



Disaster Recovery Plan

Proprietary and Confidential

This document contains the overarching disaster recovery strategy for SAP SuccessFactors. This plan is applicable for all production data centers with restoration at secondary sites. SAP SuccessFactors policy requires this plan be reviewed at least annually.

Global Cloud DR Solution – All Data Centers

October 13, 2017

Version 6.0

TABLE OF CONTENTS

1	OVERVIEW	5
1.1	PLAN COMPONENTS	5
1.2	BENEFITS OF DEVELOPING A DISASTER RECOVERY PLAN	6
1.3	CURRENT STANDARDS.....	6
1.4	PROGRAM OWNERSHIP.....	7
1.5	DOCUMENT AVAILABILITY.....	7
2	ANALYSIS PHASE	8
2.1	BUSINESS IMPACT ANALYSIS (BIA)	8
2.2	THREAT AND RISK ANALYSIS (TRA)	9
2.2.1	<i>Threats to the Business</i>	9
2.2.2	<i>Business Impact Scenarios</i>	10
2.2.3	<i>Disaster Recovery Scenarios</i>	10
2.2.4	<i>Key Risks on Production Capabilities</i>	10
2.3	ON-PREMISE RISK MITIGATION	11
2.3.1	<i>Back-up Power Arrangements</i>	11
2.3.2	<i>Data Back-ups and Restorations</i>	11
2.3.3	<i>Premises and Essential Equipment</i>	12
2.3.4	<i>Data Center Host Obligations for Resiliency</i>	12
2.4	RECOVERY REQUIREMENTS	12
2.4.1	<i>Data Centers</i>	13
2.4.2	<i>Environment Redundancy</i>	15
2.4.3	<i>Network Redundancy</i>	15
2.4.4	<i>Infrastructure Services Redundancy</i>	16
2.4.5	<i>Data Replication Basics</i>	16
2.4.6	<i>Distribution of Responsibilities</i>	16
3	SOLUTION DESIGN PHASE	17
3.1	SOLUTION LANDSCAPE	17
3.2	ACTIVE / PASSIVE DATA CENTER MODEL	18
3.3	HIGH-LEVEL ENVIRONMENT DIAGRAM	18
4	IMPLEMENTATION PHASE.....	19
4.1	HCM COMPONENT ARCHITECTURES	19
4.1.1	<i>Application Architecture</i>	19
4.1.2	<i>Integration Middleware Architecture</i>	19
4.1.3	<i>Logical Network Architecture</i>	19
4.1.4	<i>Infrastructure Services</i>	20
4.2	DEPLOYMENT AND CONFIGURATION OF DR ENVIRONMENTS.....	20
4.3	DATA REPLICATION	21
4.4	FAILOVER ACTIONS TIMELINE	21
5	TESTING AND ORGANIZATIONAL ACCEPTANCE PHASE.....	23
5.1	IDENTIFY TYPE OF DR TEST	23
5.1.1	<i>Tabletop Exercises</i>	23
5.1.2	<i>Medium Exercises</i>	23
5.1.3	<i>Complex Exercises</i>	24
5.2	DEVELOP SCOPE AND PLAN TESTS	24

5.3	IDENTIFY TEST PARTICIPANTS	25
5.4	CONDUCT THE TEST.....	25
5.4.1	<i>Backup and Restoration Testing</i>	25
5.4.2	<i>Crisis Command Team Call-out Testing</i>	25
5.4.3	<i>Failover Testing</i>	25
5.4.4	<i>Application Functionality Verification</i>	26
5.4.5	<i>Business Process Test Cases</i>	26
5.5	PERFORM POST-TEST ACTIVITIES.....	28
5.5.1	<i>Assess Test Results</i>	28
5.5.2	<i>Capture Feedback</i>	28
5.5.3	<i>Generate Test Report for Signoff</i>	28
5.5.4	<i>Prepare for Retesting</i>	28
6	MAINTENANCE PHASE	29
6.1	DR PLAN INFORMATION AND TARGETS	29
6.2	TECHNICAL REQUIREMENTS ON STANDBY	29
6.3	TESTING AND VERIFICATION OF RECOVERY PROCEDURES	29
6.4	SHARING THE PLAN	30
6.5	CHANGE CONTROLS FOR UPDATING THE PLAN.....	30
6.6	RESPONSIBILITIES FOR MAINTENANCE OF THE PLAN	30
7	DISASTER DECLARATION AND INVOCATION PROCESS.....	31
7.1	EMERGENCY AUTHORIZATION AND DECLARATION STAGE.....	32
7.1.1	<i>Handling the Emergency</i>	32
7.1.2	<i>Assessing the Situation</i>	32
7.1.3	<i>Determining Potential Impact of the Emergency</i>	33
7.1.4	<i>Declaring a Disaster</i>	34
7.2	DISASTER MANAGEMENT STAGE.....	34
7.2.1	<i>Establishing a Response and Recovery Center</i>	34
7.2.2	<i>Mobilizing the Disaster Recovery Team</i>	35
7.2.3	<i>Maintaining the Event Log</i>	36
7.2.4	<i>Recording Project Management Activities</i>	36
7.3	COMMUNICATION PLAN ACTIVATION STAGE	37
7.3.1	<i>Kicking Off Management Meetings</i>	37
7.3.2	<i>Opening a Phone Bridge</i>	37
7.3.3	<i>Reviewing and Documenting Status</i>	38
7.3.4	<i>Communicating with the Press</i>	38
7.3.5	<i>Communicating with Customers</i>	39
7.4	FAILOVER PLAN EXECUTION STAGE.....	40
7.4.1	<i>Implementing the Failover Steps</i>	40
7.4.2	<i>Performing Functionality Health Checks</i>	40
7.5	SYSTEM ACCESS AND SERVICE AVAILABILITY	41
7.5.1	<i>Granting System Access by Priority Group</i>	41
7.5.2	<i>Validating Service Availability</i>	41
7.5.3	<i>Expanding Compute Capacity</i>	41
7.5.4	<i>Declaring "Disaster Over"</i>	41
7.5.5	<i>Producing a DR Process Report</i>	42
7.6	RECONSTITUTION STAGE	42
7.6.1	<i>Reconstructing the Original Primary Site</i>	42
7.6.2	<i>Initiating the Failback Steps</i>	43

APPENDIX44

APPENDIX 1 – ABBREVIATIONS AND ACRONYMS 45

APPENDIX 2 – DEFINITIONS AND TERMINOLOGY FOR THIS DOCUMENT 46

APPENDIX 3 – SAP SUCCESSFACTORS CONTACT LIST 48

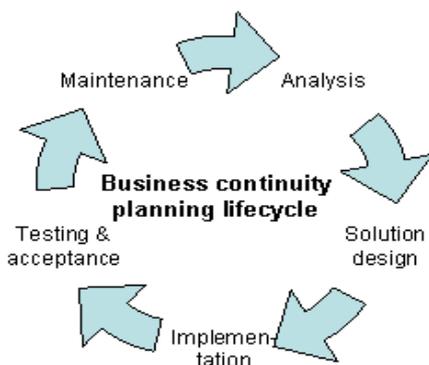
APPENDIX 4 – KEY LEASORS, DATA CENTER OPERATORS AND EMERGENCY CONTACTS 49

Disaster Recovery Plan

1 OVERVIEW

1.1 Plan Components

SAP SuccessFactors (SAP SFSF) provides a disaster recovery (DR) site and associated plan for its customers. This document describes the Cloud DR solution and fulfills the regulatory plan requirement.



A variety of catastrophic events could disable an entire SAP SFSF data center for an extended time. The disaster recovery site and plan protects all customers – in the event a SAP data center hosting production systems was severely damaged or destroyed. In this circumstance, SAP SuccessFactors is still doing business as the primary “Software as a Service” (SaaS) provider, and SAP SFSF works to minimize any negative impact to customers with an efficient restoration.

The purpose of this plan is to: (1) counteract interruptions to Cloud Operations activities, (2) protect critical business processes from the effects of major failures or disasters of information systems, and (3) ensure their timely resumption.

SAP SFSF has developed procedures to support the continuity of its operations. Plans have been developed to recover mission-critical business processes at each data center. Technical recovery procedures (TRP) are implemented to restore operations. These documents ensure availability of information at the required level and in the required timescales following interruption to, or failure of, critical business processes.

Consistent with best practices, this disaster recovery plan (DRP) is comprised of five reiterative sections – highlighting the phases in the planning lifecycle.

1. The **analysis phase** consists of business impact analysis (BIA), threat and risk analysis (TRA), identification of scenarios and critical recovery requirements.
2. The **solution design phase** identifies the most cost-effective recovery solution that meets two main business objectives from the impact analysis stage. For IT purposes, this is commonly expressed as (a) the minimum application and data requirements and (b) the time in which these must be available. This section outlines the required infrastructure, applications, software, data management and business processes.
3. The **implementation phase** primarily captures the technical requirements which dictate the “Software as a Service” solution provided by SAP SuccessFactors. This section clearly describes the HCM component architectures with diagrams of both production and disaster recovery environments. The second part of the phase focuses on deployment and configuration of the DR environment, as well as the failover steps. This phase overlaps with recovery planning methodology.
4. The purpose of the **testing and organizational acceptance phase** is to get stakeholder buy-in. Exercising the plan ensures that the solution satisfies recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws or solution implementation errors. Issues found during the testing phase often highlight the need for maintenance and/or must be reintroduced to the analysis phase.
5. The **maintenance phase** dictates that the disaster recovery plan and related documents are refreshed at least annually with current information (e.g., contact data, runbook changes, script updates, job schedule adjustments, etc.)

Finally, the **DR declaration and invocation process** is described in the last section. The procedures illustrate, at a high level, how a DR event is handled within the initial hours and early days following an event. And, appendices provide additional details relevant to this program.

1.2 Benefits of Developing a Disaster Recovery Plan

- SAP SuccessFactors has implemented a business environment designed to deliver quality services to its customers. Services are provided through (a) the adoption of standardized, repeatable processes, (b) the hiring and development of highly skilled staff, and (c) an extensive customer management infrastructure.
- SAP SuccessFactors leverages a combination of proven techniques such as ITIL process management and leading industry practices. This approach also includes documented policies and procedures for managing service-related processes, including Change Management, Security Management, Availability Management, Service Level Management and Incident Management. These standard processes serve as a baseline to develop customer-specific procedures for day-to-day activities.
- SAP SuccessFactors implements disaster recovery processes to minimize the impact on SAP SuccessFactors of an incident – such as those that may be caused by natural disasters, accidents, equipment failures or deliberate actions – through a combination of preventative and recovery controls.
- SAP SuccessFactors considers contingency planning to be an iterative process; ongoing review is required in order to assess a variety of risks and appropriate responses.
- To ensure reliability of the production environment, when introducing changes, SAP SuccessFactors demands all new system requirements be documented and tested prior to acceptance and use.

Successful businesses expect the unexpected and plan for it. Disruptions to your business can result in data risk, revenue loss, failure to deliver services as normal or in extreme cases, failure to deliver at all. That's why organizations need strong business continuity planning.
– John Sharp, BSI

1.3 Current Standards

This plan is written in accordance with the Information Security Management System (ISMS, based on ISO 27k) policies on Business Continuity and Disaster Recovery. Key documents, policies and procedures will be archived. Disaster Recovery team members also keep local and hardcopy versions of relevant documents.

For more details about SAP corporate policy and standards, refer to:

- Data Protection Management System
<https://wiki.wdf.sap.corp/wiki/pages/viewpage.action?pagelId=1711447344>
- SAP Security Policy
https://portal.wdf.sap.corp/wcm/ROLES://portal_content/cp/roles/employee/employee_services/Security/Infocenters/Cross%20Services%20for%20SAP/Security/-/Security%20Policy%20%26%20Standards

Cloud Operations guides are maintained on JAM (access restricted):

- https://jam4.sapjam.com/groups/WKCzYrXlEfNWUMqLmwDBL2/documents/FozlF75ll8dAqwuDtGHKD/slide_viewer

Disaster Recovery test plans and results are maintained in JAM (access restricted):

- https://jam4.sapjam.com/groups/gA51X6d7ynpnIoWJupMzM9/content?folder_id=y9vE0o0WHMNROjAwwhq6i

1.4 Program Ownership

Overall accountability for the Disaster Recovery program lies with our Chief Information Officer (CIO).

