CONFIDENTIAL

Disaster Recovery Plan
SAP Ariba Procurement and Business Network Procurement and Business Network
Production Site to DR Site

May 27, 2025
Version 2025.1.0

This document contains the overarching disaster strategy as provided by SAP Ariba Procurement and Business Network. This plan is applicable for all production data centers as described. SAP policy requires this plan be reviewed at least annually.

THE BEST RUN SAP

This page is intentionally blank.

TABLE OF CONTENTS

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

1 Introduction

1.1 About This Document

This disaster recovery (DR) plan contains proprietary information and data that is the exclusive property of **SAP Ariba Procurement and Business Network**. No part of this document may be reproduced, transmitted, stored in a retrieval system, translated into any language, or otherwise used in any form or by any means, electronic or mechanical, for any purpose, without the prior consent of **SAP Ariba Procurement and Business Network**.

Information contained in this document is subject to change without notice. Accordingly, **SAP Ariba Procurement and Business Network** disclaims any warranties, expressed or implied, with respect to the information contained in this document, and assumes no liability for damages incurred directly or indirectly from any error, omission, or discrepancy between any **SAP Ariba Procurement and Business Network** product or service and the information contained in this document.

Copyright 2025 SAP Ariba Procurement and Business Network. All rights reserved. Published by **SAP Ariba Procurement and Business Network**.

SAP Ariba Procurement and Business Network and respective logos are property of SAP. All brand names and product names used in this document are trade names, service marks, trademarks, or registered trademarks of their respective owners.

1.2 Sharing the DR Plan

This SAP document is classified as “internal only.” The **SAP Ariba Procurement and Business Network** Plan Owner, or a delegate, may authorize sharing a copy of this document with external parties under the following conditions:

1. The external party is an existing customer or a prospect under a Non-Disclosure Agreement (NDA), and a fully executed copy of the NDA is on file.
2. The **SAP Ariba Procurement and Business Network** Head of Security, Plan Owner as identified in Section 7.5, or a delegate, has approved the general release of this DR Plan for distribution to the external party.
3. All sensitive information — including but not limited to personally identifiable information (PII) and site logistics — has been redacted from the copy to be distributed.
4. The copy is in Adobe PDF format with standard document protection features enabled.

1.3 DR Plan Scope

Every SAP Cloud Line of Business (LoB) participates in disaster recovery planning (DRP) and business continuity planning (BCP). These are complementary activities, but not the same. The scope of DRP and BCP obligations are specified in customer contracts, but generally follow these lines:

1. **SAP Ariba Procurement and Business Network** maintains one or more disaster recovery plans (DR Plan) to protect production instances at data centers when the recovery

solution is more than restoration from backups. **SAP Ariba Procurement and Business Network** discloses to eligible customers, upon request annually, one or more DR Plans relating to the recovery of cloud products and services used by a customer.

2. **SAP Ariba Procurement and Business Network** maintains one or more business continuity plans (BC Plan) to protect the resources, buildings, and locations where there are dedicated SAP teams providing cloud services to customers. These are proprietary documents and not available to customers.

Note that in the event of a disaster, the first priority of SAP is to prevent the loss of life. Before any secondary measures are undertaken, SAP will ensure that all employees, and any other individuals on the organization's premises, are safe and secure. After all parties have been brought to safety and Crisis Management has been alerted, the next goal of SAP will be to enact the steps outlined in this plan to return to business-as-usual as quickly as possible.

Additionally, SAP is concerned about the health and well-being of planet Earth and, as such, maintains a SAP Global Environmental Policy. We are committed to reducing our impact on the environment in our operations, throughout our value chain, and with our solutions. If a business disruption could negatively impact the environment, please contact the Crisis Management organization."

This document provides an overview of the **SAP Ariba Procurement and Business Network** ***Disaster Recovery Plan***. It focuses on what is done before a *data center* disaster occurs (in terms of planning and testing), as well as during and after a disaster (in terms of response and cloud service resumption). More detailed documents are referenced within this plan but are not included here due to information security restrictions. This DR Plan does not cover:

- Step-by-step instructions for implementing ***Technical Recovery Procedures*** (TRP) for a specific data center. This information is captured in a variety of vital records maintained by data center management and/or the **SAP Ariba Procurement and Business Network** operations teams. Included are runbooks, knowledge bases, infrastructure technical manuals, run jobs, scripts and recommended actions.
- Orchestration of recovery activities across multiple cloud lines of business. This is addressed in the ***Disaster Recovery Management Handbook*** along with a flowchart and workbooks, which are maintained by Business Continuity Management (BCM).
- Formal communication with customers and other external stakeholders during a major outage. These guidelines are captured in the ***Intelligent Outage Communication Playbook,*** which is maintained by the Integrated Outage Communications (IOC) team.
- Business continuity plans, which address generic process resumption when SAP personnel or offices are threatened. SAP maintains ***Process Continuity Plans*** (PCP) for critical business processes.
- Business continuity plans for IT systems, shared services, and data center tools — which are the foundation for the SAP corporate business, as well as cloud service delivery. SAP creates ***IT Service Continuity Plans*** (ITSCM Plans) for critical systems and tools.
- Business continuity plans for handling local crises. As part of the physical security standard, SAP keeps a ***Crisis Management Handbook*** in addition to training manuals for

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

both regional representatives and local, onsite crisis management champions. These are maintained by the global Crisis Management Office.

These and many other documents are proprietary and not available to customers, but they form the basis for SOC and/or ISO certifications on which the customers may rely.

1.4 Content of DR Plans

The DR Plan incorporates industry good practices. It specifies the preventative and remedial actions for averting or minimizing any interruption of cloud services. This document also addresses restoration of connectivity and cloud services following a critical outage scenario.

A single customer may have multiple DR plans — one for each SAP Cloud LoB, cloud service, delivery model, or DR solution. All conform to the same, harmonized template, but some sections (like those containing a technical summary and service level agreements) can vary per customer contract. At a minimum, each of several DR Plans includes the following:

> *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, British Standards Institute***

- A complete list of cloud services provided by **SAP Ariba Procurement and Business Network**.
- The location of both the primary facility(ies) that SAP uses to provide cloud services, and the alternative facility(ies) used to continue the provision of the cloud services.
- A complete list of expected recovery timelines and priorities per cloud service.
- Disaster declaration criteria, which define the critical outage scenarios that will result in activation (invoking) of the DR Plan.
- A communication plan and steps to follow for notifying customers and SAP teams when an event triggering activation of the DR Plan occurs, and when deactivation of the DR Plan is initiated.
- DR Plan procedures and checklists, including:
  - DR Plan activation
  - Operational continuity
  - Escalation
  - Maintenance
  - Data recovery verification
  - Deactivation
  - Periodic testing for effectiveness.

1.5 Purpose and Key Objectives

A variety of catastrophic events could disable an entire data center for an extended period of time. The main purpose of this document is to describe the measures taken to protect SAP cloud customers when a production system is severely damaged or destroyed and unavailable for a prolonged period of time.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

This document also captures actions taken to fulfill the regulatory requirements associated with disaster recovery planning.

Cloud disaster recovery and resilience management practices are focused on (a) monitoring and identifying the risks for potential business disruption, (b) averting those risks if possible, (c) putting continuity plans into action if a disruption cannot be prevented, and (d) recovering normal business activities once the outage is resolved.

SAP Ariba Procurement and Business Network architects resilient cloud solutions and maintains this plan with **two objectives** in mind:

1. Continuing business operations through redundant infrastructure (e.g., availability sets) or from an alternate site (such as an availability zone or in-metro data center) to contain the impact of outages.
2. Efficiently recovering on-demand products at a secondary site (either in-metro or across-region) following a disaster declaration.

To address the first objective, a global cloud resilience strategy captures the various methods for providing resilience and failover during a disruptive incident. A variety of resilience methods serve to minimize the negative impact of unexpected outages; the exact mechanisms may vary according to the cloud service.

