Global Business Continuity Standard

May 1, 2017

Table of contents (“TOC Header”)

[Purpose 3](#_Toc488415951)

[Standard Statements 3](#_Toc488415952)

[1. Business Risk Assessment 3](#_Toc488415953)

[Tier 1 4](#_Toc488415954)

[Tier 2 4](#_Toc488415955)

[Tier 3 5](#_Toc488415956)

[Tier 4 5](#_Toc488415957)

[2. Impact Assessment 5](#_Toc488415958)

[3. Business Continuity Plan Development and Oversight 10](#_Toc488415959)

[4. Business Continuity Plan Exercising 13](#_Toc488415960)

[5. Training & Awareness 14](#_Toc488415961)

[6. Maintenance and Management Reporting 14](#_Toc488415962)

[Legal Conflicts 15](#_Toc488415963)

[Exceptions 15](#_Toc488415964)

[Comments 15](#_Toc488415965)

[Related Documents 15](#_Toc488415966)

[References and Mandates 15](#_Toc488415967)

[Revision History 17](#_Toc488415968)

Related Policy

* 400.00 Global Business Continuity Management Policy

## Purpose

Alight Solutions has developed a framework for developing global business continuity plans supported through established governance and a business continuity management standard. This standard supports efficient business operations, preservation of corporate memory and compliance with relevant legal and regulatory requirements.

The Alight Global Business Continuity Management Standard (“Standard”) defines Alight’s standard for developing and maintaining its global program that ensures Alight is adequately prepared to anticipate and respond to significant business disruptions in a manner that protects the welfare of Alight colleagues, business operations, reputation, image in the interests of its shareholders and clients.

## Standard Statements

### Business Risk Assessment

All Alight sites will be given a risk ranking determined by the Alight Global Business Continuity Management Program Office (“GBCM”). Risk rankings will be based on the following collective criteria and will determine the level of business continuity planning required.

* 1. The population size of Alight colleagues or contractors at a site.
  2. Whether the site hosts a key Alight data center.
  3. Whether the site / process / technology is a single point of failure for a business operation or technology stream.
  4. Whether a site failure could have a material impact on Alight.
  5. Tier details are as follows:

#### Tier 1

Sites in this category are required to complete the following planning templates:

* Site Emergency Response Plan
* Site Situation Response Plan
* Business Continuity Plan(s) for each business unit or unique business operation
* Disaster Recovery Plan (if infrastructure is present)

Sites in this category meet at least one of the following criteria or have a risk score of >/=36.

* Physical risk criteria
* Headcount risk is RED (>250) or AMBER (>100)
* Human events risk is RED as forecast. Human events include political unrest, security concerns and/or terrorism.
* Natural events risk is RED as forecast. Natural events include geographical and meteorological risks.
* Business risk criteria
* House a data center or critical infrastructure or business applications
* Is a critical single point of failure for a business operation or succession plan
* Contributes more than 1% to total global liabilities and equities.

#### Tier 2

Sites in this category are required to complete the following planning templates:

* Site Emergency Response Plan
* Small Office - Business Continuity and Situation Response
* Disaster Recovery Plan (if infrastructure is present)

Sites in this category meet at least two of the following criteria or have a combined risk score between 20 and 35. At a minimum, any site with >100 colleagues is considered a Tier 2 location.

* Physical risk criteria
* Headcount risk is AMBER (>100)
* Human events risk is AMBER or RED as forecast. Human events include political unrest, security concerns and/or terrorism.
* Natural events risk is AMBER or RED as forecast. Natural events include geographical and meteorological risks.
* Business risk criteria
* Site contains essential (non-critical) business applications or infrastructure
* Contributes more than .01% to total global liabilities and equities

#### Tier 3

Sites in this category are required to complete the following planning templates:

* Situation Response Plan
* Business Continuity Plan(s) for each business unit or unique business operation

Sites in this category meet at least one physical risk and one business risk from the following criteria or have a combined risk score between 10 and 20.