The primary owner of the program, implementation plan, and execution is the VP of Cloud Operations.

The DR Program Manager must approve all changes to the content of this and all other related DR materials (e.g., test workbooks, plan documents, templates, SOC controls, etc.). See the revision log on the last page of this document for change authorship and approval.

Employees from various parts of SAP SuccessFactors have roles and responsibilities within the DR program framework and provide input to this document.

Key project team members are listed in the Appendix.

1.5 Document Availability

This document will be stored in SAP JAM along with other SAP SuccessFactors DR plans from the various offices. In addition, hard copies of this document will be distributed to or made available to team members. Team members are also encouraged to keep local copies of this plan in electronic form.

The SAP JAM page access is restricted, but located at:

https://jam4.sapjam.com/groups/gA51X6d7ynpnloWJupMzM9/content?folder_id=pFbdSK8JeGtTvEbGzlGOyQ

The CIO, VP Security, or Director of Audit and IT Risk may authorize the DR Program Manager to share a copy of this document with external parties. This document may be shared with external parties under these conditions:

1. The external party is an existing customer or a prospect under Non-Disclosure Agreement (NDA) and a fully executed copy of the NDA has been provided to the Documentation Manager.
2. The CIO, VP of Security or Director of Audit and IT Risk has approved distribution to the external party.
3. All sensitive information has been redacted from the copy to be distributed.
4. The copy to be distributed is in PDF format with standard document protection features enabled.

2 ANALYSIS PHASE

The analysis phase consists of business impact analysis (BIA), threat and risk analysis (TRA), identification of scenarios and critical recovery requirements.

2.1 Business Impact Analysis (BIA)

A Business impact analysis (BIA) differentiates critical / urgent and non-critical / non-urgent organization activities. Critical functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions. A function may also be considered critical if dictated by law. For each critical, in-scope function, two values are then assigned:

- Recovery Point Objective (RPO) – the acceptable latency of data that will not be recovered. For example, is it acceptable for the company to lose 24 hours of data? The recovery point objective must ensure that the maximum tolerable data loss for each activity is not exceeded.
- Recovery Time Objective (RTO) – the acceptable amount of time to restore the function. For example, can the customer track compensation changes with paper records for one day and enter “en masse” manually when system access is returned?

Based on conversations with our customer base, keeping accurate compensation records is a critical function. Similarly, maintaining a current database of employee certifications and completed courseware are crucial to the business.

The following SAP SFSF application products maintain continuity of these business processes per the DR option selected by each customer. Other important, but non-critical, business functions are a secondary consideration and restoration is done only as resources become available.

SAP SuccessFactors Application Product	Category	DR Recovery Point Objective (RPO)	DR Recovery Time Objective (RTO)
Business Execution Suite (BizX) Performance & Goals Succession & Development Compensation Employee Central (EC)	Critical	Specific value varies by contract	Specific value varies by contract
Learning Management System (LMS) Validated Learning	Critical	Specific value varies by contract	Specific value varies by contract
EC Integration with SAP Payroll (i.e., on premise or Cloud product) using BOOMI or P2P	Non-Critical	Commercially reasonable effort only	Commercially reasonable effort only
Other application products (e.g., WFA, JAM, ONB, RMK, Mobile, etc.)	Non-Critical	Commercially reasonable effort only	Commercially reasonable effort only
Other internal (SAP) relationships (e.g., ERP, FieldGlass, Ariba, Concur, etc.)	Non-Critical	Commercially reasonable effort only	Commercially reasonable effort only
Other external integrations (e.g., third-party service providers / vendors)	Non-Critical	Commercially reasonable effort only	Commercially reasonable effort only

2.2 Threat and Risk Analysis (TRA)

After defining recovery objectives, each potential threat may require unique technical recovery procedures. These have been categorized as (1) a natural or (2) man-made disaster. This plan only covers the disaster recovery options for an unexpected event which causes a total loss of a data center. In this type of scenario, it is likely that the entire data center cannot be accessed and/or recovered.

2.2.1 Threats to the Business

Disaster Recovery Option	Legacy Premium and Current Enhanced DR Options	Backups and Other Included Standard DR Services
Event Scenarios	Entire production data center is incapacitated and offline due to natural or man-made catastrophic event including but not limited to: cyber-attack, earthquake, epidemic, fire, flood, hurricane, plane crash, sabotage, terrorism, theft, utility outage, war / civil disorder, or lengthy failure of mission-critical systems	Entire production data center is incapacitated and offline due to natural or man-made catastrophic event including but not limited to: cyber-attack, earthquake, epidemic, fire, flood, hurricane, plane crash, sabotage, terrorism, theft, utility outage, war / civil disorder, or lengthy failure of mission-critical systems
Offsite Backups	Weekly full / Nightly incremental / Archive logs multiple times daily to separate storage array	Weekly full / Nightly incremental / Archive logs multiple times daily to separate storage array
State of SAP SuccessFactors	Continues to do business as a SaaS organization	Continues to do business as a SaaS organization
Short Service Description	Near real-time, asynchronous data replication and failover to a fully-functional warm Disaster Recovery site with in-place network, security, available storage and a complement of basic replacement servers.	Restore replicated backups from disk at a remote location with in-place network and security. SAP may temporarily re-allocate resources from other environments and backfill. SAP maintains an open purchase order for storage and replacement servers during emergencies.
RPO: Target age of data	Could be as little as one hour, but no more than 24 hours of data loss	None specified; likely 24 hours, but last full backup could be as much as 7 days old
RTO: Data access and full application functionality	Tiered from a minimum of four hours to maximum of 72 hours to restore administrator access / service	Commercially reasonable efforts to restore service as soon as possible
RTO: Full pre-event compute capacity	Tiered from a minimum of four hours to maximum of 30 days to restore 100% service capacity	Commercially reasonable efforts to restore 100% capacity as soon as possible
Written Plan Document	Customer-specific, written DR Plan available upon request	No customer-specific written DR plan; only Global DR solution available upon request
Annual Disaster Recovery Test	Annual Cloud DR test with option for customer participation when in-region (selection at Cloud service provider's sole discretion)	Only SOC report evidence of annual DR test
Effective Dates and Restrictions	Applies to production environments for applications supporting only critical business functions effective at the time a DR event occurs or the disaster recovery plan is invoked, whichever later	Applies to production environments for applications supporting both critical and non-critical business functions per customer contract

SAP retains the right to change (at any time in its sole discretion but subject to the terms of the Agreement) the Cloud Service, this specification sheet, and/or the location of the data center(s) from which a Cloud Service is hosted.

2.2.2 Business Impact Scenarios

After identifying the applicable threats, impact scenarios are considered to support the development of a disaster recovery plan. DR test plans may provide greater detail for each identified threat and related impact scenarios.

The DR plan examines the requirements necessary for recovering the business from the widest possible damage (i.e., total loss of a data center during a catastrophic event). The risk assessment caters to impact scenarios that are applicable to:

- only critical business functions,
- the appropriate plan document
- the affected data centers hosting production instances

A “priority one (P1) incident” does not necessarily transform into a DR event. For instance, it is out of scope to trigger the DR plan because Employee Central for a handful of customers in a single database pool has been down 10 hours at the production site. This scenario does not qualify as a DR incident.

2.2.3 Disaster Recovery Scenarios

A disaster is only declared when there is a loss of utilities and services. A loss of electricity, including backup power, would take a data center offline. A loss of connectivity to the internet would also take a data center offline. As long as the production site has power and is connected to the Internet, it will not be considered a disaster. At the highest level, there are two possible scenarios that would require we invoke the disaster recovery plan:

1. Natural Catastrophe:

This is generally an unexpected occurrence with little or no lead time. Seasonal weather patterns and geographic anomalies affect data centers in different ways, but regardless of the circumstances, the primary site is left inoperable. SAP SFSF takes a leadership role in monitoring risk, declaring a disaster and invoking the DR plan – ensuring personnel in the “failover site” are prepared to support production for a minimum of six months from handover. After the DR event has been resolved and the data center rebuilt, SAP SFSF makes the decision to reconstitute in the original production site.

2. Man-made Incident:

This, too, is an unplanned event which incapacitates infrastructure at the production site. Emergency incidents are assessed by SAP SuccessFactors and SAP Cloud Infrastructure Services (CIS). A SAP management member with proper authorization must officially declare a disaster in order to initiate a DR plan. Operations from the secondary site could last anywhere from a few days to many months. Initiation of the fallback plan is at SAP’s sole discretion.

2.2.4 Key Risks on Production Capabilities

SAP SuccessFactors conducts annual risk assessments in accordance with the American National Standards Institute (ANSI) ISO 27001 Risk Assessment and Treatment policies. Risk assessments identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to SAP SuccessFactors. The results guide and determine the appropriate action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

Before considering the treatment of a risk, SAP SuccessFactors shall decide criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is very low or that the cost of treatment is not cost-effective for the company. Such decisions are recorded. SAP SuccessFactors has evaluated the sources of risk to its business model and determined risks can result from, but are not limited to, the following:

- **Environmental Risks** are generally regional in nature and follow seasonal patterns. These natural catastrophes include blizzard, earthquake, flash flood, hurricane, thunderstorm, tornado, tsunami, wildfire and the like.
- **IT Emergency Situations** are man-made events relating to information technology. Serious equipment or system failures, information security incidents or other emergency situations (like fire and explosion of equipment) could result in a data center going offline.
- **Organized and/or Deliberate Disruption** are also man-made incidents triggered by war / civil disorder, terrorist acts, cyber-attacks, sabotage and theft

Loss of one or more of the three main components affecting business continuity are:

- IT infrastructure
- Operational infrastructure
- Employees

Enterprise-level risks are considered highly confidential and often cross multiple lines of business. Many SAP products – in addition to SuccessFactors applications -- may be hosted in the same data center (albeit in segregated cages). These applications have proprietary architectures; thus, separate recovery and continuity plans. Service restoration of these other products will not be individually detailed in this document.

2.3 On-Premise Risk Mitigation

2.3.1 Back-up Power Arrangements

All SAP SuccessFactors production data centers have uninterruptible power supplies (UPS), back-up power generators and fuel on-site to continue operations for multiple days. Local utility power feeds for data centers come into main switches located in secured areas. The utility-supplied power feeds the UPS and, in turn, the UPS feeds the distribution points where cabinets and racks are plugged in.

Should the utility power fail for a short time, the UPS instantaneously provides power and prevents an outage. If the utility power fails for an extended period, the onsite generators will start. SAP SuccessFactors data center providers test their generators periodically to ensure proper functioning. Data center providers keep several days' supply of fuel on-hand and have contracted with local vendors to provide additional supplies if required.

2.3.2 Data Back-ups and Restorations

The following reflects the standard SAP SuccessFactors policies (ISMS 10-05-01) regarding backups:

- Backups are taken of database instances and OS's from the DB servers.
- The backups are stored on disk at an off-site location using Data Domain replication.
- The retention period for essential business information and archive copies is 30 days. After that, the media will be reused.
- Backup information is classified and treated the same as production. That is, the same security controls are applied at the back-up site as media at the main site.
- Backup media is tested periodically to ensure it can be relied upon for emergency use when necessary.

The backup platform is a central system attached to a dedicated Backup LAN on which SAP SuccessFactors gets an individual (dedicated) VLAN. Inter-VLAN traffic is not permitted within this network to keep the path to the backup platform as secure as possible.

A multi-tiered backup process is used to ensure a customer's data can be recovered in a rapid and reliable manner. The Backup and Restore (B & R) procedures have the following features:

- Database Archive logs are backed up multiple times daily
- Databases are backed up on a Daily Incremental and Weekly Full basis
- All backups are copied to a local data center secondary storage system where data is encrypted using an AES256 cipher
- Each local data center secondary storage array is synchronized with a mirror storage array located in an “in region” Disaster Recovery site.