To satisfy the second objective, the Business Continuity Management Standard and related procedural documents establish the appropriate response to severe and unexpected events that impact the security and availability of cloud products. For catastrophic events in which the restoration of cloud services at the primary facility is not feasible — at least not in a commercially reasonable timeframe — SAP establishes, governs, and supports disaster recovery at an alternate facility with its documented strategies.

A DR Plan details the recovery service level agreements that are defined, at a minimum, by customer contract. The objectives provide the requirements for the management of operations and in-house or subcontractor services.

1.6 SAP DR Plan Benefits

SAP Ariba Procurement and Business Network has established a business environment designed to deliver quality services to its customers by:

- Adopting standardized, repeatable processes.
- Hiring and developing highly-skilled staff.
- Establishing an extensive customer management infrastructure.

SAP Ariba Procurement and Business Network implements disaster recovery processes to minimize the impact of an incident — such as those caused by natural disasters, accidents, equipment failures, or deliberate actions — through a combination of preventative and recovery controls.

SAP Ariba Procurement and Business Network leverages a combination of proven techniques such as ITIL process management and leading industry practices from SOC, ISO, BCI, NIST, and others. This approach also includes documented policies and procedures for managing service-related processes,

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

including Change Management, Security Management, Availability Management, Service Level Management, and Incident Management. To view certifications specifically for **SAP Ariba Procurement and Business Network**, visit the SAP Trust Center.

The Business Continuity Management Standard is one component of the SAP Global Security Policy — which encompasses disaster recovery and resilience management. This standard describes the fundamentals, framework, tasks, and responsibilities for BCM according to ISO 22301:2019 and ISO 27031:2011.

The DR Plan is written in accordance with the Integrated Information Security Management System Framework (IISMS based on ISO 27001) used for SAP Business Units — also known as SAP Lines of Business.

1.7 Business Continuity Planning Lifecycle

SAP Ariba Procurement and Business Network considers continuity planning to be an iterative process: ongoing review is required in order to assess a variety of risks and appropriate responses. Consistent with good practices, this DR Plan is comprised of five reiterative sections — highlighting the phases in the planning lifecycle.

1. The **analysis phase** lays the foundation for the DR solution — consisting of business impact analysis (BIA), threat and risk analysis (TRA), and critical recovery requirements. This section also identifies probable scenarios and provides a definition of disaster and the declaration criteria.
2. The **solution design phase** identifies the most cost-effective recovery solution that meets the 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 describes resilience planning and the DR solution specifications.
3. The **implementation phase** primarily captures the technical requirements that dictate the DR solution provided by **SAP Ariba Procurement and Business Network**. The solution design incorporates onsite risk mitigation with data center resilience and restoration from backups as a first line of defense. This section clearly describes the active / passive DR model, includes a technical summary with basic diagrams, and details recovery methodology with high-level failover steps. The second part of the phase discloses the six stages of disaster recovery management following a disruption and a typical recovery timeline.
4. The purpose of the **testing phase** is to achieve organizational acceptance by obtaining stakeholder buy-in. Exercising the plan ensures that the DR 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 DR Plan and related documents — collectively known as the DR manual — are refreshed at least annually with current information (e.g., contact data,

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

runbook changes, test plan updates, communication templates, handbook revisions, etc.). Issues found during the maintenance phase often must be reintroduced to the analysis and/or testing phase.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

2 Analysis Phase

The analysis phase lays the foundation for the DR solution — consisting of business impact analysis (BIA), threat and risk analysis (TRA), and critical recovery requirements. This section also identifies probable scenarios and provides a definition of disaster and the declaration criteria.

2.1 Business Impact Analysis

A Business impact analysis (BIA) differentiates critical / urgent and non-critical / non-urgent organization activities. Critical functions are those for which 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 changes in a spreadsheet for one business day and enter them "en masse" with a script when cloud services have been returned?

The table below lists the application products and cloud services that support critical business processes. Other important, but non-critical business functions, listed as non-mission critical are a secondary consideration, and restoration is performed only as resources become available.

Application Product or Cloud Service	BIA Category	DR Recovery Point Objective (RPO)	DR Recovery Time Objective (RTO)
SAP Ariba Buying	Mission Critical	5 Mins	4 hours
SAP Ariba Catalog	Mission Critical	5 Mins	4 hours
SAP Ariba Contracts	Mission Critical	5 Mins	4 hours
SAP Business Network Ariba Network/Commerce Automation - Buy-side - Sell-side - Digital Supplier Network	Mission Critical	5 Mins	4 hours
SAP Ariba Sourcing	Mission Critical	5 Mins	4 hours
SAP Spend Analysis	Mission Critical	5 Mins	4 hours

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

SAP Ariba Supplier Inform. & Perform. Mgmt	Mission Critical	5 Mins	4 hours
SAP Ariba Supplier Lifecycle & Perform. Mgmt	Mission Critical	5 Mins	4 hours
SAP Ariba Supplier Risk	Mission Critical	5 Mins	4 hours
SAP Ariba Payables	Mission Critical	5 Mins	4 hours
SAP Ariba Supply Chain Collaboration	Mission Critical	5 Mins	4 hours
SAP Ariba Invoice Management	Mission Critical	5 Mins	4 hours
SAP Ariba Central Invoice Management	Mission Critical	24 hours	336 hours
SAP Ariba Category Management	Mission Critical	Best Effort	168 hours
SAP Ariba Buying, Base Edition	Less Critical	Best Effort	Best Effort
SAP Ariba Procurement Mobile Android	Less Critical	5 Mins	4 hours
SAP Ariba Procurement Mobile IOS	Less Critical	5 Mins	4 hours

2.2 Threat and Risk Analysis

This plan only covers the disaster recovery options for **SAP Ariba Procurement and Business Network** during an unexpected event that 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 for a lengthy period of time. **SAP Ariba Procurement and Business Network** maintains a list of 30 recognizable threats to a data center. These have been classified as (1) a natural catastrophe or (2) a man-made incident. An analysis is routinely performed for each production site to rate the probability and severity of these threats. These ratings are essential for the risk assessment.

Threat	Class	Type	Description
Earthquake	NC	Natural	Tectonic shifting of plates causing large scale damage
Extreme Heat	NC	Natural	Period of extreme warm weather

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

Threat	Class	Type	Description
Flood	NC	Natural	Inundation of water
Landslide	NC	Natural	Fast moving flow of land/material down an elevation
Sea Level Rise / Flooding	NC	Natural	Elevated sea level depth/flooding of coastal areas
Severe Storm	NC	Natural	Extreme weather event
Tsunami	NC	Natural	Massive water wave
Volcano	NC	Natural	Conical vent through which gas, steam, and lava flows
Wildfire	NC	Natural	Uncontrolled fire in woodland area
Labor Shortage/Strike	MMI	Human	Lack of qualified labor or purposeful refusal to work
Biological Incident	MMI	Human	Biological issue including pandemic
Biological Threats	MMI	Human	Threat of biological issue including pandemic
Bombing	MMI	Human	Threat of bomb blast or bomb detonation
Burglary	MMI	Human	Unlawful entry with intention to commit a crime
Civil Unrest/Riot	MMI	Human	Public uprising
Proximity to Target Orgs	MMI	Human	Operations in vicinity of targeted entities
Terrorism	MMI	Human	Violence/intimidations in pursuit of political gain
Theft	MMI	Information Security	Loss of data or work products due to unauthorized access
Unauthorized Physical Access	MMI	Information Security	Any physical access on the part of uncredentialed parties
Vandalism	MMI	Information Security	Purposeful destruction of IT systems, applications, or data
Airplane Crash	MMI	Infrastructure	Accident involving aircraft
Dam/Levee Failure	MMI	Infrastructure	Failure of water retention devices
Explosion, Gas, Steam, etc.	MMI	Infrastructure	Blast caused by gas or steam
Hazardous Materials Spill	MMI	Infrastructure	Loss of control of damaging substances
Infrastructure Failure	MMI	Infrastructure	Failure of civil engineered structures
Oil Spill	MMI	Infrastructure	Loss of control of oil
Radiological Incident	MMI	Infrastructure	Incident involving radioactive materials
Toxic Inhalation of Hazard	MMI	Infrastructure	Loss of control of any substance causing damage if inhaled
Hardware Failure	MMI	Technical	Breakdown of one or more devices involved in networking
HVAC Failure	MMI	Technical	Heating, ventilation, air conditioning breakdown

2.3 Risk Assessment

Risk assessments identify, quantify, and prioritize risks to the organization. Of most importance is the loss of one or more of the following three main components affecting business continuity: IT infrastructure, operational infrastructure, and employees.