* Physical risk criteria
* Headcount risk is GREEN (>25)
* Human events risk is AMBER or RED as forecast. Human events include political unrest, security concerns and/or terrorism.
* Natural events risk is AMBER or RED as forecast. Natural events include geographical and meteorological risks.
* Business risk criteria
* Site contains essential (non-critical) business applications or infrastructure
* Site contributes more than .0009% to total global liabilities and equities

#### Tier 4

Sites in this category are required to complete the following planning templates:

* Micro-Plan (combined form)

**Tier 4** sites do not meet any of the above criteria and/or have a combined risk score of <10.

### Impact Assessment

* 1. All Alight business units must identify business processes and dependency information that are determined to have the greatest potential impact to the company in the event of a significant business disruption.
  2. All Alight business units are required to identify the following informational components as it relates to critical business processes. They include but are not limited to:
     1. Process Name: name of the critical process.
     2. Process Description: a brief description of the process.
     3. Process Owner: the business executive responsible for, or who owns, the process.
     4. Client Facing: identify if process is client facing.
     5. Frequency Performed: identify the frequency process is performed.
     6. Critical Working Period(s): time (month, week, day, or time of day) in which the process is most critical to the business and/or Company.
     7. Data Sensitivity: classifies the sensitivity of the data related to the process. There are four Alight Standard classifications, as defined in GSS Information Security’s 100.01 Information Classification Standard:
        1. Highly Confidential / High Business Impact (HBI)
        2. Confidential / Moderate Business Impact (MBI)
        3. Internal / Low Business Impact (LBI)
        4. Public / No Business Impact (NBI)
     8. Enterprise Criticality: aims to determine the criticality of a Process based on the following classifications and supporting criteria.
        1. High
* Process or function that must be maintained throughout staffing shortages or facility outages.
* When not delivered, creates an impact on the health and safety of employees, may lead to the failure of a business unit if activities are not performed in a specified period of time, or must be performed to satisfy regulatory requirements.
  + - 1. Medium
* Process or function that can be discontinued for a short period of time; greater than or equal to 5 days but less than or equal to 30 days.
  + - 1. Low
* Process or function that can be discontinued for extended periods of time without creating tremendous hardship to the business; greater than 30 days.
  + 1. Recovery Time Objective (“RTO”): the maximum time notated in hours within which the business requires the process to be available.
    2. Recovery Point Objective (RPO): the maximum time notated in hours within which the business could sustain a loss of data for the required process.
    3. Financial Impact: aims to identify the financial impact should this process not be available within the defined RTO.
       1. Low - Less than US $100,000
       2. Medium - Less than US $1,000,000
       3. High - More than US $1,000,000
    4. Reputational Impact: aims to identify the reputational impact should this process not be available within the defined RTO.
       1. Low - No adverse media coverage and no negative impact on brand. Client confidence can be maintained.
       2. Medium - Limited media coverage and limited negative impact on brand. Client confidence can be maintained.
       3. High - Adverse media coverage with negative impact on brand. Client confidence cannot be maintained.
    5. Regulatory Impact: aims to identify the regulatory impact should this process not be available within the defined RTO.
       1. Low - Not required to notify regulators and/or financial exchanges.
       2. Medium - Required to notify regulators and/or financial exchanges.
       3. High - Required to notify regulators and/or financial exchanges and there has been a breach in compliance or law.
    6. Legal Impact: aims to identify the legal impact should this process not be available within the defined RTO.
       1. Low - No breach of any law or contract
       2. Medium - Limited breach of a law or contract than can be managed and has less than US $100,000 in penalties, and would not result in contract termination.
       3. High - Breach of a law or contract than cannot be managed, has more than US $100,000 in penalties and would result in contract termination.
    7. Client Impact: aims to identify the client impact should this process not be available within the defined RTO.
       1. Low - No impact to Alight clients.
       2. Medium - Impact is limited to a single client with no material damage to their reputation, operations or regulatory compliance.
       3. High - Impacts multiple clients and/or there is material damage to their reputation, operations or regulatory compliance.
    8. Primary Workspace Impact: Identify impact to the process in the event there is a loss of the primary workspace for up to 30 days.
       1. Low - Process can be maintained at full capacity. Documented and tested workarounds and/or redundancies exist for this process.
       2. Medium - Process can be maintained at a degraded level. Workaround and/or redundancies exist for this process but they are not documented or tested.
       3. High - Process activity cannot be maintained. Workarounds and/or redundancies do not exist for this process.
    9. Information Technology Impact: Identify impact to the process in the event there is a loss of technology for up to 30 days.
       1. Low - Process can be maintained at full capacity. Documented and tested workarounds and/or redundancies exist for this process.
       2. Medium - Process can be maintained at a degraded level. Workaround and/or redundancies exist for this process but they are not documented or tested.
       3. High - Process activity cannot be maintained. Workarounds and/or redundancies do not exist for this process.
    10. Staff Impact: Identify impact to the process in the event there is a loss of staff (</= to 50%) for up to 30 days.
        1. Low - Process can be maintained at full capacity. Documented and tested workarounds and/or redundancies exist for this process.
        2. Medium - Process can be maintained at a degraded level. Workaround and/or redundancies exist for this process but they are not documented or tested.
        3. High - Process activity cannot be maintained. Workarounds and/or redundancies do not exist for this process.
    11. Additional Impact Notes: aims to provide specific details on notable impacts as necessary
    12. Process Workarounds: describe available workarounds for this process.
    13. In-flow Dependencies: identify internal and external entities that this process is dependent upon to be performed. (In-flow dependencies)
    14. Out-flow Dependencies: identify internal and external entities that are dependent upon the output from this process. (Out-flow dependencies)
    15. Locations Performing Function: identify locations that perform this critical function.
    16. Performed By: aims to identify the role(s) performing this critical process.
    17. Additional details: may include any additional information notes or details about the process that would be helpful in the recovery or analysis of the process.
  1. Each Alight business unit with input from their IT support partners is responsible for identifying dependencies (systems, people, sites, and vendors), manual workarounds, recovery requirements and locations, vital records, and special circumstances for their particular business processes.
  2. All business process information must be approved in writing, minimally, by the Business executive who owns the process. Once the Business Unit processes are identified and ranked and approval has been obtained, the results must be provided to GBCM using the appropriate template (Process Import Template).
  3. All the Business Impact Assessment (“BIA”) process information will be completed using the Process Import Template for upload into the Continuity & Analytics Management (“CAM”) Tool or by using the globally approved template for business units on an alternate approved framework.