To summarize, we maintain three copies of customer data; (1) Production, (2) Primary Storage Backup, and (3) Remote Secondary Storage Backup.

2.3.3 Premises and Essential Equipment

All SAP SuccessFactors Production data centers have taken measures to help prevent or mitigate possible emergencies. All production data centers are TIA / EIA 942 Tier III+, ISO 27001 certified facilities.

2.3.4 Data Center Host Obligations for Resiliency

Environment protection mechanisms are in place and are maintained on a regular maintenance schedule. Fire detection and suppression systems are in place to help support continuity of operations. Redundant power supplies are in place to provide continuous power for computer processing in the event of electrical failure.

Production Data center hosts also provide redundant connections to the Internet.

Production Data centers are equipped with state-of-the-art equipment designed to detect, suppress and recover from fire, floods and earthquakes.

Heating, ventilation and air conditioning systems provide appropriate and consistent airflow, temperature and humidity levels. The systems are fully redundant and are monitored 24 hours a day, seven days a week. Air-cooled package chillers arranged in a redundant configuration and backed up by the generator supply provides round-the-clock chilled water supply to the precision air conditioner units.

As a countermeasure for earthquakes, structural systems meet or exceed seismic design requirements of local building codes for lateral seismic design forces. Equipment and nonstructural components, including cabinets, are anchored and braced in accordance with the requirements of the 1997 Uniform Building Code.

2.4 Recovery Requirements

Next, the impact analysis dictates the recovery requirements for each critical function. Recovery requirements consist of the following information:

- The business / application support requirements for recovery of the critical function, and/or
- The technical / infrastructure requirements for recovery of the critical function

The robustness of an emergency management plan is dependent on how much money an organization or business can place into the plan. The organization must balance realistic feasibility with the need to properly prepare. In general, every \$1 put into an emergency management plan will prevent \$7 of loss. -- BSI

It is the goal of SAP/SF to provide disaster recovery for all HCM applications that meets with our contractual obligations.

Many of our customers did not purchase disaster recovery services over and above what we include with the base subscription (i.e., standard DR services with restoration from backups). To those customers we are only obligated to restore all of their services at an alternate datacenter after a site-impacting disaster within a “commercially reasonable” amount of time.

Other customers have purchased the enhanced DR option for application products supporting critical business functions. To those customers we are obligated to restore their services at an alternate datacenter after a site impacting disaster within a prescribed amount of time (RTO) and with only a prescribed amount of data loss (RPO).

In order to carry out our obligations, SAP/SFSF has identified recovery requirements and implemented the DR strategy summarized in the sections below.

2.4.1 Data Centers

The main objective of the disaster recovery program is to ensure each SAP SuccessFactors production data center has a current and actionable failover plan to a secondary site within geographic or metro region.

The backbone of every disaster recovery solution includes:

- A primary site hosted at a SAP SFSF data center for all applications.
- A DR site hosted at a SAP SFSF data center for all applications.

The following diagram shows SAP SuccessFactors Production Data Centers. These host one or more of the SAP SuccessFactors applications. SAP SuccessFactors has consolidated operations into seven paired sites, or a total of 14 data centers. The two in each metropolitan area and/or geographic region back each other up. Essentially, if one goes offline, the other in the same region will be used as a failover.



For example, picture a customer with production applications hosted out of SAP SFSF data centers located in Amsterdam (DC2) and Rot (DC12). Applications with production instances in Amsterdam will have DR instances in Rot. Conversely, applications with production instances in Rot will have DR instances in Amsterdam. The table below lists the addresses for all of the production data centers and backup / disaster recovery sites.

Data Center	Address
Ashburn (DC8)	[REDACTED]
Chandler (DC4)	[REDACTED]
Rot (DC12)	[REDACTED]
Amsterdam (DC2)	[REDACTED]
Sydney1 (DC10)	[REDACTED]
Sydney2 (DC10DR)	[REDACTED]
Toronto1 (DC17)	[REDACTED]
Toronto2 (DC17DR)	[REDACTED]
Brazil1 (DC19)	[REDACTED]
Brazil2 (DC19DR)	[REDACTED]

Data Center	Address
Moscow1 (DC18)	[REDACTED]
Moscow2 (DC18DR)	[REDACTED]
Shanghai1 (DC15)	[REDACTED]
Shanghai3 (DC15DR)	[REDACTED]

2.4.2 Environment Redundancy

For each active production environment, SAP/SFSF will deploy a DR environment at an alternate datacenter for application products supporting critical business functions.

- The DR environment will include 100% of the compute capacity as the production environment for customers electing the legacy premium and current enhanced DR options.
- The DR environment will include the same amount of storage capacity as the production environment for *all* customers – regardless of selected DR option.

The DR environments at each datacenter will be pre-deployed with the following to ensure a failover can be completed within each customer's RTO.

- All the Web and Application virtual servers required
- All of the database pools and customer schemas required
- All integration services (e.g., Boomi, etc.) required
- All of the firewall rules, load balancer configurations and DNS records required

2.4.3 Network Redundancy

Every datacenter will have sufficient network capacity to satisfy the load of the production environments installed locally as well as the production environments installed at the alternate datacenter.

This capacity will include, but is not limited to, the following components:

- Routers
- Switches
- Firewalls
- Load Balancers

Between each pair of alternate datacenters SAP/SF will provision a point-to-point network circuit with sufficient capacity to allow data replication and backup replication to occur between the two datacenters.

2.4.4 Infrastructure Services Redundancy

Every datacenter will have sufficient infrastructure services capacity to satisfy the load of the production environments installed locally as well as the production environments installed at the alternate datacenter.

This capacity will include, but is not limited to, the following components:

- Active Directory
- Authentication and Authorization
- DNS
- Monitoring

To ensure the ability to perform a transparent DR failover, infrastructure services such as DNS as well as user Authentication and Authorization will need to be configured with active/active redundancy between sites (the typical configuration for infrastructure services under the control of Microsoft Active Directory).

Monitoring will need to be fully and independently implemented for both the production and the disaster recovery environments. This will ensure that all environments are fully monitored at all times.

In short, if infrastructure services are properly configured, no replication between redundant sets of datacenters over and above what is normally in place will be required.

2.4.5 Data Replication Basics

Continuous, asynchronous data replication is a design requirement to ensure committed service level agreements can be met for critical business functions.

All database pools will be replicated to the alternate datacenter using native database replication tools.

All NAS shares will be replicated to the alternate datacenter using operating system replication tools when possible and using storage system replication when required.

2.4.6 Distribution of Responsibilities

As the Software as a Service (SaaS) provider, SAP SuccessFactors manages all of the following:

1. Servers
2. Storage
3. Network (to include load balancers, firewalls, etc.)
4. Hypervisors
5. Infrastructure services (to include DNS, authentication/authorization, Active Directory)
6. Monitoring
7. Backups and restoration
8. Internet connectivity and dedicated link
9. Operating systems
10. Database software
11. Web Applications and application services
12. Monitoring
13. Data replication

Note: SAP SFSF uses third-party / contract personnel to augment the SAP SFSF HCM support group. In the event of a disaster, SAP SFSF would leverage these fully-experienced support engineers to assist with the failover to a secondary site.

3 SOLUTION DESIGN PHASE

The solution design phase identifies the most cost-effective recovery solution that meets two main business objectives from the impact analysis stage. For IT purposes, this is commonly expressed as (a) the minimum application and data requirements and (b) the time in which these must be available. This section outlines the required infrastructure, applications, software, data and business processes.

The solution phase determines:

- location of secondary sites
- telecommunication architecture between primary and secondary sites
- data replication methodology between primary and secondary sites
- applications and data required at the secondary site
- physical data requirements at the secondary site

3.1 Solution Landscape

Specifically, the intent of the Disaster Recovery site and plan is to protect customers if SAP experiences a catastrophe at the production data center. The technical recovery procedures allow our customers to continue accessing BizX, LMS, EC, Payroll and other products indefinitely at a secondary site. To meet service level agreements (SLAs) for critical applications, we will need to perform continuous replication of all the databases, filesystems and other data repositories to the disaster recovery sites. Applications supporting non-critical functions (as defined in an earlier section), are restored from backups.

The diagram below captures the current product availability around the globe and the landscape for disaster recovery.

REGION	DATACENTER	BizX		LMS			RMK		WFA		ONB		Mobile		Boomi		Cloud Payroll		JAM
		Prod	Preview	Prod	Preview	VSaaS	Prod	Preview	Prod	Preview	Prod								
North America	Chandler 1/HCM (HCM04)	✓	✓	✓	✓	---	---	---	✓	✓	✓	✓	✓	✓	✓	✓	---	---	✓
	Ashburn 1/HCM (HCM08)	✓	✓	✓	✓	✓	✓	Coming	✓	✓	✓	✓	✓	✓	✓	✓	---	---	✓
	Toronto 1/HCM (HCM17)	✓	✓	✓	✓	---	Coming	Coming	✓	✓	✓	✓	✓	✓	✓	✓	---	---	✓
	Ashburn 1/HCM (HCM171) - US Federal	---	---	✓	✓	---	---	---	✓	---	---	---	---	---	---	---	---	---	---
SA	São Paulo 1/HCM (HCM19)	Coming	Coming	Coming	Coming	Coming	Coming	Coming	Coming	Coming	Coming	Coming	Coming	Coming	Coming	Coming	---	---	Coming
EMEA	Amsterdam 2/HCM (HCM02)	✓	✓	✓	✓	✓	---	---	✓	✓	✓	✓	✓	✓	✓	✓	---	---	✓
	Rot 1/HCM (HCM12)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Biere 1/HCM (HCM16) -T Systems	✓	---	✓	✓	---	Coming	Coming	---	---	---	---	---	---	---	---	---	---	---
RU	Moscow 1/HCM (HCM18)	✓	✓	✓	✓	---	---	---	✓	✓	✓	✓	✓	✓	✓	✓	---	---	✓
AU	Sydney 1/HCM (HCM10)	✓	✓	✓	✓	✓	Coming	Coming	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CN	Shangai 1/HCM (HCM15) - China Telecom	✓	TBD	✓	✓	---	---	---	✓	TBD	✓	✓	✓	TBD	✓	✓	---	---	✓

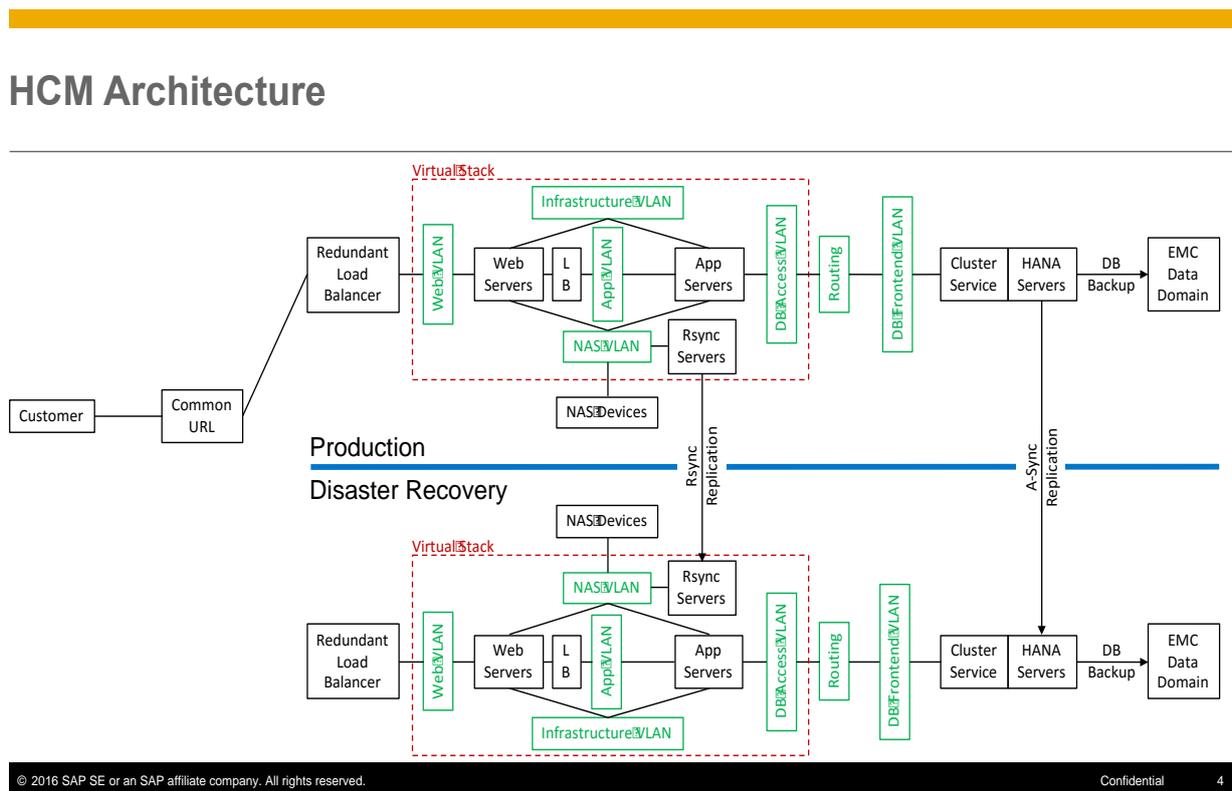
3.2 Active / Passive Data Center Model

The chosen approach for SAP Cloud Operations and the Disaster Recovery Plan is an active/passive data center model with the following features:

- Production is only “run” at either a Prod or DR data center, depending on “business as usual” or in response to a declared event.
- Data flow (i.e., replication) between data centers is based on a “store-and-forward” basis (e.g., every 15 minutes).
- Failover between a Prod site and the DR site is manually initiated and could take as long as 24 hours for critical applications which are covered by the enhanced DR option
- The failover is designed to be seamless and transparent. A single business user may not know which data center is being used at a given time.
- Software architecture (for a system / product) is designed for single-site use only.
- Hardware infrastructure may be identical (or nearly so) between data centers.
- Annual failover tests inherently come with risk and can be potentially destructive to the production environment. For this reason, simulations and use of a preview environment is encouraged for testing.

3.3 High-level Environment Diagram

The diagram below shows the production and DR environment design at a high level.



4 IMPLEMENTATION PHASE

The implementation phase primarily captures the technical requirements which dictate the “Software as a Service” solution provided by SAP SuccessFactors. This section clearly describes the HCM component architectures with diagrams of both production and disaster recovery environments. The second part of the phase focuses on deployment and configuration of the DR environment, as well as the failover steps. This phase overlaps with recovery planning methodology.

4.1 HCM Component Architectures

4.1.1 Application Architecture

The Human Capital Management (HCM) applications in the SAP SuccessFactors suite follow the standard three-tier model consisting of separate Web, Application and Database tiers. Load balancers are used to distribute user load across the different servers in the Web tier and in most cases the load balancers are also used to distribute load from the Web servers across the Application servers.

Databases are used to store all application structured data. In all but a few cases the databases are not configured as active/active but as individual database servers with cold standby servers in case of a hardware failure.

Unstructured data is stored at the Web and Application tiers on either NFS or CIFS shared filesystems hosted by NetApp NAS devices.

Database backups are written to EMC Data Domain backup appliances.

Both the structured (database) and unstructured (NAS) data will need to be replicated from the production to the disaster recovery environment. See section below labeled “Data replication” for details.

4.1.2 Integration Middleware Architecture

Dell Boomi is the enterprise integration platform used to coordinate communication between customer on-premise systems (such as SAP Payroll) and their hosted HCM applications (such as Employee Central). It is a cloud-based iPaaS solution from Dell.

The architecture of the Boomi environment at SAP/SF makes use of a load balancer to distribute the customer load across two or more redundant servers. The Boomi software itself (to include all configuration files and metadata) is installed on NFS shares with those shares mounted on all the servers in a redundant set. This allows servers to be added and removed from a redundant set with minimal effort.

The NFS shares storing the Boomi installations will need to be replicated from the production to the disaster recovery environment. See section below labeled “Data replication” for details.

4.1.3 Logical Network Architecture

The logical network architecture used at SAP/SF is consistent with industry best practices and works well with the three tier application model used by the HCM application suite.

All traffic coming in from the internet bound for Web and integration servers goes through a firewall. SSL Termination and Logical PAT (Port Address Translation) is performed by the load balancers.

Separate VLANs are used for each tier of the application as well as for other services such as NAS, Backup and Replication. Firewalls are also used to secure all traffic moving between VLANs.

Finally, data replication between redundant pairs of datacenters is done over point-to-point network circuits which are also secured using firewalls.

The SSL certificates, firewall rules and load balancer configurations will need to be replicated from the production to the disaster recovery environment. See section below labeled “Data replication” for details.

4.1.4 Infrastructure Services

The SAP/SF applications use a typical suite of infrastructure services to include:

1. Active Directory
2. DNS
3. Authentication and Authorization
4. Monitoring

To ensure the ability to perform a transparent DR failover, infrastructure services such as DNS as well as user Authentication and Authorization is configured with active/active redundancy between sites (the typical configuration for infrastructure services under the control of Microsoft Active Directory).

Monitoring is fully and independently implemented for both the production and the disaster recovery environments. This ensures that all environments are fully monitored at all times.

In short, if infrastructure services are properly configured, no replication between redundant sets of datacenters over and above what is normally in place will be required.

4.2 Deployment and Configuration of DR Environments

To ensure DR failovers can be successfully completed within our contractually obligated RTOs, SAP SFSF has pre-deployed all web and application virtual servers, physical database servers, integration virtual servers and NAS shares. Also, all load balancer configurations and firewall rules have been pre-configured.

From a network capacity perspective, there is sufficient capacity to carry the production network load of both datacenters at each datacenter with a margin of overhead. Failing to do so would likely result in either an unsuccessful failover or overloading the network at the remaining datacenter in the pair and causing either a performance problem or a complete outage.

From a compute perspective, SAP SFSF has deployed 66% of the entire production server hardware into the DR environments. This is sufficient since a sizable amount of the production compute capacity is tagged for redundancy and emergency capacity. It is extremely unlikely that we would experience a site disaster at one datacenter and a substantial compute capacity failure at the other datacenter in the redundant pair within a short period of time.

From a storage perspective, SAP SFSF has deployed the same amount of storage to the DR environments as we do the production environments. This is necessary to ensure that the DR environments do not run out of space.

Monitoring for DR environments is in place at all times, just as it is for production environments. This not only facilitates a timely failover, but also ensures that the DR environments are at all times ready for a disaster declaration.

Finally, the SAP/SF HCM software on the web and application servers is fully configured and integrated with load balancers and firewalls. In short, the only difference between the configuration of a production environment and the associated DR environment is the production application URL. The URL will be located at the production datacenter and resolve to the IP address of the applications internet facing load balancer configuration. The internet facing load balancer entry will be configured in the DR environment but there will not be an internet DNS record that points to it.

4.3 Data Replication

Database replication is done using native database tools (i.e., Oracle Data Guard, HANA SLT, etc.). This ensures all changes to the databases are replicated to the DR environment as fast as the point-to-point circuits between the data centers will allow.

Preferably, NAS replication uses rsync servers with connectivity to the NAS devices. Using the rsync servers keeps the replication and failover of NAS data under the control of HCM Operations. However, in some cases, the NAS replication needs to be done using native NetApp SnapMirror replication. In these cases, SAP SFSF works with the SAP CIS storage team to manage the data replication and the DR failover.

Additional features of data replication include the following:

- All network firewall and load balancer configurations will be simultaneously deployed to both datacenters in a failover pair.
- Infrastructure services will either be configured for active/active operations with replication (as is the case for Microsoft Active Directory) or changes will be simultaneously deployed to both datacenters in a failover pair.
- COTS packages and SAP/SF application code updates deployed to production environments will be deployed to the corresponding DR environments once it is established that they are working correctly in production.

4.4 Failover Actions Timeline



Remote access to the warm standby data center is continuously available prior and immediately after the invocation. Following the activation of the failover plan, the recovery process includes four sections:

1. Network verification requires operations staff to verify the configuration of firewalls, routers, switches, and load balancers.
2. Global traffic redirection involves preparation for changes in the DNS records of the applicable URL's. These changes may be carried out using intelligent global traffic managers hosting that record.
3. Application recovery requires Cloud Operations to verify the configuration and activate the SAP SuccessFactors applications at the recovery site. Application data replication is also verified at this time.
4. Data recovery requires operations to verify the replicated data at the recovery site.

Cloud Operations maintains recovery materials (i.e., plans, task lists, configuration sheets, etc.) in Confluence, JAM and locally.

Once the datacenter failover was complete, SAP/SF would begin to contact customers by order of priority to test their respective sites. This order would be based on the RTO and RPO we are obligated to provide as well as the individual customer's criticality ranking.

5 TESTING AND ORGANIZATIONAL ACCEPTANCE PHASE

The purpose of testing is to achieve organizational acceptance by getting stakeholder buy-in. Exercising the plan ensures the solution satisfies recovery requirements. Plans may fail to meet expectations due to inaccurate recovery requirements, solution design flaws or implementation errors. Issues found during the testing phase often highlight the need for maintenance and/or must be reintroduced to the analysis phase.

5.1 Identify Type of DR Test

There are three types of exercises that can be employed when testing disaster recovery plans. As a best practice and in preparation for the annual DR test, SAP SFSF and independent third parties may choose to perform a tabletop or medium exercise at any time.

Since the recovery strategy is the same regardless of location, SAP SFSF is required to execute only a single datacenter DR test each year and rotate the failover location around the globe. Of course, SAP SFSF may elect to perform additional tests at our discretion. All DR tests include volunteer participation by a premier, in-region customer. Additional tests of varying types may be performed and the selection of participants is at SAP's sole discretion.

5.1.1 Tabletop Exercises

Tabletop exercises typically involve a small number of people and concentrate on a single aspect of a DRP. They can easily accommodate complete teams from a specific area of a business (i.e., disaster declaration and invocation of the DR plan).

Another form involves a single representative from each of several teams. Typically, participants work through a simple scenario and then discuss specific aspects of the plan. For example, a small plane crash takes out an electrical transformer station. Both primary power and Internet service are expected to be out for several weeks.

Sometimes, the exercise consumes only a few hours and is split into two or three sessions – each concentrating on a different theme. For instance, two four-hour workshops to individually review BizX and LMS support team responsibilities during first 24 hours following a DR event.

5.1.2 Medium Exercises

A medium exercise is conducted within a "Virtual World" and brings together several departments, teams or disciplines. It typically concentrates on multiple DRP aspects, prompting interaction between teams. The scope of a medium exercise can range from a few teams from one organization co-located in one building to multiple teams operating across dispersed locations.

The environment needs to be as realistic as practicable and team sizes should reflect a realistic situation. For instance, focus of a medium exercise may be to step through each of the failover steps – with handoffs from one team / organization to another. This test may involve running scripts, providing proof of backups, capturing screenshots of replication logs, identification of NAS stores, etc. But, there is no sandbox, nor test of application functionality.

A medium exercise typically lasts a few hours, though they can extend over several days. They typically involve a DR scenario that adds pre-scripted "surprises" throughout the exercise.

5.1.3 Complex Exercises

A complex exercise aims to have as few boundaries as possible. It incorporates all the aspects of a medium exercise. This exercise remains within a virtual world and/or test environment, but maximum realism is essential. This may include any of the following: no-notice activation of the call tree, engagement of support personnel, suspension of data replication, actual failover to a secondary site, execution of import/export scripts and scheduled job runs imitating production.

While start and stop times are agreed upon in advance, the actual duration might be unknown if events are allowed to run their course. Customers with the legacy premium or enhanced DR option may elect to participate in a regional Cloud DR exercise. Selection of testers is at SAP SFSF sole discretion. Tasks include developing use cases, verifying database content and proving successful return of software functionality. Test execution is generally during the local maintenance window (i.e., Saturday mornings just after midnight).