Results of the study determine the appropriate action and priorities for (a) managing information security risks and (b) implementing controls 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 Ariba Procurement and Business Network** uses established criteria for determining whether or not risks can

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

be accepted. Risks may be accepted if, for example, it is assessed that the likelihood of occurrence is very low or the cost of treatment is not cost-effective for the company. Such decisions are recorded.

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

2.4 Business Impact and DR Scenarios

After identifying the applicable threats, impact scenarios are considered to support the development of a DR solution. Based on the risk assessment, existing data center management and/or technical recovery procedures are adjusted to counteract the impact and meet DR service level agreements. Additionally, DR test plans may provide greater detail for each identified threat and related impact scenarios. For security reasons, these assessments are proprietary and not available to customers.

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 and cloud services.
- The appropriate contractual commitments made to customers.
- The affected data centers hosting production instances.

A “priority one incident” (P1) does not necessarily transform into a disaster recovery event. For instance, it is out of scope to trigger the DR Plan because a cloud service for a handful of customers has been down 10 hours at the production site. This scenario does not qualify as a disaster incident. There are innumerable disaster recovery scenarios with many nuances. In short, a disaster is only declared when there is a loss of utilities and services. As long as the production site has power, network connectivity, and redundant infrastructure, a short-term outage will not be considered a disaster. For instance, a loss of Internet connectivity for a few hours would not necessarily take a data center offline for all customers, but the situation is still disruptive and likely a P1 incident, just not a disaster. On the other hand, a loss of electricity and backup power — taking a data center offline for more than 24 hours — could qualify as a disaster.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

2.5 Definition of Disaster

All SAP cloud lines of business conform to a standard definition of disaster. This has been expanded to include several characteristics as shown below.

a. A disaster is any unexpected catastrophic event causing widespread damage and/or a total loss of a data center for a significant amount of time (i.e., more than 24 hours)

b. The event includes physical damage or destruction to the SAP-managed data center or a computing environment (i.e., co-location in a third-party owned data center).

c. Disasters can be a natural catastrophe (NC) — such as floods, hurricanes, tornadoes, or earthquake.

d. A disaster can also be a man-made incident (MMI) — including hazardous material spills, infrastructure failure, bio-terrorism, or cyber-attack.

e. A disaster is typically not limited to one individual server, system, or landscape, but affects larger parts of an infrastructure. For example, fire damage incapacitates shared storage arrays supporting production of one or more cloud services, and replacement is not available in the short term.

f. A disaster may be declared when there is a loss of utilities, and cloud services will not return for a considerable period of time.

g. A disaster may also be declared if cloud customers cannot connect to the production data center (e.g., SAP network down, Internet unavailable, VPN not working) and repair will be lengthy.

h. As long as the production site has power, network connectivity, and redundant infrastructure, the event will not be considered a disaster. Note that a disaster recovery solution is no measure to overcome outages of isolated systems due to hardware or software incidents; failover to DR site is no replacement for high availability.

i. When an event takes down only one cloud service wholly or in part (i.e., the incident affects the productive use by a majority of customers or users of the cloud service hosted at same data center), a single cloud line of business may declare a disaster ahead of other organizations. For example, a fire destroys primary production and redundant servers for one cloud service in a contained area.

j. An in-region “disaster recovery site” is prepared to support production for a minimum of six months from handover.

k. After the disaster event has been resolved and the primary data center rebuilt, SAP solely makes the decision to reconstitute in the original production site.

l. Operations from the secondary site could last anywhere from a few days to many months. If necessary, failback to a different site within the same region is at sole discretion of SAP.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

2.6 Declaration Criteria

Every major outage has the *potential* to become a crisis — with catastrophic impact to customers. However, every lengthy outage is NOT a disaster. To help make the distinction between an outage and a disaster, a tiered list of criteria has been designed. A questionnaire with fifteen "yes/no" questions is used by the incident SWAT team lead. These are answered by each cloud line of business that hosts production instances at the damaged site.

SAP DISASTER DECLARATION CRITERIA
DATA CENTER 1. Has the event caused a total loss of a data center? Or, is total loss imminent? 2. Is there a loss of utilities, including backup power? Or is electricity expected to out shortly? 3. Will the entire SAP data center (or third-party colocation site) be out of commission for more than 24 hours?
SHARED INFRASTRUCTURE 4. Have Cloud customers lost network connectivity to production site? Will outage continue for more than 24 hours? 5. Are shared IT components unrecoverable for 24+ hours at primary site, but immediately available at DR site? 6. Is storage or other platform infrastructure inoperable? Can these not be replaced / repaired in less than 24 hours?
CLOUD SERVICES 7. Is production for one or more Cloud LoBs impacted by the event? 8. Will dependencies across two or more Cloud LoBs remain intact during failover? 9. Can a single LoB failover all services earlier than other Cloud LoBs with little or no risk? 10. Will recovery using normal measures at the production site (i.e., restart, restore, repair) take significantly longer (greater than 120%) than failover to secondary site? 11. Are all customers of the Cloud LoB recoverable at the secondary site with failover procedures (i.e., zero customers with just restoration from backups as the only recovery method)?
RECONSTITUTION AND FAILBACK 12. Are the negative side effects of a DR failover (i.e., disruption of landscape, potential loss of data, business downtime for later failback) worth the potential for a shorter business downtime? 13. Is there sufficient storage and compute capacity at DR site for failover? 14. Are operations personnel prepared to support production at DR site for a minimum of six months from failover, if necessary? 15. After disaster event is resolved and primary data center rebuilt, can a failback be performed?

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

A “no” answer to any of these criteria may impede the declaration of a disaster — keeping the event classified as a crisis.

Not all questions are of equal value. When considering a declaration, the DATA CENTER criteria bear more weight than the RECONSTITUTION AND FAILBACK category.

Multiple “no’s” across all four categories of criteria make it far less likely to be a disaster. Thus, the crisis outage would not warrant a large-scale migration to a secondary site.

Nevertheless, to limit the impact of a lengthy outage, each Cloud LoB can make an independent business decision and accept the risk of failing over all or part of a customer population. In other words, a cloud LoB doesn’t have to wait for a disaster declaration before moving to an alternate location. In fact, some cloud services have automated failover — moving to a secondary site within minutes of the disruption without manual intervention and long before a disaster might be declared.

If qualified as a data center-wide disaster, the Global Head of Business Continuity Management makes the final recommendation and then collaborates with the Mission Control Center to engage one of three persons to officially make the declaration and invoke the various Cloud LoB DR Plans:

- C-Level Executive on Duty.
- Chief Security Officer (CSO).
- A Level 1 Manager for Global Cloud Services (GCS).

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

3 Solution Design Phase

The solution design phase identifies the most cost-effective recovery solution that meets the 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 describes resilience planning and the DR solution specifications.

3.1 Resilience Planning

Resilience is defined as the ability of a system or application to handle and recover from failures gracefully, without violating service level agreements for availability and disaster recovery. As expressed in the previous phase, threats and challenges to service can range from simple misconfiguration to large scale natural disasters to targeted site attacks. Therefore, comprehensive resilience planning is a necessity.