### Business Continuity Plan Development and Oversight

* 1. All businesses within Alight are responsible for developing, maintaining, and exercising business continuity plans.
  2. Each business unit is responsible for identifying key individuals and succession plans to ensure the following business continuity 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 BC Program sponsor, is the ultimate decision maker over budget, and is accountable for all business continuity 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 business functions, identifying plan owners, and approving recovery strategies. They will also be a decision maker in the execution of business continuity plans.
     3. Executive Plan Owner: must be of management level and is responsible for the development and management of business continuity plan(s). They are required to participate in regular exercises, plan sign-off, and be responsible for executing recovery strategies in the event of a significant business disruption.
     4. Plan Coordinator: is responsible for coordinating the development and management of business continuity plan(s). They are required to participate in regular exercises and publishing plan documentation as changes are approved. The plan coordinator may also be called upon to assist in the execution of recovery strategies in the event of a significant business disruption.
  3. Business continuity plans must be developed utilizing the Global Business Continuity Management Program Office’s Continuity & Analytics Management (“CAM”) tool and/or template located at <https://enterprise.sungardas.com> or by using the globally approved template for business units on an alternate approved framework. At a minimum, plans must identify and document the following components:
     1. Business process details (see section 2 Business Impact Analysis for specific details)
     2. Identification of critical applications used to support critical business processes
     3. Logistics that document the following organizational components of a plan
        1. Employees: identify employees that are part of the business unit/team for which the plan is being created. Additionally for each employee, identifying supporting attributes, Primary Recovery Strategy, Secondary Recovery Strategy and RTO (day employee is required).
        2. Work Area Recovery Strategies: document solutions designed to accommodate the resumption of a business’s critical processes in the event of a significant business disruption. Alight utilizes five standard Work Area Recovery Strategies for Business Continuity Planning.
* Relocate to an Alternate Alight Location
* Virtual (i.e. virtual or other work from home type)
* Shift Work to Unaffected Alight Location
* Relocate to a Contracted Work Area Recovery Center
* Stop Work

Selection of strategies and relocation facilities should be coordinated through the Global GBCM Program Office and/or assigned Regional GBCM Lead.