5.2 Develop Scope and Plan Tests

SAP SuccessFactors Cloud Operations periodically performs disaster recovery tests to ensure organizational and technical measures are in place to restore customer data. A project manager from SAP SuccessFactors Cloud Operations is responsible for the success of the annual DR test. Planning generally begins eight weeks in advance. Regular updates are made to the test plans to ensure consistency with current technology and practices. Annual testing may include:

- Crisis command team call-out testing
- Failover test from primary to secondary work locations
- Application functionality verification
- Business process test

SAP SuccessFactors customers are generally deployed in a multi-tenant, public cloud. As such, there is no segregation of the customers hosted in a data center with “standard DR” from those paying for “premium options” or “enhanced DR.” There is a single datacenter-specific technical recovery procedure which conforms to the most stringent DR SLAs (i.e., 4-hour RTO and 1-hour RPO). SFSF prioritizes the order in which customers are given system access following a disaster. Essentially, customer access is granted in seven tiers (i.e., within 4-hour, 24-hour, 48-hour, 72-hour and commercially reasonable RTO).

Resources have been allocated to test the existing physical and procedural assets which support a disaster recovery at each of the nine global DR data centers. SAP SuccessFactors Cloud Operations has developed various tests to ensure customer data can be restored in the event of a disaster. Test scope varies between customers requesting a disaster recovery test. An objective may simply focus on restoration of production data to a test instance at the secondary site, or scope may expand to a recovery of many customers at once.

For example, in November 2012, Cloud Operations migrated over 100 customers from a data center being decommissioned into the Verizon Ashburn data center. This migration was performed using a DR test plan.

Another example is the failover test successfully performed in December 2014. Biz-X and LMS customers in production at the Amsterdam facility (DC2) were recovered in a test environment at the RoT Germany site (DC12) within a 24-hour RTO.

The test performed in April 2016 follows the same recovery steps after replicating data from Toronto to Amsterdam. Simply stated, this exercise is a failover of a private cloud of one customer with Biz-X and LMS.

Restoration of backups is reviewed as part of the Availability portion of the twice yearly SOC 2 audits. Several IT Direct tickets are executed as proof backups can be restored at the production site and verification that data is “recoverable, readable and not corrupt.” Additional tests are conducted and/or reviewed as part of the Availability portion of the twice yearly SOC 2 audits. These generally prove backups can be restored at the production site, and verify data are “recoverable, readable and not corrupt.” Customers and sales prospects under NDA may request copies of SOC 2 audit reports.

5.3 Identify Test Participants

SAP SuccessFactors Cloud Operations management assigns personnel from various teams to take part in the test. Teams will include: Disaster Recovery Program Office (PMO), Production Operations, Infrastructure Services and Database Management. Customers have the option to participate in a regional Cloud DR exercise. Tasks include developing use cases, verifying database content and proving successful return of software functionality. Requests should be submitted to the Disaster Recovery PMO in the quarter preceding the planned test. Selection is at SAP SuccessFactors sole discretion.

5.4 Conduct the Test

5.4.1 Backup and Restoration Testing

SAP SuccessFactors Cloud Operations will conduct routine backup and restore tests on a random sampling of servers and databases in each region. Annual disaster recovery tests are performed in accordance with ISMS policies, following established test plans. Test plans, results and after-action reports will be kept as evidence for Service Organization Control (SOC) compliance.

Redacted versions of test deliverables may be made available to customers upon request to the DR program manager.

5.4.2 Crisis Command Team Call-out Testing

Purpose of this test is to determine effectiveness of the communication plan in place. When a DR event occurs and the plan is invoked, a streamlined communication plan is executed, and all DR team members are alerted. Each team member must be familiar for his/her assigned role prior to this testing.

During the call-out, the DR Manager assembles the team, briefs the team on the nature of the (practice) event and outlines the recovery process. A (practice) task is assigned to each member. The call-out test should be executed at least once during business hours and at least once outside business hours in alternating years. The call-out list should include primary and secondary staff who are responsible for each task or area of expertise. At the closure of the call-out test, each team member's contact details are verified.

5.4.3 Failover Testing

Assuming that the DR environments have been correctly deployed and configured, a DR test would require that the following take place:

1. All database and operating system based NAS replication from the primary environments to the DR environments would be suspended
2. All DR databases at the alternate datacenter would be taken out of replication target mode and would be made read/write
3. FlexClone copies of any NAS shares using storage based replication would be created at the alternate datacenter and then mounted onto the appropriate integration, web and application servers
4. All software on the DR integration, web and application servers at the alternate datacenter would be brought online
5. Test internet facing URL's would be created to reflect the IP addresses at the alternate datacenter

Upon completion of the DR test, the following would need to take place to return to normal operations:

1. The internet facing URL's created for the test would be deleted
2. All software on the DR integration, web and application servers at the alternate datacenter would be taken offline
3. The FlexClone based NAS shares mounted for the test would be unmounted and the associated FlexClones would be deleted
4. All DR databases at the alternate datacenter would be placed in replication target mode
5. All database and operating system based NAS replication from the primary environments to the DR environments would be resumed,

5.4.4 Application Functionality Verification

After the system is recovered in the DR site, the operations team verifies basic application functionality (without visible data) before handing over the system to the customer. Below is an example of BizX health checks verifying application functionality.

Test ID	Test description	Expected result	Actual result	Status
1	Login	Successful login	Login successful	Pass
2	Top left's navigation menu is available	"Home" tab is available	Home tab is available	Pass
3		"Goal" tab is available	Goal tab is available	Pass
4		"Performance" tab is available	Performance tab is available	Pass
5		"Development" tab is available	Development tab is available	Pass
6		"My profile" is available	My Profile is available	Pass
7		"Reports" tab is available	Reports tab is available	Pass
8	Click on top left menu's "Performance" tab	Page "My Forms" is displayed	Page - My Forms is displayed	Pass
9	Click on "Create New Form" in Performance module	Page for creation of new form is displayed	Page for creation of new form is displayed	Pass
10	Click on top left menu's "Company Info" tab	Page Org Chart and <USERNAME> is displayed	Page- Org Chart and USERNAME is displayed	Pass
11	Click on top left menu's "My Profile" tab	Employee profile is displayed	Employee profile is displayed	Pass
12	Click on "Logout"	Successful logout	Logout successful	Pass

5.4.5 Business Process Test Cases

A standard set of BizX, EC and LMS test cases have been designed to validate service availability. These represent critical business functions and require performance by the end user. In this way, each customer is able to signoff on successful return to service using the same objective measure. There are two objectives for each case:

1. Validate that the application functions and the files are populated in the DR environment as generally experienced in production, and
2. Confirm data changes made in production during the previous 24 hours are also seen in the DR instance.

These tasks cannot be performed by SAP SuccessFactors; due to data privacy restrictions, a customer participant is required for this test step.

Although this may be an inconvenience, DR testing is performed after standard business hours and usually during the regularly-scheduled maintenance window on weekends.

Listed below is an example of BizX test cases for performance by the customer.

Position Management(Do not save)
Change position details for existing position
Job Info (Insert New Record but DO NOT save)
Ensure Position associations are in place
Ensure Dept to LOB to Entity associations are in place
Ensure BU to Location/Country/Working Hours etc. associations are in place
Ensure Job Code derivations are in place (eg. Officer Code etc.)
Ensure Salary Band/Structure associations are in place
Review Comp Info/OTP sections and ensure Pay Components are correct
Custom Objects
Confirm that the UI hasn't changed for Talent Profile and Home Page
Confirm configuration for talent module. Launch and delete forms
Review the custom objects and ensure they look correct
Position (Add New but DO NOT save)
Ensure Position Number is Automatic
Ensure Position Open is 'Yes'
Ensure Dept to LOB to Entity associations are in place
Ensure BU to Country/Geography Code/Working Hours etc. associations are in place
Ensure Job Code derivations are in place (eg. Officer Code etc.)
Ensure Multiple Incumbents defaults to Yes
Hire (Begin Process but DO NOT save)
Ensure Position associations are in place
Ensure Dept to LOB to Entity associations are in place
Ensure BU to Location/Country/Working Hours etc. associations are in place
Ensure Job Code derivations are in place (eg. Officer Code etc.)
Ensure Salary Band/Structure associations are in place
Review Comp Info/OTP sections and ensure Pay Components are correct
Check transactions (Begin Process but DO NOT save)
Check a Transfer - current
Check a OTP - current
Check a Compensation Change - current
Check Manager Change - current
Terminate
View aTerminated an employee
View a Terminated a non-employee
Time-off
Check and validate time-off accounts
Check all unique cases
International transfers
Expats
Role Based Permission (RBP)
Compare RBP reports vs PROD
Check all Roles (proxy and confirm that access vs RBP PDF report)
Talent(PGD)
Confirm Access to PE, Self Assessment
Compensation(CMP)
Ensure that you can access and run your Total Comp Statement
Proxy as a few employees and ensure that they can run their Total Comp Statement-Please do not save.
Reports(RPT)
Confirm that reports are exporting to Excel
Confirm that the fields have been captured and data is present in key reports.

5.5 Perform Post-test Activities

5.5.1 Assess Test Results

Cloud Operations management will review test results and determine whether they were satisfactory. Management will also review the independent auditors report on SOC 2 – Availability. SAP SuccessFactors strives to kaizen (i.e., continuously improve) operational efficiency.

5.5.2 Capture Feedback

SAP SuccessFactors management encourages test participants and customer representatives to provide feedback on tests and results in order to kaizen the process.

5.5.3 Generate Test Report for Signoff

The test report is generally produced within 10 business days following test execution – although resource constraints may require a lengthier period.

SAP SFSF has a standard template for all disaster recovery tests. Content is customized as needed to fully capture test details.

Customer signoff is expected by email reply within 10 business days following test report delivery.

Copies of past and current test deliverables are available upon request to the DR program manager.

5.5.4 Prepare for Retesting

SAP SFSF disaster recovery infrastructure and the technical recovery procedures will be refreshed on at least an annual basis. Target dates for regional tests may shift out a bit if resources are redirected to production work and/or peak season support. Evidence will be provided proving success consistent with contractual service level agreements.

6 MAINTENANCE PHASE

The maintenance phase dictates that the disaster recovery plan and related documents are refreshed at least annually with current information (e.g., contact data, runbook changes, script updates, job schedule adjustments, etc.). The annual maintenance cycle of a DRP manual is broken down into three periodic activities.

- Confirmation of information in the manual, including rollout to staff for awareness and specific training for critical individuals.
- Testing and verification of technical solutions established for recovery operations.in, at minimum, a single region
- Validation of organization recovery procedures.

Issues found during the testing phase often must be reintroduced to the analysis phase.

6.1 DR Plan Information and Targets

The DRP manual must evolve with the organization. Activating the call tree verifies the notification plan's efficiency as well as contact data accuracy. Like most business procedures, disaster recovery planning has its own jargon. Organization-wide understanding of DR terms is vital and glossaries are available. Types of organizational changes that should be identified and updated in the manual include:

- Staffing
- Third-party providers
- Vendors/suppliers
- Organization structure changes
- Communication and transportation infrastructure such as roads and bridges

6.2 Technical Requirements on Standby

Specialized technical resources must be maintained. Checks include:

- Virus definition distribution
- Application security and service patch distribution
- Hardware operability
- Application operability
- Data verification
- Data application

6.3 Testing and Verification of Recovery Procedures

As work processes change, previous recovery procedures may no longer be suitable. Checks include:

- Are all work processes for critical functions documented?
- Have the systems used for critical functions changed?
- Are the documented work checklists meaningful and accurate?
- Do the documented work process recovery tasks and supporting infrastructure allow staff to recover within the predetermined recovery time objective?
- Are backups and/or data replication jobs occurring routinely so the recovery point objective can be met?

6.4 Sharing the Plan

This document will be stored in SAP JAM along with other SAP SuccessFactors DR plans from the various offices. In addition, hard copies of this document will be distributed to or made available to team members. Team members are also encouraged to keep local copies of this plan in electronic form.