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

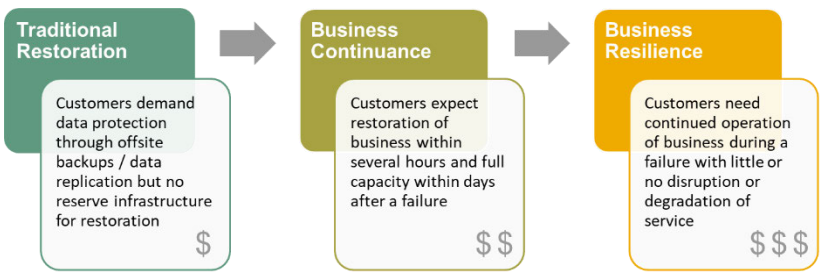
High availability can be described in two main areas:

- **System Availability:** A system is available when it can respond to a client request.
- **Data Durability**: Data durability is provided independent of system availability and provides guarantees for data being stored in the system without loss or corruption. This means that even if the SAP system is down (e.g., network outage), the data is still protected.

From a solution point of view, resilience can be achieved by:

- Minimizing single points of failure and building in elasticity.
- Quick diagnosis of issues and recovery from errors.
- Fast failover to a secondary site, and an ability to failback to the original primary data center.

So, whether recovering from a disaster or mitigating the effects of an outage or simply performing maintenance, movement across paired data centers is a key means to create resilience. Exactly how high availability is achieved depends, in large part, on the specific Cloud Line of Business and the SAP products / services being protected.



© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

3.2 DR Solution Specifications

Resilience goals may vary by service, since resilience comes at a cost, and thus service design must balance constraints including customer tolerance for service outages or data loss, competitive pressure, and cost/price sensitivity. All SAP disaster recovery solutions are designed to meet the desired resilience characteristics of the service being offered. The outputs from the analysis phase — along with the customer contracts — prescribe the recovery requirements for each critical function.

The chart below summarizes the specifications for the **SAP Ariba Procurement and Business Network** disaster recovery solution(s).

DR Option	Current Enhanced or Premium DR Option
Event Scenarios	Entire production data center is incapacitated and offline due to natural catastrophe or man-made incident
Resilience Type	Business Continuance
Short Service Description	*DR Solution is Active/Passive paired sites:* Continuous, asynchronous or synchronous data replication to alternate facility. Failover to a fully functional data center with an in-place network, security, reserved storage, and a complement of basic replacement servers.
Offsite Backups	In addition to standard offsite backups, enhanced DR includes near real-time, asynchronous data replication, which minimizes data loss.
RPO	5 mins
RTO	4 hours
MTD	
Written Plan Document	No customer-specific written DR plan; only Global DR solution available upon request
Annual DR Test	Only SOC report evidence of annual DR test
In-Scope	Applies to production environments for applications supporting only critical business functions per customer contract
Annual Recurring Fee	Included with customer's subscription; no additional charges

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

4 Implementation Phase

The implementation phase primarily captures the technical requirements that dictate the DR solution provided by **SAP Ariba Procurement and Business Network**. The solution design incorporates on-premise risk mitigation with data center resilience and restoration from backups as a first line of defense. This section clearly describes the active / passive DR model, includes a technical summary with basic diagrams, and details recovery methodology with high-level failover steps. The second part of the phase discloses the six stages of disaster recovery management following a disruption and a typical recovery timeline.

4.1 Data Center Resilience

SAP customers expect uncompromising information security for their cloud environments. **SAP Ariba Procurement and Business Network** works continuously to strengthen and improve security features in all of our software and service offerings, as well as protect our own company and assets. Ironclad SAP-operated data centers -- and facilities run by qualified third parties -- have instituted measures to prevent or mitigate crisis outages.

4.1.1 Data Center Assignments

A fully-functioning DR site with reserved infrastructure is paired with select production data centers. For SAP owned and operated production sites, the region and secondary data centers are shown in the table below:

Global Region	Primary Data Center	Secondary / DR Data Center
NAMER	Council Bluffs (GCP- US1)	Las Vegas (GCP- US2)
EMEA	Frankfurt (GCP-EU1)	Eemshaven (GCP-EU2)
China	Shanghai (CCEE- CN1)	Shanghai (CCEE- CN2)
Mena UAE	Dubai (CCEE-UAE1)	Dubai (CCEE- UAE2)
MENA KSA	Riyadh (CCEE-KSA1)	Dammam (CCEE-KSA2)
Australia	Sydney (GCP-AUS1)	Sydney (GCP- AUS2)
Japan	Tokyo (GCP-JPN1)	Osaka (GCP- JPN2)

The above table reflects traditional, static failover pairs. Hyperscalers provide a wide range of services such as serverless technologies (e.g., Google Cloud Platform SQL, Google Cloud Platform Functions, or Google Kubernetes Engine) and datastores. Data can be stored in a single location (e.g., Frankfurt 1, 2 or 3), in “multi-zones” (e.g., across all 3 Frankfurt zones) or regional (e.g., within Europe). Therefore, hyperscalers generally do not document HA/DR sites in the traditional sense.

4.1.2 Location/Access of Customer Data

Independent of the situation (owned data center or co-location) the same or very similar procedures, standards, etc. do apply. SAP does not transfer customer data outside the contractually defined geographic area unless the customer has been notified or such transfer is a feature of the solution. Furthermore, SAP does not share customer data with unauthorized third parties. The co-location provider is solely responsible for the operational running of the physical datacenter facilities.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

4.1.3 Data Center Baselines

SAP Cloud uses SAP-owned data centers in combination with rented private space (co-location) at external data center providers (co-location provider) as well as Cloud providers around the world. This enables a global reach and fast growth into various countries. SAP only uses co-location or Cloud providers that can fulfill the minimum SAP data center service availability (at least SAP data center level III) and baseline physical security measures. Additionally, SAP demands industry standard attestations and certifications, including ISO 27001, SOC, and C5. These support the external Cloud business and show our customers secure, reliable operations and a strong control framework for our co-location and Cloud providers.

According to the Cloud Security Framework (CSF), all production data centers are TIA / EIA 942 Tier III, ISO 27001 certified facilities, or better (reference the chart below). Reflecting ANSI/TIA-942 and the Uptime Institute Data Center tier definitions, SAP has defined the following SAP data center level and corresponding requirements regarding the power supply, cooling, incident response times or network connectivity. Cloud production environments need to be operated at least in an SAP Data Center Level III, III+ or IV classified data center to meet the physical security and operational compliance requirements. SAP tracks the corresponding level and available certifications. Additionally, SAP and/or third-party audits validate the security measures outlined in this paper.

Minimum availability requirements	Level I	Level II	Level III	Level III+	Level IV
Stand-alone Data Center building necessary	no	no	no	yes	yes
Amount of external electrical power suppliers	1	1	1	1	2
Amount of transformers to power the Data Center	n	n	n+1	n+1	2n
Uninterruptible power supply (UPS) Battery System necessary	no	yes	yes	yes	yes
Minutes UPS must provide power	0	5	>10	>10	>10
Amount of UPS Systems necessary	n	n	n+1	n+1	2n
(Diesel-) Generators needed	no	no	yes	yes	yes
Amount of cooling systems needed	n	n	n+1	n+1	2n
Server cooling is independent from an office Air Conditioning (AC)	no	no	yes	yes	yes
Fire detection system needs to be installed	yes	yes	yes	yes	yes
Fire extinguishing system must be installed	no	yes	yes	yes	yes
On-site response time of Data Center personnel	<48h	<8h	<1h	<1h	<1h
Available Wide Area Network (WAN) connection lines	1	n+1	n+1	n+1	2n
Available Local Area Network (LAN) connection lines	n	n+1	n+1	2n	2n

Legend:

'1' = Exactly one item or component of this type is needed; no redundancy in place;

'n' = No redundancy in place; no spare or standby component available; all components (n) are in use and if one fails, the whole system (power, cooling, network) goes down;

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

‘n+1’ = If 'n' items of equipment are required for something to work, there would be one additional spare item. If any one item of equipment breaks down, everything can still work as intended;

‘2n‘ = There are twice as many items as needed. Therefore ‘n’ items can fail without interruption.