* + - 1. Work Area Recovery Locations: document specific location(s) and the number of seats required over time that will be used to support the Work Area Recovery Strategies identified within the business continuity plan.
      2. Teams: are used to help provide organization and structure to recovery activities or tasks within the Business Continuity Plan. Teams are comprised of a team leader, team member positions, and alternates. People assigned to the team positions should be qualified individuals who can execute or manage the tasks assigned to the team.
      3. Recovery Actions / Tasks: are actions performed with the purpose of fulfilling an objective and are typically related to recovery of the business unit. A task can also be divided into a group of more detailed, procedural, or explanatory subtasks. Pre-Planning tasks are actions that usually occur prior to an event and assist in the creation or building of a plan. There are four types of tasks that may be identified:
* Response
* Resumption
* Recovery
* Restoration

A standardized checklist is included within the approved GBCM framework and prints as part of the plan. Business units may add additional recovery actions by uploading BU specific actions in the Documents section of the online planning tool.

* + 1. Resources: documents the tangible resources needed to recover and support the business. Resources are comprised of the following components and identify quantities of items needed within specified timeframes.
       1. Documents: supplemental reference information for the business unit or leaders if and when this plan is activated.
       2. Equipment: items used as part of business operations, such as postage meters, desktop printers, laptops, PCs, notary stamps, etc.
       3. Software: identify software “shrink-wrap” that is not part of the larger Corporate IT Application Portfolio.
       4. Supplies: identify and document materials that are needed in order to perform the tasks and procedures outlined within the business continuity plan.
       5. Telecom: identify and document critical telephone or fax numbers that need to be redirected in the event the primary work location becomes unavailable.
       6. Vital Records: identify and document critical hard copy and/or electronic data that will need to be recovered or retrieved in order to support the business recovery process.
    2. Call lists with up-to-date contact information.
    3. Required approval signatures.
  1. An approved copy of the plan needs to be available to or submitted to the appropriate Regional BC Manager. If required, signatures of approved parties should be on file with the documentation. This copy will be retained on file with the GBCM Program Office and within the Plan Management Details of the Continuity Analytics Management tool. It will also be used to provide management with compliance statistics.

### Business Continuity Plan Exercising

* + 1. Each business unit must exercise their business continuity plan and execute contact information validation exercises annually to ensure that business continuity plans are up-to-date, effective, and address the needs of the Business. Annual exercises must be at the appropriate level of maturity as approved by your global/regional BC leader in advance. Exercises will align to the GBCM Maturity Model exercise levels.
    2. Level 0 - Exercises and tests have not been conducted.
    3. Level 1 - Exercises and tests are conceptual in nature with no formal documentation. Call tree/cascade testing is conducted. (Example: checklist exercise or gap assessment, or peer review)
    4. Level 2 - Exercises and tests use document-based discussions. (Example: structured walk-thru, tabletop (paper) exercise or desktop (paper) scenario)
    5. Level 3 - Exercises and tests are focused on individual plan effectiveness under simulated operating conditions. (Example: standalone test)
    6. Level 4 - Exercises and tests focused on recovery actions of inter-related business operations (plans) under simulated disaster conditions. (Example: simulation, mock disaster, or operational testing)
    7. Level 5 - Exercises and tests simulating recovery actions under simulated/modified operating conditions. Business operates in recovery mode to support production operations, including return to normal operations. (Example: integrated testing or exercising and full rehearsal)
  1. Each business unit must document and submit exercise results utilizing Alight's Business Continuity Management exercise framework. Forms are supplied by the Regional Business Continuity Management Leader and/or Global Program Office.
  2. Each business unit must remediate and update its business continuity plan(s) in accordance with any deficiencies or issues discovered during the annual exercise or after plan execution. Risk acceptance will be handled by the GBCM Program Office as is deemed necessary.