The SAP JAM page access is restricted, but located at:

https://jam4.sapjam.com/groups/gA51X6d7ynpnl0WJupMzM9/content?folder_id=pFbdSK8JeGtTvEbGzlGOyQ

The CIO, VP Security, or Director of Audit and IT Risk may authorize the DR Program Manager to share a copy of this document with external parties. This document may be shared with external parties under these conditions:

1. The external party is an existing customer or a prospect under Non-Disclosure Agreement (NDA) and a fully executed copy of the NDA has been provided to the Documentation Manager.
2. The CIO, VP of Security or Director of Audit and IT Risk has approved distribution to the external party.
3. All sensitive information has been redacted from the copy to be distributed.
4. The copy to be distributed is in PDF format with standard document protection features enabled.

6.5 Change Controls for Updating the Plan

All content must be approved by the DR program manager. All changes to the plan will be performed in accordance with the governing ISMS policies.

6.6 Responsibilities for Maintenance of the Plan

The Disaster Recovery Plan document is maintained by the DR Program Manager. Cloud Operations and Corporate Infrastructure Services are responsible for providing updates as necessary to technical procedures, architecture and other components of the DR solution. Test plans and results will be kept in Confluence or JAM for a period of time for future reference.

7 DISASTER DECLARATION AND INVOCATION PROCESS

A clearly-defined action plan is required to enable organization continuity in the event of an emergency. These activities fall into six distinct stages as described in the table below.

This process breakdown illustrates, at a high level, how a DR event is handled within the initial hours and early days following an event. The “RTO clock” starts once a disaster is formally declared. “T” in the chart below represents the disaster declaration. Therefore, any activity before declaration is noted as T minus some number of minutes (i.e., T - 60 minutes). Shown below are estimated start times for each action.

Timescales are only an estimation and simply act as a guideline for critical path events – not an absolute expectation to perform within strict time constraints.

STAGES 1 THRU 6	ACTION	EARLIEST START
Emergency Authorization and Declaration	Handling the Emergency	T - 60 minutes
	Assessing the Situation	T - 45 minutes
	Determining Potential Impact of the Emergency	T - 30 minutes
	Declaring a Disaster	T + 0 minutes
Disaster Management	Establishing a Response and Recovery Center	T + 15 minutes
	Mobilizing the Disaster Recovery Team	T + 30 minutes
	Maintaining the Event Log	T + 30 minutes
	Recording Project Management Activities	T + 30 minutes
Communication Plan Activation	Kicking Off Management Meetings	T + 45 minutes
	Opening a Phone Bridge	T + 60 minutes
	Reviewing and Documenting Status	T + 90 minutes
	Communicating with the Press	T + 2 hours
	Communicating with Customers	T + 2 hours
Failover Plan Execution	Implementing the Failover Steps	T + 3 hours
	Performing Functionality Health Checks	T + 20 hours
System Access and Service Availability	Granting System Access by Priority Group	T + 24 hours
	Validating Service Availability	T + 24 hours
	Expanding Compute Capacity (if necessary)	T + 4 days
	Declaring “Disaster Over”	T + 5 days
	Producing a DR Process Report	T + 7 days
Reconstitution (optional)	Reconstructing the Original Primary Site	T + n weeks
	Initiating the Failback Steps	T + n months

Throughout the first 24 hours, activities and procedures will fall into the first four stages noted above. The initial goal is to counteract the disaster and stabilize in a secondary site. Ultimately, the objective is to return access to critical business systems in stage five. Full compute capacity for non-critical functions could extend days beyond the event. The sixth stage for reconstitution back to the primary site is dependent on damage repair and data center reconstruction.

7.1 Emergency Authorization and Declaration Stage

This first stage is likely to involve emergency services. **The priority during this phase is the safety of employees, contractors, and other people involved in the event.** One or more of these circumstances could imply a disaster has occurred or is imminent.

- Employees could be at risk of harm or injury
- Buildings or property suffers extensive damage (i.e., cannot be occupied),
- People will be asked to stay home from work due to local emergency situations, including pandemics
- Power outages for the entire data center are expected to exceed 24 hours
- You anticipate significant interaction with law enforcement agencies
- There is a nationwide or a locally-declared “state of emergency”
- Significant business systems are disrupted or inoperative
- Tragic accident or event in vicinity of the data center

In addition to the emergency services, this activity may involve different personnel from outside the production data center.

7.1.1 Handling the Emergency

Estimated Start: T – 60 minutes

The first stage of handling the emergency involves assessment of the initial emergency situation. Someone must determine at an early point whether the DR team must be involved. This section of the plan covers the identification of the emergency, mobilizing the DR Team, and assessing the scale of the emergency.

Following a serious, high impact priority one (P1) incident, a ticket is created and the VP, SAP Cloud Operations is contacted. The initial step is to evaluate the present circumstances.

1. The emergency itself must be resolved (e.g., the fire extinguished, or the floodwaters pumped out).
2. The threat of further damage should be minimized (e.g. stay sheltered during extreme weather events, work once the storm has passed).
3. Essential services must be restored (e.g., power, water, and telecommunications).

In addition to the emergency services, this activity may involve different personnel from outside the production data center. A Disaster Recovery Team (DRT) may need to be assembled based on the assessment in the next step. But, pre-invocation call may be made to put the disaster recovery service on standby, thereby reducing the response time should the plan be formally invoked.

7.1.2 Assessing the Situation

Estimated Start: T – 45 minutes

This assessment will be performed by a member of SAP senior management -- who will also make a decision if the customer team needs to be assembled. Pre-defined trigger points are needed to guide actions during an emergency and, in particular, to decide whether or not the DR Plan is to be implemented.

Criteria for determining whether an emergency situation requires the mobilization of the DR Team are in the table below. If one or more are applicable, the DR Team will likely be engaged.

Criteria	Applicable?
Application is unavailable to all clients	
Systems are offline	
Networking is offline	
ISP is offline	
Major infrastructure problems	
Primary site is offline	
Storage is offline	

7.1.3 Determining Potential Impact of the Emergency

Estimated Start: T – 30 minutes

An assessment to determine the potential scale of the emergency from a business perspective is to be made at regular intervals during the recovery process, and recorded on this form. (The initial assessments will usually be carried out by the DR Team who may call on other specialists to help with this process as appropriate.)

Description of Disaster:
Start Date:
Date DR Team Mobilized:

Business Process Affected	Status Level	Assessment Done By	Comments

Use the following status levels:

- 1 - Primary site no longer exists
- 2 - Primary site offline long-term
- 3 - Primary site offline short-term
- 4 - Application not available
- 5 - Major application problems

7.1.4 Declaring a Disaster

Estimated Start: T + 0 minutes

Declaring a disaster can be a difficult process particularly in the early stages of an event. SAP SuccessFactors will declare a disaster and invoke the recovery plan when specific criteria are met. Keep in mind, a disaster is only declared when there is a loss of utilities and services. A loss of electricity, including backup power, would take a data center offline. A loss of connectivity to the internet would also take a data center offline. As long as the production site has power and is connected to the Internet, it will not be considered a disaster.

The following personnel are authorized to invoke the DR plan:

- CIO, SAP CIO
- VP, SAP IT Security and Risk Office
- SVP, SAP SaaS Cloud Operations
- VP, SAP SFSF Cloud Delivery, US Cloud Operations
- VP, SAP SFSF Cloud Delivery, EU Cloud Operations
- VP, SAP SFSF Cloud Delivery, Bangalore

Once a disaster is declared, the employee who made the declaration will notify other personnel listed in the Appendix via phone, text message, or email. The IT Managers have a method of sending out bulk SMS messages. This method will be adopted in the event of requiring a communication channel with staff and line employees.

7.2 Disaster Management Stage

Maintaining good levels of communications is one of the most important factors during the disaster recovery process. It is important that any information released is both accurate and timely. It is necessary to keep various groups informed including the Disaster Recovery Team, the Business Recovery Team, senior management, media, and other key members of staff.

7.2.1 Establishing a Response and Recovery Center

Estimated Start: T + 15 minutes

Formally identify the Recovery Coordinator. If available, this is generally the SVP of SAP SaaS Cloud Operations. If this person is unavailable, the Recovery Coordinator is the VP of Cloud Operations for the region. If these people cannot be reached, it is the VP, SAP IT Security and Risk Office.

The recovery coordinator is responsible for the overall effort, team engagement and delegation of responsibilities as necessary.

The global recovery team will be assembled from staff with the following areas of expertise: Data center operations, Networking, Database and storage, Virtualization, and Application Support. Team members may be selected from SAP, SAP SFSF, the SaaS or third party providers.

The local recovery team members and/or third-party vendors may require physical access to the data center facility. Remote team members will likely already have VPN access, but there may be new personnel. All persons requiring access must be identified, along with relevant telephone numbers and email addresses. The SAP SFSF Data Center Executive will facilitate physical entry and/or VPN access.

7.2.2 Mobilizing the Disaster Recovery Team

Estimated Start: T + 30 minutes

Use this form to record the mobilization of the DR Team following an emergency situation.

Description of Emergency			Date Occurred:		
Team Member	Contact Method	Contacted On	By Whom	Response	Time of Arrival On Site / Call
Comments:					
Comments:					
Comments:					
Comments:					
Comments:					
Comments:					

7.2.3 Maintaining the Event Log

Estimated Start: T + 30 minutes

During disaster recovery, employees will maintain logs to record their activities. The Disaster Recovery Team leader (or a nominated team member) will record key events during the Disaster Recovery process, until responsibility is handed over to the Business Recovery team.

Disaster Description:
Start Date:
Date DR Recovery Team Mobilized:

Key Activities Undertaken by DR Recovery Team	Time & Date Started	Outcome	Follow up Action Required

7.2.4 Recording Project Management Activities

Estimated Start: T + 30 minutes

During the Disaster Recovery Process all activities will be determined using a standard structure. When necessary, this plan may need to be updated on a regular basis throughout the Disaster Recovery period. All events during this phase will also need to be recorded.

Activity Name:
Reference Number:
Brief Description:

Start Date	Completion Date and Time	Resources Involved	Individual In Charge

7.3 Communication Plan Activation Stage

Maintaining good levels of communications is one of the most important factors during the disaster recovery process. It is important that any information released is both accurate and timely. It is necessary to keep various groups informed including the Disaster Recovery Team, the Business Recovery Team, senior management, media, and other key members of staff.

7.3.1 Kicking Off Management Meetings

Estimated Start: T + 45 minutes

If it is necessary to call a formal meeting, this ought to take place inside 1 hour of the event. It may not be feasible to get all members of the team together in these timescales. Subsequently, all critical management members should be identified, briefed and documented in the strategy.

The DR Event Management Team's principal function would be to:

- Define the situation
- Define the extent of the disruption, the effective date and time
- Evaluate the most likely impact on customers
- Estimate how long disruption may last
- Invoke disaster recovery plan and gather response team
- Formally set up Response and Recovery Center
- Agree on team's objectives for next 3 hours
- Agree on formal verbal report for senior management
- Agree on staffing levels needed at the present time
- Send non-essential staff home (if for the duration of workplace hours)
- Contact non-vital staff at home (if outside of standard business hours)
- Call in additional staff support (if outside of standard business hours)
- Set up subsequent meeting for T + 4 hours
- Open a bridgeline for remote team members

7.3.2 Opening a Phone Bridge

Estimated Start: T + 60 minutes

Once notifications have been sent, Cloud Operations and Corporate IT will open a phone or online bridge. The phone bridge will remain open as the event unfolds to keep a line of communication open. Participants will include as many of the following personnel as possible:

- CIO, SAP Global Delivery
- VP, SAP IT Security and Risk Office
- SVP, SAP SaaS Cloud Operations
- VP, SAP SFSF Cloud Delivery, US Cloud Operations
- VP, SAP SFSF Cloud Delivery, EU Cloud Operations
- VP, SAP SFSF Cloud Delivery, Bangalore
- VP, SAP SFSF SaaS Cloud Operations, Application Management
- VP, Product Implementation, HCM Cloud Delivery
- SAP Chief Legal Counsel
- Sr Director, Global Database Operations, HCM Cloud Delivery
- Director, Program Management Office
- DR Program Manager
- Data Center Executive
- Other IT directors, managers and personnel as appropriate for the location and type of event.

On this call, the SAP team will discuss the event, response plans, roles and responsibilities, and critical action items. Team members will provide status updates from various perspectives. A team member will be identified to notify senior management of progress. Another team member will be identified to send status updates to Customer Success for communication to customers.