To achieve these availability requirements, SAP data center core components (e.g., power supply, batteries, diesel generators and air conditioning) are maintained and tested on a regular basis based on critical supplier recommendations and applicable laws.

Furthermore, the fabric of the data center building is designed to prevent the ingress of rain and to facilitate that surface water is routed out of the building. A lightning protection system is installed to prevent or lessen lightning strike damage to the Cloud IT equipment.

The data center security measures are implemented and regularly audited by third-party public auditors via compliance and certification audits. In addition, depending on third-party contracts with Cloud Service Providers, SAP may also perform on-site reviews to validate and check the security implementation.

4.2 Restoration from Backups

The following reflects the standard SAP Ariba Procurement and Business Network policies regarding backups and traditional restoration:

SAP Ariba Procurement and Business Network’s production backups are made to disk. Production data is stored in databases on high-availability storage disk-based systems in the primary datacenter and replicated to partner databases located in secondary data centers. Backup failures are captured within 5 minutes by a monitoring system.

Procedures, tests and reports are produced to confirm the usability of the backups and an annual validation of restoration is performed.

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

- Full databases are backed up once per week, differential backup once per week, and incremental backups on remaining 5 days.
- Postgress databases are backed up daily, weekly and monthly cycles into NFS mounted disk storage.
- Application files are stored on highly-available NFS storage in the primary data center and replicated to the partner datacenter in near real-time.
- Storage-based snapshots are performed four times per day in each datacenter.
- All encrypted using an AES256 encryption standard.

To summarize, three copies of customer data are maintained: Production, Primary Storage Backup, and Remote Secondary Storage Backup.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

4.3 Attributes of an Enhanced DR Solution

At **SAP Ariba Procurement and Business Network**, business continuance and business resilience is provided through an enhanced disaster recovery solution with the following design attributes:

1. An active / passive "standby" design exists today. Production for a customer is solely "run" at site A or site B.
2. Failover for all customers with enhanced DR is possible from a primary production site to a secondary location.
3. A DR solution for products / services is architected to meet contract requirements. All cloud LoB dependencies are accounted for.
4. A fully-functioning DR site with reserved infrastructure is paired with select production data centers currently in use.
5. DR site or auto-generation scripts are routinely updated to match primary site (e.g., code releases, compute capacity, storage upgrades, etc.).
6. Asynchronous replication between production and DR sites is on a store-and-forward basis (i.e., every 15 minutes or better).
7. Data replication feature has been implemented for failback from a secondary location to the repaired primary site or accomplished by two or more active/active availability zones.
8. Current enhanced DR offering includes the following SLAs: **5 minutes** RPO, **4 hours** RTO and **99.7%** or better Service Availability.
9. A formal disaster recovery plan exists and is updated at least annually. A plan owner has been identified.
10. A disaster recovery test is performed at least once a year and DR Test Plan is revised as needed based on the results. Note: A customer may elect to forego a DR test with a written request for an exception.
11. Technical recovery procedures are documented in runbooks, shared with Operations personnel, and made readily accessible.
12. SOC and/or ISO certification has been achieved or is planned for the near future.

4.4 Delivery Methods for Enhanced DR

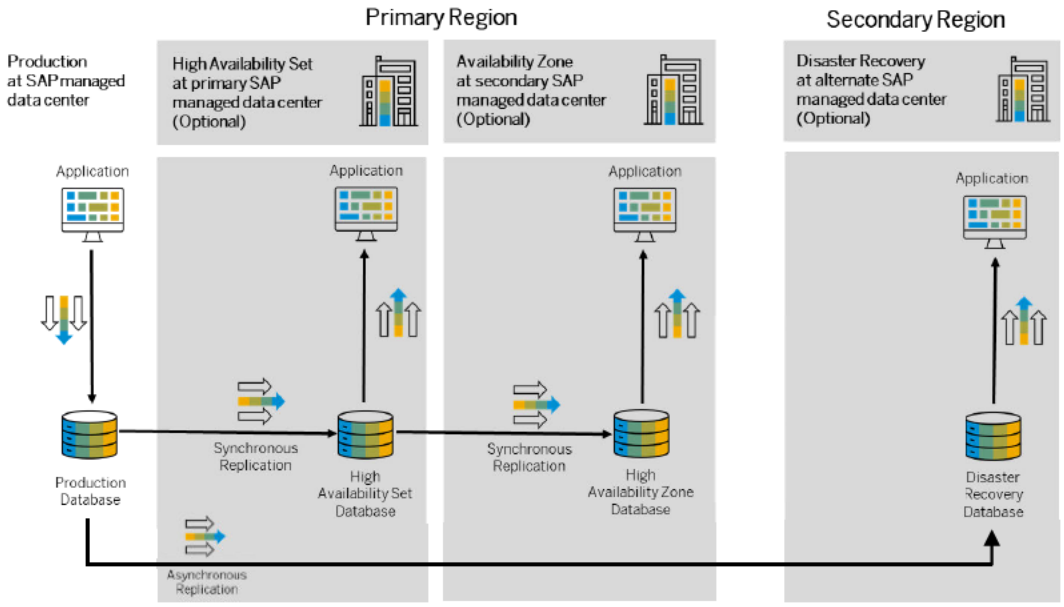
The chosen approach for SAP Cloud Operations and the DR Plan is an active/passive data center model. There are three methods of delivery:

1. **SAP Legacy Delivery Method:** Production is at an SAP-managed data center with failover to either an availability zone or disaster recovery site at an alternate data center also managed by SAP. These locations can be SAP-owned facilities or a colocation cage at a data center operated by a third-party.
2. **Hybrid Delivery Method:** Again, production is at an SAP-managed data center, but failover is to a site operated by a hyperscaler (e.g., Amazon Web Services, Microsoft Azure, Google Cloud Platform).

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

3. **Hyperscaler Delivery Method:** Both production and secondary sites are hosted and operated by a hyperscaler.

This DR Plan is exclusively for the SAP Legacy Delivery Method presented by **SAP Ariba Procurement and Business Network**. Below is a simple diagram.



The amount of resilience is determined by the product offering and/or a customer's contract terms. For example, the diagram above represents the overall architecture of both the SAP Business Technology Platform high availability (HA) and the enhanced disaster recovery (DR) setup that may be purchased by a customer. During a major outage, failover may occur to the availability zone. Enhanced DR is based on a mirrored customer landscape in a remote data center with asynchronous data replication between them. In the case of a disaster, the application and database in the secondary region become active and replace the primary setup.

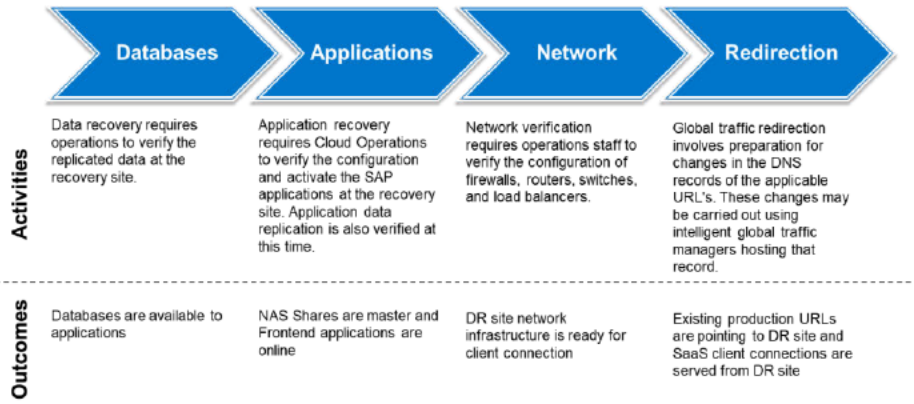
© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

Key features of the SAP Legacy Delivery Method:

1. Production for a customer is only "run" at a primary site, secondary data center with AZ, or alternate DR location.
2. Application architecture (for a system / product) is designed for single-site use only. Transaction load is not balanced across two sites.
3. Replication for structured data between primary and DR sites is on a "store-and-forward" basis in 15 minute intervals or less.
4. Failover between a Production site and a secondary data center is manually initiated with some level of automation in the recovery procedures.
5. Failover is designed to be seamless and transparent. A single user may not know which data center is being used at a given time.
6. Hardware infrastructure may be identical between the two data centers (or nearly so depending on product design and contract terms).