### Training & Awareness

* 1. Plan owners are responsible for ensuring Alight colleagues within their business unit’s business continuity plan(s) are briefed at a minimum annually or when significant changes occur, so they understand the plans they are part of, and what will be involved in responding to a situation. New Alight employees should be given an overview of the department’s Business Continuity Plan and their role in the event of incident as soon as reasonably practical.
  2. Alight colleagues with a virtual (i.e., work from home or alternate location) recovery strategy have a duty to take appropriate equipment (i.e., laptops, mobile devices, chargers, files, etc.) home on a daily basis to enable them to continue business operations in the event of a disruption. Alight colleagues should periodically exercise remote working capabilities.
  3. For further information and guidance on Business Continuity plan development, exercising (including specific region or country requirements), and use of the Continuity & Analytics Management (“CAM”) Tool, refer to your Regional GBCM Manager.
  4. Questions regarding this Standard should be directed to the Alight GBCM Program Office.

### Maintenance and Management Reporting

* 1. Business Continuity plans for all sites and/or critical business processes must be reviewed and maintained on an annual basis or as significant changes occur that may affect or influence the plan.
  2. All Business Continuity plans must be developed, maintained, and stored in Alight’s online Continuity & Analytics Management (“CAM”) Tool, https://enterprise.sungardas.com or in a globally approved alternate format.
  3. Regional Business Continuity Management leaders should be notified of any material changes that occur to business continuity operations, strategies or plans. This includes, but is not limited to creating or removing plans, processes or operating locations.
  4. Regular compliance reporting will be generated by the GBCM Program office utilizing the online CAM Tool to create awareness and drive development, exercising and maintenance of business continuity plans according to this Standard.

## 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 Global Security Services at [global.security.services@aon.com](mailto:global.security.services@aon.com) for further guidance.

## Comments

* None

## Related Documents

* Global Business Continuity Management Policy
* Data Security Classification Standard

## References and Mandates

SEC 17 CFR 240 (2005) – SEC regulations require that financial transaction histories be maintained for all electronic securities transactions, and backup power be in place to maintain continuity. This regulatory requirement is mandatory for applicable entities.

GLBA: Gramm-Leach-Bliley Act (1999) – Applies to all US financial institutions, which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers.

NYSE Rule 446 / NASD 3510/3520 (2004) – Applies to all members and member organizations of the NYSE or NASD.Document Control Information

|  |  |
| --- | --- |
| Document Control Information | |
| Document Name | 400.01 Global Business Continuity Management Standard |
| Primary Contact | Global Security Services global.security.services@aon.com |
| Version Number | 1.5 |
| Owner | Alight Global Security Services | Global Business Continuity Management Program Office |
| Author(s) | Mary De Angelo, VP – Global Emergency Operations Center & Global Business Continuity Management  Vickie Reuther, Sr. Manager - Global Business Continuity Management |
| 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 | Internal / Low Business Impact (LBI) |

## 

## 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 | Added Section 1.5 Tiers and made wording changes to 2.2.9, 2.4, 2.5, 3.3, 3.4, 4, 5, 6.2, 6.3 and 6.4 |
| 1.2 | 2014 July | 2014 Annual Review | Standard has been reviewed |
| 1.3 | 2015 July | 2015 Annual Review | Updated wording 1, 1.5, 2.2.4 – 2.2.8, 2.2.9, 2.4, 3.3.3.5, 4.1  Updated and added sub-sections to 2.2 and 4.1 to reflect additional program enhancements in GBCM Framework |
| 1.4 | 2016 July | 2016 Annual Review | Replaced all instances of Global Business Continuity / Disaster Recovery (GGBCM/DR) and replaced with Global Business Continuity Management to reflect the team’s new name. Also replaced all instances of Security Risk Management (SRM) with Global Security Services (GSS) to reflect new organization name. |
| 1.5 | 2017 May | 2017 Annual Review | Rebranded Standard due to Aon Hewitt divestiture  Wording changes from Global Business & Technology Resilience to Global Business Continuity Management  Standard name changed from Business Continuity Standard to Global Business Continuity Management Standard  Acronym changed from BTR to GBCM  5.3 Deleted the words, “visit the GBCM SharePoint site, or”. Alight does not have a SharePoint site for GBCM. |