements

* 1. DR plans are essential documents that contain the needed information for proper failover and failback operations. The DR plans should be detailed enough so that, at time of disaster, no information gathering is required and decision-making is clear. Ideally, the only decision that should be made is whether to declare a disaster or not. Following a disaster declaration, the actions should be scripted, in detail, in the DR plans based on validated recovery procedures through proper DR exercising. Eliminating the need to make decisions and gather information or data following a disaster declaration improves the chances of meeting the prescribed RTOs.
  2. DR planning requirements:
     1. All Tier 1, 2, and 3 application disaster recovery plans should use the globally approved template or an alternate globally approved framework that contains the standard Alight Global Application DR Plan components.
     2. Embedding documents into the DR plans is not allowed. Any useful information deemed necessary for the failover/failback procedures should be included as-is in the DR plan. If the information is too large, appendices can be used or the plans can link to appropriate documents in an approved resilient location (i.e. NOT network drives).
     3. Detailed DR Plan Sections
        1. Recovery Strategy Overview – detailed discussion of disaster scenarios, recovery scope objectives, recovery scale objectives, and overview/diagram(s) of recovery strategy
        2. Application Description – business description of application uses and end users
        3. Application Criticality Tier – assigned and agreed tier based on the outcome of the application criticality framework
        4. Production Location – location and configurations of production locations and system(s)
        5. Recovery Location – location and configurations of the recovery location and system(s)
        6. Recovery Time Objective
        7. Recovery Point Objective
        8. Disaster Recovery Team(s) – listing of recovery team members with specific roles and responsibilities. Contact details and escalation procedures for recovery team(s)
        9. Interdependencies – list and/or diagrams of interdependent infrastructure, services, and/or applications and systems
        10. Detailed Recovery Procedures – “step by step” procedures to recover the system, application, or infrastructure
        11. Plan Maintenance & Exercising History
     4. An approved copy of the plan needs to be available to or submitted to the appropriate Regional BC Manager. If required, evidence of approval by the relevant parties should be on file with the documentation.

### Global DR Exercising Requirements

1. 1. DR Exercising Requirements: DR exercising is essential in building the confidence needed that applications can, in fact, be recovered after real disasters, in the timeframe as provided by the business. DR exercising also provides an opportunity for the recovery teams to practice and get familiar with the specific actions they will need to take during the recovery process. Recovery teams can be comprised of Alight and non-Alight staff, and DR exercising presents these recovery teams with opportunities to clearly define and validate their roles and responsibilities. Most importantly, DR exercising ensures that the recovery strategies and procedures are fully validated should a disaster occur. Validating recovery strategies and procedures proves that they are viable.

This section discusses Alight’s global DR exercising maturity models, definitions, and requirements.

* + 1. Alight’s DR Exercising Maturity Models
       1. Replicated and non-replicated environments utilize different recovery procedures, and consequently, have different exercising maturity models. Below is an outline of the major milestones in the recovery process of a replicated environment:
       2. Based on the outline above, Alight’s DR exercising maturity model for replicated environments is as follows:
          1. Exercising Maturity Level 1:

Stop replication from production to DR

Bring up data at DR Site

Validate DR environment (UAT, etc.)

* + - * 1. Exercising Maturity Level 2:

Exercising Maturity Level 1 requirements

Failover network from production to DR

Validate network changes

Run production operations from the DR Site

* + - * 1. Exercising Maturity Level 3:

Exercising Maturity Level 2 requirements

Setup data replication from DR to production

* + - * 1. Exercising Maturity Level 4:

Exercising Maturity Level 3 requirements

Stop replication from DR to production

Bring up data at Production Site

Validate production environment (UAT, etc.)

* + - * 1. Exercising Maturity Level 5:

Exercising Maturity Level 4 requirements

Network failback to production

Validate network changes

Run production operations from Production Site

Setup data replication from production to DR

* + - 1. Environments that rely on recovery from tape as their primary recovery strategy (non-replicated environments) or employ recovery processes that are fundamentally different from the ones utilized by replicated environments, require a different maturity model. Below is an outline of the major milestones in the recovery process of non-replicated environments:
      2. Based on the outline above, Alight’s DR exercising maturity model for non-replicated environments is as follows:
         1. Exercising Maturity Level 1:
* Successfully recover data from tape at DR Site
  + - * 1. Exercising Maturity Level 2:
* Exercising Maturity Level 1 requirements
* Validate DR environment (UAT, etc.)
* Run production operations on DR environment with the production environment still up and running
  + - * 1. Exercising Maturity Level 3
* Exercising Maturity Level 2 requirements
* Validate DR environment (UAT, etc.)
* Failover network
* Validate network changes
* Run production operations from DR Site
  + - * 1. Exercising Maturity Level 4:
* Exercising Maturity Level 3 requirements
* Network failback to production
* Validate network changes
  + - * 1. Exercising Maturity Level 5:
* Exercising Maturity Level 4 requirements
* Recover tape at Production Site
* Validate production environment (UAT, etc.)
* Network failback to production
* Validate network changes
* Run production operations from Production Site
  1. Alight’s DR Exercising Requirements
     1. Replicated environments should strive to exercise at Maturity Level 5 within a reasonable time period, as agreed upon with the business based on the perceived or known risks of a system outage.
     2. Non-replicated environments should strive to increase exercising maturity and exercise at Maturity Level 4 within a reasonable time period, as agreed upon with the business based on the perceived or known risks of a system outage.
     3. All IT projects for new applications – or migrations of existing applications – that have been identified to require DR should scope disaster recovery infrastructure and exercising in the planning and deployment phases. DR exercising at the highest applicable maturity level should be performed before production go-live.
     4. The Alight global application DR exercise plan template or the globally approved template for DR plans on an alternate approved framework will be used as part of the planning process for all application DR exercises. DR exercise success criteria should be documented with the appropriate weights prior to conducting an application DR exercise. The success criteria define the baseline that determines whether an exercise can be considered successful or not. They also feed into the DR test report template. DR exercise reports are required to be published following successful, partially successful, and unsuccessful DR exercises.
     5. Failure to document success criteria prior to executing a test will result in the DR readiness for the application to be reported at a lower level.
  2. Alight’s Global DR Exercising Schedule
     1. Global, regional, and country annual exercising schedules will be compiled and published.