4.5 Enhanced DR Failover Actions

Being able to failover successfully is the core of the DR solution. Following the activation of the failover plan, the recovery process includes four sections:



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

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

4.6 Stages of DR Management

A clearly-defined action plan is required to enable organization continuity during 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.

STAGES 1 THRU 6	ACTION
1. Emergency Authorization and Declaration	1.1 Engaging BCM
	1.2 Handling the Emergency
	1.3 Assessing the Situation
	1.4 Determining Potential Impact of the Emergency
	1.5 Declaring a Disaster
2. Disaster Management	2.1 Establishing a Response and Recovery Center
	2.2 Mobilizing the Disaster Recovery Team
	2.3 Maintaining the Event Log
	2.4 Recording Project Management Activities
3. Communication Plan Activation	3.1 Kicking Off Management Meetings
	3.2 Opening a Phone Bridge
	3.3 Reviewing and Documenting Status
	3.4 Communicating with the Press
	3.5 Communicating with Customers
4. Failover Plan Execution	4.1 Implementing the Failover Steps
	4.2 Performing Functionality Health Checks
5. System Access and Service Availability	5.1 Granting System Access by Priority Group
	5.2 Validating Service Availability
	5.3 Expanding Compute Capacity (if necessary)
	5.4 Declaring "Disaster Over"
	5.5 Producing a DR Process Report
6. Reconstitution (optional)	6.1 Reconstructing the Original Primary Site
	6.2 Initiating the Failback Steps

Throughout the initial 24 hours, activities 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.

Detailed procedures are captured in the ***Disaster Recovery Management Handbook*** along with a flowchart and workbooks, which are maintained by Business Continuity Management (BCM). These documents are proprietary and not available to customers.

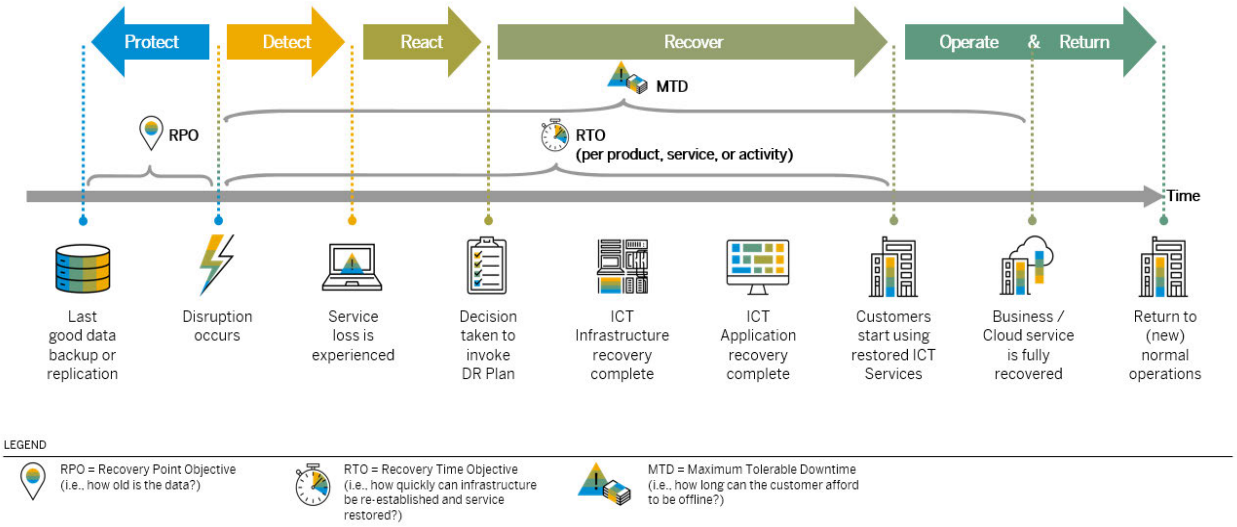
© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

4.7 High-Level Timeline

Although disaster scenarios can vary considerably, milestones for recovery are universal. The DR solution(s) designed by **SAP Ariba Procurement and Business Network** follows a common timeline, as shown below. The following service level agreements (SLAs) are key for **SAP Ariba Procurement and Business Network**:

- **RPO: Recovery Point Objective**
  (i.e., how old is the data?)
- **RTO: Recovery Time Objective**
  (i.e., how quickly can infrastructure be re-established, and service restored?)
- MTD: Maximum Tolerable Downtime
  (i.e., how long can the customer afford to be offline, or functioning at less than 100% capacity?)

Many countries and regulatory organizations have diagrams explaining these SLAs. The timeline shown here serves as an SAP version. It is based on the Standard 100-4 of Business Continuity Management from the German BSI (Bundesamt für Sicherheit in der Informationstechnik translated as the Federal Office for Information Security).



© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

5 Testing Phase

The purpose of the testing phase is to achieve organizational acceptance by obtaining stakeholder buy-in. Exercising the plan ensures that the DR 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.

5.1 Identify Type of DR Test

DR Test Plans cover key failure(s) and recovery scenarios related to the cloud services. Six different types of exercises can be employed by SAP Cloud LoBs when testing DR Plans:

1. **Desk Check.** A simple review of the completeness of DR Plan documentation. This test can be performed by a single employee with expert knowledge of the content that is covered by the respective DR Plan. Testing scenario and testing procedures are chosen and executed by the employee conducting the test.
2. **Table-Top Test.** A test carried out with upstream or downstream dependencies in a joint discussion. This test is held in informal settings, where DR Manager, DR Facilitator and other key members discuss their roles and responsibilities in a potential scenario where unexpected threats arise. There is no utilization of equipment or deployment of resources. The success of this test is determined by group participation in the identification of problem areas.
3. **Call-Tree Test.** The validation and verification of contact information maintained as part of the DR Plan. This effort may be manual or utilize an automated notification system.
4. **Simulation Test.** A test in which a disaster recovery situation is simulated, and members of the team are required to take necessary actions to respond to that situation. The goal is to review the adequacy of BCM strategies. This exercise is a test that minimally uses the “four-eyes-principles” where at least two employees conducting the test must have expert knowledge of the content of the DR Plan. Furthermore, there is utilization of equipment/infrastructure and deployment of resources. Technical test is based on an actual simulation and conducted either at a modular level focusing on a single cloud service, or at a functional level focusing on the recovery of a full cloud service and all its constituent parts.
5. **Full Integrated Test.** A test based on a realistic scenario spanning several, select cloud services, constituent parts, and dependencies, where the Cloud Service delivery or some its constituent parts are suspended until the test is completed. Participants may or may not realize the event is purely an exercise.
6. **Site-Wide Test.** A test that spans several, selected cloud services in collaboration with selected customers and third-party suppliers delivering services at the same site.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

5.2 Develop Scope and Plan Tests

SAP Ariba Procurement and Business Network will test specific features of its DR Plan (i.e., execute the DR Test Plans) for selected cloud services at least once per calendar year. If performing test types 5 or 6 above, **SAP Ariba Procurement and Business Network** will align the timing of DR tests with the customer's established, pre-determined maintenance windows. A regular test schedule is developed and communicated to minimize the risk to plan execution. Individual components of the plan are tested more frequently. The test schedule should indicate how and when each element of the DR Plan should be tested.