The phone bridge is to remain open unless/until the call leader determines it can be ended. The call leader is the most senior person on the call. The call may be suspended and resumed at the call leader's direction.

7.3.3 *Reviewing and Documenting Status*

Estimated Start: T + 90 minutes

At this stage, the team lead must have a substantially more detailed understanding of the situation. This will enable a full written report to be produced for senior management. The Disaster Management Team will have by this time:

- Invoked the disaster recovery plan
- Set up a temporary Response and Recovery Center
- Established an open bridgeline
- Mobilized vital staff members
- Prepared to activate the failover plan

Once the disaster recovery plan is invoked, the employee who made the invocation will notify other personnel via phone, text message, or email.

The IT Managers have a method of sending out bulk SMS messages. This method will be adopted in the event of requiring a communication channel with a larger employee audience.

As another means of internal communication the Outage Notification JAM group will be kept up-to-date. The Group URL is: <https://jam4.sapjam.com/groups/wall/0BHraGPOX2fRHZxzYE6qyh>

7.3.4 *Communicating with the Press*

Estimated Start: Inside 1 hour (T + 2 hours)

All employees must refer all inquiries from the media, analyst, financial, political, and academic communities – regardless of how, where, and when they are received – to SAP Global Communications. Responses may only be offered in coordination with SAP Global Communications. For more information, see the SAP Communications Policy at:

https://portal.wdf.sap.corp/irj/go/km/docs/corporate_portal/Global%20Communication%20for%20SAP/GLOBAL/Policies%20%26%20Guidelines/Global%20Policies/PolicyDocuments/5_Communications_Policy.pdf

In the event of any disaster, the only people authorized to make any announcements to the press are:

1. _____, VP, Corporate Communications
2. _____, General Counsel
3. _____, SVP of Business Operations

In the unlikely event that the VP of Corporate Communications, General Counsel, and SVP of Business Operations are unavailable, any C Level SAP Cloud Executive is then authorized to make the appropriate public announcement.

4. _____, Chief Information Officer, SAP Global Delivery
5. _____, Other C-level SAP Cloud Executive

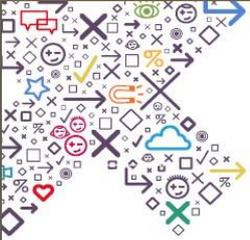
7.3.5 Communicating with Customers

Estimated Start: Inside 1 hour (T + 2 hours)

Once an issue has been identified and acknowledged, Cloud Operations will communicate with Customer Success and Legal. Customer Success will send Legal-approved messages to impacted customers.

When an incident occurs, Customer Success will attempt to notify all affected customers via email. Customer Success will initiate and follow the normal Outage Notification Process to communicate with customers. Customer Success Incident Managers are assigned in each region and are dedicated to frequent customer communication.

The Customer Success (CS) Communication Plan is summarized here:



CUSTOMER SUCCESS
successfactors[™]
An SAP Company

SuccessFactors Outage Notification Process

Communicating Status and Root Causes

Site availability and system performance are the highest priority for SuccessFactors. We recognize that alerting customers when we have a system issue is a critical function, so we have established a system outage notification process when incidents occur. We are committed to restoring services as quickly as possible while keeping customers informed, and have created the following goals for handling system outages.

	SuccessFactors Internal Process	Customers Can Expect
<p>Phase 1 Identification</p>	<p>Objective: Initial Customer Notification</p> <ol style="list-style-type: none"> 1. Issue identified 2. Incident Manager, internal teams and SuccessFactors executives alerted 3. Communication bridge opened between Support, Operations and Engineering 4. Customers impacted and level of impact determined 	<p>An incident notice targeted to occur within 1 to 2 hours (depending on impact)</p>
<p>Phase 2 Isolation</p>	<p>Objective: Troubleshooting & Ongoing Customer Updates</p> <ol style="list-style-type: none"> 1. Operations and Engineering teams work to troubleshoot issue 2. Incident Manager notifies, and regularly updates, support teams 	<p>Update notices targeted to occur every 1 to 6 hours</p>
<p>Phase 3 Resolution</p>	<p>Objective: Issue Resolution Communication</p> <ol style="list-style-type: none"> 1. Issue resolution and time to service restoration identified 2. Incident Manager notifies support teams 	<p>A resolution notice</p>
<p>Phase 4 Root Cause</p>	<p>Objective: Root Cause Analysis</p> <ol style="list-style-type: none"> 1. Operations and Engineering teams perform root cause analysis 2. Corrective action to avoid future incidents identified 	<p>Root Cause Analysis notice targeted to occur within 1 week</p>

Follow the Sun Notifications

When an incident occurs, our goal is to notify all customers affected via email, 24 x 7. Customers can also receive real-time notices by requesting to follow [SAPCloudSupport](#) on Twitter. Customer Success Incident Managers are assigned in each region and are dedicated to frequent customer communication.

Customers can also follow @SAPCloudSupport on Twitter for live updates. Note that only confirmed followers have access to these tweets.

7.4 Failover Plan Execution Stage

Following the formal declaration of a disaster, Cloud Operations will execute failover strategies. Key Teams involved will include Cloud Operations, Operations Control Center (OCC), SAP Cloud Factory, ██████████ DBAs, and Customer Success.

The recovery process includes three sections: network recovery, data recovery, and application recovery. Network recovery requires operations to verify the installation and configuration of firewalls, routers, switches, and load balancers. Data recovery requires operations to verify and restore data to the recovery site. Application recovery requires Cloud Operations to verify the configuration and activate the SAP SuccessFactors application at the recovery site.

Cloud Operations maintains recovery materials (i.e., plans, task lists, configuration sheets, etc.) in Confluence, JAM and locally. Below is a summary of steps to be taken to recover in a secondary site.

7.4.1 Implementing the Failover Steps

Estimated Start: T + 3 hours

In the event of a datacenter site failure, the following would take place:

1. All DR databases at the alternate datacenter would be taken out of replication target mode and would be made read/write
2. All NAS shares at the alternate datacenter using storage based replication would be taken out of replication target mode, would be made read/write and then mounted onto the appropriate integration, web and application servers
3. All software on the DR integration, web and application servers at the alternate datacenter would be brought online
4. The internet facing URL's would either have their internet DNS records changed to reflect IP addresses at the alternate datacenter or global load balancing would be used to automatically redirect the URL's to IP addresses at the alternate datacenter.
5. These IP addresses will (as previously mentioned) be present and configured on load balancers to distribute user connections across the correct groups of web and integration servers

Provided that all environment, network and infrastructure services configurations are correct and that all data had been properly replicated; this will result in the affected production environments being made available at the alternate (DR) datacenter.

7.4.2 Performing Functionality Health Checks

Estimated Start: T + 20 hours

Verifications and testing is performed by Cloud Operations and quality assurance to verify the application is functioning properly. Cloud Operations performs network, web, application, and database testing. These "health checks" guarantee the systems are completely operational ahead of the announcement to end user.

Final verification results are reviewed in a Go / No-Go decision meeting. If decision is a Go, the site will be activated in the next stage. If the decision is No-Go, Cloud Operations will evaluate and address outstanding issues before re-attempting.

SAP SuccessFactors relies on a quorum among the following personnel to make the Go / No-Go decision:

- CIO, SAP Global Delivery
- VP, SAP IT Security and Risk Office
- SVP, SAP SaaS Cloud Operations
- VP, SAP SFSF Cloud Delivery, US Cloud Operations
- VP, SAP SFSF Cloud Delivery, EU Cloud Operations
- VP, SAP SFSF Cloud Delivery, Bangalore
- VP, SAP SFSF SaaS Cloud Operations, Application Management
- VP, Product Implementation, HCM Cloud Delivery

7.5 System Access and Service Availability

7.5.1 Granting System Access

Estimated Start: T + 24 hours

Restoration of production instances will be prioritized according to each customer's contract terms and the DR options in force at time of disaster.

Note that the "RTO clock" starts once a disaster is formally declared.

For non-production systems (i.e., Sales Demos, Test, Preview and Development), a formal disaster recovery strategy will not be implemented; these are handled with "commercially reasonable effort" to restore as soon as possible – after production environments have been returned to service.

Partner Development systems are handled like a production system.

7.5.2 Validating Service Availability

Estimated Start: T + 24 hours

A standard set of BizX, EC and LMS test cases have been designed to validate service availability. These represent critical business functions and require performance by the end user. In this way, each customer is able to signoff on successful return to service -- using the same measure. There are two objectives for each case:

1. Validate that the application functions and the files are populated in the DR environment as generally experienced in production, and
2. Confirm data changes made in production during the previous 24 hours are also seen in the DR instance.

These tasks cannot be performed by SAP SuccessFactors; due to data privacy restrictions, a customer participant is required for this test step.

7.5.3 Expanding Compute Capacity

Estimated Start: T + 4 days

From a compute perspective, SAP SFSF has deployed 66% of the entire production server hardware into the DR environments. This is sufficient since a sizable amount of the production compute capacity is tagged for redundancy and emergency capacity. It is extremely unlikely that we would experience a site disaster at one datacenter and a substantial compute capacity failure at the other datacenter in the redundant pair within a short period of time. Procurement orders will be started as soon as possible to backfill the repurposed redundant capacity.

7.5.4 Declaring "Disaster Over"

Estimated Start: T + 5 days

A disaster will be declared to be over when full service has been restored with full Disaster Recovery capability at the secondary site. Only the SAP SuccessFactors CIO or their designated delegate may declare that a disaster is officially over, and SuccessFactors applications are operational as it would be at the production site.

7.5.5 *Producing a DR Process Report*

Estimated Start: T + 7 days

After the initial Disaster Management stage ends and the failover plan has been executed, the Recovery Coordinator will write a report with the content about the event, the response, and the outcome. Content will include:

- Description of the event/emergency
- People notified of the emergency with date and time of notification
- Actions taken by the DR Team members
- Results from the actions taken
- An assessment of the impact to business operations
- An assessment of the DR plans effectiveness
- Lessons learned and suggestions for improving plans and processes

Reports will be kept for a period of time for future reference.

7.6 *Reconstitution Stage*

7.6.1 *Reconstructing the Original Primary Site*

Estimated Start: T + n weeks

Reconstitution back to the primary site is dependent on damage repair and data center reconstruction. Depending on the severity, return to the original production site can occur weeks or months after the event. Alternately, SAP SFSF may decide reconstruction is cost-prohibitive and elect to remain in the failover site indefinitely. Thus, the Reconstitution Stage could be skipped altogether. If a feasible opportunity, the following are major factors in reconstructing the original environment.

1. **Power and Other Utilities:** Production data center hosts will work with the local utilities to restore services. The host companies have local power generators and several days' supply of fuel. They have contracted with local suppliers to ensure additional deliveries if required.
2. **Communications Systems:** Production data center hosts will work with its local telecommunication companies and Internet Service Providers (if required) to restore services.
3. **IT Systems (Hardware and Software):** In Production data centers, SAP SuccessFactors will work with its vendors to procure equipment to repair/rebuild/ replace equipment as required.
4. **Premises, Fixtures and Furniture (Corporate Office Facilities Recovery Management):** For Production data centers, the host company will work with local vendors to restore the local premises, fixtures and furniture.
5. **Other Equipment:** SAP SuccessFactors will work with SAP Cloud Infrastructure Services to procure equipment to revamp / rebuild.