### Change Management

* 1. Where applicable, all Information Technology change management requests must clearly state the impact(s) of the stated changes on the current disaster recovery capabilities.
  2. Where applicable, all Information Technology change management activities must ensure that existing DRPs are updated to reflect the change.
  3. All changes must comply with the appropriate Information Technology change management policy.

### Training and Awareness

* 1. This standard shall be made available to all Alight colleagues.
  2. Alight Information Technology colleagues are briefed at least annually so they understand the plans they are part of and what will be involved in responding to a situation.
  3. Each DR plan must include a regular briefing of colleagues utilizing the appropriate exercising maturity level.

### Maintenance and Management Reporting

* 1. All DR plans will be developed and stored in Alight’s online Continuity & Analytics Management (“CAM”) Tool, [https://enterprise.sungardas.com](https://enterprise.sungard.com/), the Alight SharePoint Sites (one.Alight.net), or approved hosting vendor plan management system.
  2. Regular compliance reporting will be generated by the Global BTR Program office utilizing the online CAM Tool to create awareness and drive development, exercising and maintenance of business continuity plans according to this Standard.
  3. Compliance reporting will be based on the following factors:
     1. Date of last plan update, review, and approval
     2. Date of last DR exercise and maturity level of exercising
     3. Status of noted deficiencies and/or required remediation

### Business Partners

* 1. Third-party Information Technology outsource providers must demonstrate Disaster Recovery capability through appropriately documented and exercised strategies and plans, ensuring that plans are ‘fit for purpose’ and that they can recover/continue to deliver services at a level acceptable to Alight.
  2. Third party suppliers must have disaster recovery arrangements in place. These arrangements should ensure that they are able to continue to provide services and support to Alight in the event of a disruption that affects their business.
  3. Third-party Information Technology outsource partners must ensure their Disaster Recovery plans are compatible with Alight’s plans and strategies, and specifically detail an agreed upon notification and escalation process with Alight, roles and responsibilities, and clear procedures for crisis management.

## 

## Legal Conflicts

Alight’s Security Policies and Standards were drafted to address the protections found in existing laws and regulations and may be amended as necessary due to law, regulation, or business requirements. There is no intent to conflict with relevant local laws or regulations. In the event of any conflict with relevant local laws or regulations, they will control.

Alight’s Security Policies and Standards may be supplemented by other policies or standards of Alight. In the case of a conflict or ambiguity, the more specific provisions of any such policy or standard shall take precedence over the more general provisions contained in Alight’s Security Policies and Standards.

## Exceptions

Exceptional circumstances occur from time to time. In these situations, contact Alight Global Security Services at [global.security.services@Aon.com](mailto:global.security.services@aon.com) for further guidance.

## Comments

* None

## Related Documents

* None

## References and Mandates

* None

## Document Control Information

Document Control Information

|  |  |
| --- | --- |
|  |  |
| Primary Contact | Alight Global Security Services | [global.security.services@Aon.com](mailto:SRM.Mailbox@aon.com) |
| Version Number | 1.5 |
| Owner | Alight Global Security Services | Global Business & Technology Resilience |
| Author(s) | Alight Global Security Services | Global Business & Technology Resilience |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | May 2, 2011 |
| Information Classification | General Internal – Low Business Impact (Green) |

## 

## Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2012 March | Original | Restructured policy due to Aon Hewitt acquisition |
| 1.1 | 2013 June | 2013 Annual Review | Changed wording 6.2.1 and 7.2.4  Added 6.2.4 |
| 1.2 | 2014 July | 2014 Annual Review | Reviewed and validated |
| 1.3 | 2015 July | 2015 Annual Review | Updated wording in 3.1.2, 6.2.2, 6.2.4, and 10.1 |
| 1.4 | 2016 July | 2016 Annual Review | Replaced all instances of Global Business Continuity Management / Disaster Recovery (GBCM/DR) with Global Business & Technology Resilience to reflect the new team name. Also, replaced all instances of Security Risk Management (SRM) with Global Security Services (GSS) to reflect new organizational name. |
| 1.5 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |

## Appendix A: Global DR Approach: Criticality, RTO/RPO and Exercising Requirements