As a best practice and in preparation for the annual DR test, **SAP Ariba Procurement and Business Network** and independent third parties may choose to perform a desk check, a tabletop exercise, or a call-tree test at any time.

A Simulation Test may be performed in a lab environment specifically set up to simulate production failover to an alternate site, thereby continuing to provide cloud services to customers with minimal business interruption or risk during test execution. Recognize that this approach is not always feasible; some Cloud lines of business do not have infrastructure reserved for DR testing.

A Full Integrated Test of the DR involves a shutdown of primary and secondary delivery locations alternately. Depending on the DR solution(s), these tests could cause degradation or disruption of cloud services. For this reason, suspension of cloud services may be necessary within a pre-approved outage / maintenance window for such testing. If performing test types 5 or 6 above, a customer can opt-out of the annual DR test and accept the risk. The customer's decision is documented by the Cloud line of business and maintained for audit purposes.

If performing test types 5 or 6 above, in some cases participation by the customer may be necessary. It is the customer's responsibility and in their best interest to perform a joint DR test together with SAP. The request for a DR test is made by the customer through the engagement executive.

Where the recovery strategy is the same for multiple locations and/or multiple customers, **SAP Ariba Procurement and Business Network** is required to execute only a single data center DR test each year and rotate the failover location around the globe. Of course, **SAP Ariba Procurement and Business Network** may elect to perform additional tests at its discretion.

Restoration of backups is reviewed as part of the Availability portion of the twice-yearly SOC 2 audits. During the normal course of business, several IT Direct tickets are executed for various customers as proof that backups can be restored at the production site as well as verification that data is "recoverable, readable and not corrupt." Customers and sales prospects under a Non-Disclosure Agreement (NDA) may request copies of SOC 2 audit reports.

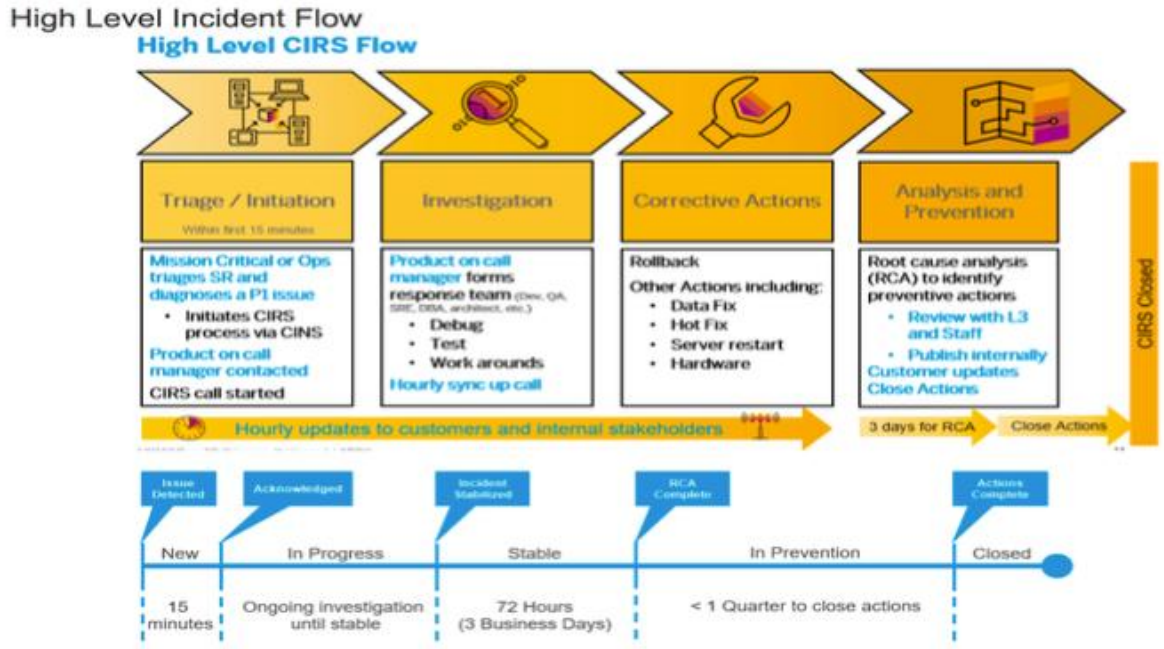
Ariba Operations maintains a 'Follow-the-Sun' model for supporting its production datacenter infrastructure and product performance.

- The Critical Incident Response System ensures stabilization of all service impacting events which have an adverse effect on the customer experience.

- The following workflow outlines the process used to detect, triage, isolate, stabilize, identify root cause and lessons learned in an effort to prevent a reoccurrence. Lessons learned are conducted 30 days after the close of an outage event.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

• Throughout the duration of a site wide incident, courtesy notification updates are sent to customers and the executive leadership teams.



5.3 Determine Test Participants

For all test types, Cloud Operations for **SAP Ariba Procurement and Business Network** assigns personnel from various teams to take part in the test. Teams may include, but may not be limited to, local or regional Disaster Recovery teams, Cloud Engineering, Production Operations, Infrastructure Services, and Database Management.

This paragraph is only applicable if performing test type 5 or 6 as described in section 5.1 above. According to some Cloud Service contracts, customers have the option to participate in a regional Cloud LoB DR exercise. In other cases, SAP **Ariba Procurement and Business Network** may ask for volunteer participation by an in-region customer. Tasks include developing use cases, verifying database content, and proving successful return of software functionality. Customer participation, or not, in each test is at the sole discretion of **SAP Ariba Procurement and Business Network.**

5.4 Execute the Test

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

1. Validate that the application functions properly and the files are populated in the DR environment as generally experienced in production.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

2. Confirm data changes made in Production immediately prior to the test are also seen in the DR instance.

Depending on the cloud service, these tasks cannot be performed by some **SAP Ariba Procurement and Business Network** personnel due to data privacy restrictions. Under these circumstances, a customer participant may be required for this step if test type is 5 or 6.

Although this may be an inconvenience to customer participants, DR testing is often performed after standard business hours and usually during the regularly-scheduled maintenance window on weekends. This approach controls risk and reduces the interruption to the customer's business.

5.5 Document the Test

Cloud Operations management will review the outcome of the test, including how the team performed according to schedule and whether there were any errors. Suggestions include documentation updates and recommendations for future drills.

SAP Ariba Procurement and Business Network management encourages test participants and customer representatives to provide feedback on tests and results in order to continually improve the process. The DR Plan may incorporate input from customers at the discretion of **SAP Ariba Procurement and Business Network**.

Upon request and according to contract, **SAP Ariba Procurement and Business Network** may provide a relevant (but not necessarily customer-specific) DR Test Report as soon as reasonably practical after performing the test. Where applicable, **SAP Ariba Procurement and Business Network** has a standard template for all disaster recovery tests. Content is customized as needed to fully capture test details.

The report includes, at a minimum, the following:

1. Predefined scope and testing approach, and expected results
2. Date and time
3. Participants, with redacted Personal Identifiable Information
4. Results, and comparisons against expected results
5. Issues / failures observed
6. Corrective actions.

Coincident with test execution, the DR Plan will be reviewed at least annually, and the review will be documented by updating the revision history.

5.6 Prepare for Retesting

If testing of the DR Plan results in any identified issues or failure, **SAP Ariba Procurement and Business Network** implements a remediation plan to address such issues as soon as is reasonably practical.

In some Cloud LoBs, the remediation is proven successful through the standard quality assurance procedure and the next failover to the secondary site.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

If necessary, in other Cloud LoBs scheduling of retests is at the sole discretion of **SAP Ariba Procurement and Business Network**. Target dates for regional tests may shift out if resources are redirected to production work and/or peak season support. If risk is low, retesting may be rolled into the next regularly-scheduled annual exercise. Evidence will be provided proving success consistent with the original test scope.

If any changes need to be introduced to Production during or after the annual test, these actions will be vetted through the proper / required Change Control processes, and all necessary approvals will be obtained and documented for audit purposes.