7.6.2 *Initiating the Failback Steps*

Estimated Start: T + n months

For disasters where failback will be possible, once the production systems were restored the following would take place:

1. All production databases at the recovered datacenter would be placed in replication target mode
2. All NAS shares at the recovered datacenter using storage based replication would be placed in replication target mode
3. Reverse replication of the databases and NAS filesystems would be established from the alternate datacenter back to the recovered datacenter
4. Reverse replication would be allowed to become current and complete.
5. During the next maintenance window, all software on the DR integration, web and application servers at the alternate datacenter would be taken offline
6. A final reverse replication cycle would be allowed to run and complete
7. All Production databases at the recovered datacenter would be taken out of replication target mode and would be made read/write
8. All NAS shares at the recovered datacenter using storage based replication would be taken out of replication target mode, would be made read/write and then mounted onto the appropriate integration, web and application servers
9. All software on the Production integration, web and application servers at the recovered datacenter would be brought online
10. The internet facing URL's would either have their internet DNS records changed to reflect IP addresses at the recovered datacenter or global load balancing would be used to automatically redirect the URL's to IP addresses at the recovered datacenter.
11. All DR databases at the alternate datacenter would be placed in replication target mode
12. All NAS shares at the alternate datacenter using storage based replication would be placed in replication target mode
13. Replication of the databases and NAS filesystems would be established from the recovered datacenter to the alternate datacenter

APPENDIX

Appendix 1 – Abbreviations and Acronyms

Appendix 2 – Definitions and Terminology

Appendix 3 – SAP SuccessFactors Contact List

Appendix 4 – Key Leasors, Data Center Operators and Emergency Contacts

Appendix 1 – Abbreviations and Acronyms

Acronym	Stands for...
AAtd	Administrator's Access to Data
AKA	Also Known As
ANSI	American National Standards Institute
B & R	Backup and Restore
BC	Business Continuity
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BRT	Business Recovery Team
CIS	Cloud Infrastructure Services
COTS	Commercial Off the Shelf Software
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DRT	Disaster Recovery Team
IaaS	Infrastructure as a Service
HA	High Availability
HCM	Human Capital Management
IaaS	Information as a Service Provider
ISMS	Information Security Management Systems
ISO	International Standards Organization
P1	Priority One Incident
RACI	Responsible, Accountable, Consulted and Informed Chart
RCap	Restore 100% Capacity
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAP SFSF	SAP SuccessFactors aka primary Software as a Service provider
SLA	Service Level Agreement
TRA	Threat and Risk Analysis
TRP	Technical Recovery Procedures
UPS	Uninterruptible Power Supplies

Appendix 2 – Definitions and Terminology for this document

Term	Definition
Backups	<p>SAP SuccessFactors backs up data daily using a disk-to-disk system; we do not use tapes. SAP SuccessFactors does both full and incremental backups. We also backup transaction archives. Backups are mirrored across data centers, with data centers in the same region backing up one another. That is, backup data is securely transferred across private networks from the primary to the secondary data center.</p> <p>SAP SuccessFactors has implemented a delay in the replication of mirrored data to prevent possibly corrupted production data from being instantaneously copied to the backup. Were that to happen, the backed up data would be corrupted as well.</p>
Disaster	<p>Any unexpected event that causes a total loss of a data center. In this type of scenario, it is unlikely the entire data center can be accessed and/or recovered again. The typical disaster involves earthquake, fire, flood, hurricane, plane crash, terrorist attack or tsunami, for example, which causes extensive and not immediately repairable damage to the facility and/or data center.</p> <p>A disaster is only declared when there is a loss of utilities and services. A loss of electricity, including backup power, would take a data center offline. A loss of connectivity to the internet would also take a data center offline. As long as the production site has power and is connected to the Internet, it will not be considered a disaster.</p>
Disaster recovery (DR)	<p>Disaster recovery (DR) should not be confused with High Availability (HA). DR typically requires a formal declaration of a disaster by management prior to initiating any recovery procedure. HA addresses the avoidance of single points-of-failure within hardware, software and/or data center architectures such that failure in any one component is immediately, automatically and transparently transferred to a duplicate component.</p>
Data Replication	<p>SAP SuccessFactors uses native database tools to replicate data from the primary production site to the standby DR site for data recovery purposes.</p>
High Availability Architecture (HA)	<p>SAP SuccessFactors' infrastructure architecture is designed with high availability in mind. For example, production data centers have uninterruptible power supplies (UPS) and backup power generators and redundant Internet connections. They have raised floors to help avoid floodwaters, as well as redundant HVAC systems and fire suppression systems. Production data centers have strict access controls -- continuously staffed and monitored to help prevent acts of sabotage or vandalism. All SAP SuccessFactors' production data centers are TIA / EIA 942 Tier III+, SOC audited or ISO 27001 certified facilities.</p>

Term	Definition
HA (cont.)	SAP SuccessFactors production data centers are geographically dispersed, to help prevent a single event from affecting more than one data center. In the event a Production data center has an outage we failover to the other data center in the same geographic region to minimize impacts to customers. Our Cloud Operations teams are also geographically dispersed, working in offices in the US, Europe, South America, and India. Should an office be impacted by an environmental event or pandemic, other offices can continue operations.
JAM	SAP JAM is a cloud-based enterprise social networking suite and collaboration app that helps users connect with employees, partners, and customers. SAP JAM can be utilized to protect company data by collaborating over a secure network.
RACI	A responsibility assignment matrix (RAM), also known as RACI chart, describes the participation by various roles in completing tasks or deliverables for a project or business process.
Recovery Point Objective (RPO)	Answers the question: How old is the data when system is returned to service? The RPO is the maximum age of files that must be recovered from backup storage for normal operations to resume. Upon a declared test or actual disaster, the business-critical application will be reverted to a prior state no older than the RPO stated in the customer's contract.
Recovery Time Objective (RTO)	Determines how quickly infrastructure can be re-established and the business-critical application brought back up. The RTO is the length of time that a computer, system, network, or application can be down. RTO represents the time needed to get an application up, running and accessible to the system administrator after a declared disaster. The requirement is to have the customer's Administrator Access to Data (AAtd) within the RTO stated in the customer's contract.
Restore 100% Capacity (RCap)	Sets a target for how much time is needed to run again at full production capacity. The RCap is the time it takes to get critical business functions back up-and-running at full production capacity once the systems (i.e., hardware, software and configuration) are restored to the RPO. This includes the manual and automated processes necessary to verify that the system has been restored to the RPO, and all necessary steps to address the remaining lost or out-of-synch data. This value may vary by application module depending on the priority to the organization. Restoration target is generally stated in the customer's contract.
Service Level Agreements (SLAs)	<p>Customers should review their contract to understand SAP SuccessFactors obligations with regard to uptime, recovery point objective (RPO) and recovery time objective (RTO). Contracts vary quite a bit depending on the application modules and DR option purchased at time of sale.</p> <p>Should there be a catastrophic event that wipes out a data center, customers are granted access in priority groups according to their elected service level agreements.</p>

Appendix 3 – SAP SuccessFactors Contact List

#	Name / Role	Office Phone	Email
1.	[REDACTED]	[REDACTED]	[REDACTED]
2.	[REDACTED]	[REDACTED]	[REDACTED]
3.	[REDACTED]	[REDACTED]	[REDACTED]
4.	[REDACTED]	[REDACTED]	[REDACTED]
5.	[REDACTED]	[REDACTED]	[REDACTED]
6.	[REDACTED]	[REDACTED]	[REDACTED]
7.	[REDACTED]	[REDACTED]	[REDACTED]
8.	[REDACTED]	[REDACTED]	[REDACTED]
9.	[REDACTED]	[REDACTED]	[REDACTED]
10.	[REDACTED]	[REDACTED]	[REDACTED]
11.	[REDACTED]	[REDACTED]	[REDACTED]
12.	[REDACTED]	[REDACTED]	[REDACTED]
13.	[REDACTED]	[REDACTED]	[REDACTED]
14.	[REDACTED]	[REDACTED]	[REDACTED]
15.	[REDACTED]	[REDACTED]	[REDACTED]
16.	[REDACTED]	[REDACTED]	[REDACTED]

Appendix 4 – Key Leasors, Data Center Operators and Emergency Contacts

The following external data center operators should be contacted by SAP SuccessFactors and/or the Cloud Infrastructure Services team, as appropriate, in the event of a disaster situation.

Data Center	Leasor / Data Center Operator	Type
Ashburn (DC8)	[REDACTED]	[REDACTED]
Chandler (DC4)	[REDACTED]	[REDACTED]
Rot (DC12)	[REDACTED]	[REDACTED]
Amsterdam (DC2)	[REDACTED]	[REDACTED]
Sydney1 (DC10)	[REDACTED]	[REDACTED]
Sydney2 (DC10DR)	[REDACTED]	[REDACTED]
Toronto1 (DC17)	[REDACTED]	[REDACTED]
Toronto2 (DC17DR)	[REDACTED]	[REDACTED]
Brazil1 (DC19)	[REDACTED]	[REDACTED]
Brazil2 (DC19DR)	[REDACTED]	[REDACTED]
Moscow1 (DC18)	[REDACTED]	[REDACTED]
Moscow2 (DC18DR)	[REDACTED]	[REDACTED]
Shanghai1 (DC15)	[REDACTED]	[REDACTED]
Shanghai3 (DC15DR)	[REDACTED]	[REDACTED]

Revision History:			
Date	Version	Description	Who
09/28/2012	V01	Draft	[REDACTED]
1/30/2013	V1.0	New document	[REDACTED]
2/20/2013	V1.1	Updated cover page statement. Added RTO clock information to page 26. Added Declaration of "Disaster Over" section to page 29.	[REDACTED]
3/8/2013	V1.2	Minor updates to Phase IV wording on page 21. From customer perspective, URLs do not change.	[REDACTED]
3/25/2013	V1.3	Minor edits.	[REDACTED]
3/27/2013	V1.4	Updated formatting	[REDACTED]
4/4/2013	V1.5	Minor edits	[REDACTED]
4/19/2013	V1.6	Minor edits	[REDACTED]
4/22/2014	V1.7	Minor edits. Updated contact info. SharePoint now hosted at Verizon Ashburn.	[REDACTED]
10/31/2014	V2.0	Minor edits	[REDACTED]
2/2/2016	V3.0	Converted Disaster Recovery Plan template to SAP standard format.	[REDACTED]
2/9/2016	V3.1	Refreshed DR Plan template with 2015-16 program information.	[REDACTED]
2/23/2016	V3.2	Improved format with numbering scheme. Incorporated Mary Walby's comments.	[REDACTED]
2/19/2016	V3.2	Added table of DR options and expanded section on testing.	[REDACTED]
2/26/2016	V3.3	Minor formatting, added ISMS, DPMS, and security links.	[REDACTED]
3/8/2016	V3.4	Incorporated Mary's comments, updated footer, added SuccessFactors Contact List, and Updated DR Project Team contacts.	[REDACTED]

Revision History:			
Date	Version	Description	Who
04/26/2016	V3.5	Included instructions for converting template to a customer-specific disaster recovery plan. Modified table of recovery options and inserted recovery priority groups. Incorporated updates from Abe Phillips.	[REDACTED]
05/02/2016	V3.6	Corrected conflicting service level agreement statements in Section 1.2 by referring to tables in Section 10 of this document. Also, expanded descriptions in 12.1.1 and 12.2.3 to include seven tiers as shown in Section 10 tables.	[REDACTED]
09/23/2016	V4.0	Merged DRP template (version 3.6) with a premier customer's BCP template (version 1.0) for consistency between two plan types. Incorporated relevant sections of DR Strategy document.	[REDACTED]
09/22/2017	V5.0	Performed annual review as required for SOC compliance. Changed footer to "customer-facing" document. Updated links in Section 1.3 and 1.5. Spelled out SOC as Service Organization Control in Section 2.1. In 2.1, replaced application names with product descriptions. <i>Confirmed critical business functions as solely BizX, EC and LMS.</i> In 2.2, expanded table to match revised 2017 Sales Spec Sheet. Corrected SAP CIS to Cloud Infrastructure Services in Section 2.2.3 and Appendix 1. Expanded on test definitions and sample scenarios in Section 5. Updated table with new SAP contact information in Appendix 3.	[REDACTED]
10/13/2017	V6.0	<p>Eliminated appendix of Key IT Supplier phone numbers. SAP CIS acts as IaaS for SuccessFactors. Hardware vendor calls would be made solely by SAP CIS on behalf of SFSF.</p> <p>Removed references to the SAP SFSF business continuity (BC) plans. (These are maintained by a separate organization outside the DR program and under different SOC controls.)</p> <p>Removed chart of recovery priorities from Section 7.5.1 (and put in DR Strategy only).</p>	[REDACTED]

© 2015 SAP SE or an SAP affiliate company. All rights reserved.
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice.

The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.