5.7 Train the DR Team

SAP Ariba Procurement and Business Network provides support personnel with sufficient training, information, and knowledge to manage the recovery effectively. All personnel who will participate in disaster recovery activities will be familiarized with the DR Plan. A training session is held prior to each annual DR test and includes a discussion of the key components of the plan including:

1. Purpose and goals
2. Definition of disaster
3. Disaster Declaration Criteria
4. DR Team structure and other players
5. DR solution, including Service Level Agreements
6. Plan administration

The annual test also serves as a review of the DR Plan changes, as well as a training session for the various teams to ensure that everyone understands roles and responsibilities.

It is the responsibility of the DR Plan Owner, or his designee, to review the document with newly-hired employees who will be involved in the execution. This includes, but is not limited to, staff from Cloud Engineering, Application Support, Database Management, and Information Technology.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

6 Maintenance Phase

The maintenance phase dictates that the DR Plan and related documents — collectively known as the DR manual — are refreshed at least annually with current information (e.g., contact data, runbook changes, test plan updates, communication templates, handbook revisions, etc.). Issues found during the maintenance phase often must be reintroduced to the analysis and/or testing phase.

The annual maintenance cycle is broken down into three periodic activities:

1. Confirmation of the DR Plan content, including rollout to staff for awareness and specific training for critical individuals.
2. Testing and verification of the technical solutions established for recovery operations in, at a minimum, a single region.
3. Validation of organization recovery procedures, including the communication plan.

6.1 Organizational Changes Affecting Plan

The DR Plan 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; therefore, glossaries need to be kept current. Some types of organizational changes that should be identified and updated in the manual include:

- Transfers, promotions, and terminations of personnel
- SAP organizational structure
- Telephone numbers and addresses
- SAP stakeholder distribution lists
- Business strategy
- Acquisitions or mergers
- Legislative or regulatory requirements
- Contractual obligations
- Third-party providers and contact information
- Critical suppliers and contact information
- Threats or risks

6.2 Technical Requirements on Standby

Specialized technical resources must be maintained. For instance, patches applied to the production site need to be routinely installed at the DR site or inserted into scripts in anticipation of a disaster event. Similarly, capacity increases at the production site should be mirrored at the secondary site in

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

accordance with the DR solution and/or contracts. Following are examples of events that may trigger unscheduled maintenance to the DR Plan, test plan, and/or operations runbooks:

- Location, facility, or production equipment additions, changes, or upgrades
- Virus definition distributions
- Application security and service patch distributions
- Implementation of Operating Systems upgrade levels or patches
- Hardware operability changes
- Application operability changes
- New application systems deployments
- Discontinuance or retirement of applications
- Data verifications
- Design changes to production application database
- WAN/LAN network design modifications
- Backup or failover procedure changes
- Changes in offsite storage facilities and methods of cycling files and materials
- Storage capacity enhancements
- Compute capacity enhancements

6.3 Verifying Recovery Procedures

As work processes change, previous recovery procedures may no longer be suitable. Verification checks include the following questions:

- Are all work processes for critical functions documented?
- Have the IT systems used for critical functions changed?
- Are the documented work checklists in the handbook still meaningful and accurate?
- Are the templates and talking points still useful for communicating with stakeholders?
- Do the documented work processes for performing recovery tasks and the restoration of the supporting infrastructure allow staff to recover within the predetermined recovery time objective?
- Are backups and/or data replication jobs occurring routinely so that the recovery point objective can be met?

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

6.4 Provisioning and Updates

Where applicable, a DR Plan will be provided by **SAP Ariba Procurement and Business Network** and shared with a customer according to the following timescales:

1. Within ninety (90) days of the provisioning of a new production environment and go-live use of a Cloud Service.
2. In the event of a material change to the Cloud Services under any Service Agreement or Catalogs, within ninety (90) days of a customer's reasonable written request.

A formal written plan and any updates according to the above timeframes is considered material to the provision of disaster recovery services.

Again, per contract, **SAP Ariba Procurement and Business Network** will make the current DR Plan, DR Test Plans, and related documentation, procedures, and checklists available to the customer promptly upon written request. To avoid dissemination of proprietary information, the level of detail provided in the documentation is at the sole discretion of SAP.

6.5 DR Plan Maintenance Responsibilities

Overall accountability for the **SAP Ariba Procurement and Business Network** disaster recovery program lies with the Chief Information Officer or a delegate. Governance and oversight are provided by SAP Global Security under the direction of the Chief Security Officer and the Global Head of Business Continuity Management.

This document is maintained by the DR Plan Owner, who 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.). Reviews and changes are recorded in the Revision History. Check the last page of this document for the most recent change authorship and approval.

Employees from various parts of **SAP Ariba Procurement and Business Network** have roles and responsibilities within the DR program framework and provide input to this document. As necessary, Engineering, Cloud Operations and Global Cloud Services are primarily responsible for updates to technical procedures, architecture, and other components of the DR solution. All changes to the plan and related material will be performed in accordance with the governing ISMS policies.

DR Plans, test reports, operations runbooks, and other relevant documentation are archived in an SAP repository (like a Work Zone, SharePoint, or Wiki site) and also stored in an offsite ServiceNow tool for future reference.

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

7 Quick Reference

7.1 Common Acronyms

Acronym	Stands for…
AKA	Also Known As
ANSI	American National Standards Institute
AZ	Availability Zone
B & R	Backup and Restore
BC	Business Continuity
BCI	Business Continuity Institute
BCM	Business Continuity Management
BCP	Business Continuity Planning
BIA	Business Impact Analysis
BRT	Business Recovery Team
BSI	Bundesamt für Sicherheit in der Informationstechnik -- translated as the Federal Office for Information Security
CIO	Chief Information Officer
COTS	Commercial Off the Shelf Software
CSF	Cloud Security Framework
CSO	Chief Security Officer
DR	Disaster Recovery
DRP	Disaster Recovery Planning
DRT	Disaster Recovery Team
GCS	Global Cloud Services
IaaS	Infrastructure as a Service
HA	High Availability
IaaS	Information as a Service Provider
IISMS	Integrated Information Security Management System
ISO	International Standards Organization
ITSCM	Information Technology Service Continuity Management
LoB	Line of Business
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
P1	Priority One Incident
PCP	Process Continuity Plan

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

Acronym	Stands for…
RACI	Responsible, Accountable, Consulted and Informed Chart
RCap	Restore 100% Capacity
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA	Service Availability
SaaS	Software as a Service
SGS	SAP Global Security
SLA	Service Level Agreement
SOC	Service Organization Control
TRA	Threat and Risk Analysis
TRP	Technical Recovery Procedures
UPS	Uninterruptible Power Supplies

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

7.2 Customer Contact List

The Customer Contact List is maintained in a separate system.

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

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

7.3 SAP Contact List

Personal Identifiable Information is not shared in this document. The SAP Contact List is maintained in a separate system.

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

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)

7.4 Document Information

Document Title		SAP Ariba Procurement and Business Network DR Plan
Document Creation Date		May 27, 2025
Security Classification		Internal
Document Purpose		For SAP Ariba Procurement and Business Network to respond to a disaster or other emergency that affects information systems and minimize the effect on the operation of the businesses running SAP Ariba Procurement and Business Network solutions.
Document Owner	**Department**	SAP Cloud Delivery Experience (CDX)
	Title	[redacted]
Review Cycle		Annually
Control Framework		SOC1, SOC2 ISO27001
Intended Audience		SAP Ariba Procurement and Business Network Operations team, SAP Ariba Procurement and Business Network Customer upon request
Approvers		[redacted]

7.5 Document Revision History

Date	Version	Description	Author
May 8, 2025	2025.1.0	Annual DR plan update in 2025	[redacted]

© 2025 SAP SE or an SAP affiliate company. All rights reserved. | CONFIDENTIAL (INTERNAL - Authorized for SAP Customers and Partners)