



ASC

Business Continuity and Disaster Recovery Plan

Document Owner:

Information Security Committee

Last Review Date:

June 2024

Purpose, scope and users

The purpose of the Business Continuity and Disaster Recovery Plan is to define precisely how Assessment Systems will recover its IT infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident. The objective of this Plan is to complete the recovery of IT infrastructure and IT services within the set recovery time objective (RTO).

This Plan includes all resources and processes necessary for the recovery and covers all the information security aspects of business continuity management.

Users of this document are members of the top management and Security Committee members necessary for the recovery of this activity.

Assumptions

In order for this plan to work, the following conditions must be met:

- All the equipment, software and data are available
- At the moment of an incident, the Security Committee was notified – this is the starting point for this Disaster Recovery Plan

General information

Location of the alternative site / recovery strategy	All remote workforce so deciding on scenarios will most likely revolve around the ability to access AWS and manually configure the infrastructure.
Recovery time objective:	8 hours
Person responsible for Disaster Recovery Plan activation / means of activation:	Assessment Systems Executive Committee
People who must be notified about plan activation / who is responsible:	Assessment Systems Security Committee
Person responsible for deactivation of Disaster	Security Committee Leader

Recovery Plan / means of deactivation / criteria:	
Key tasks / obligations / SLAs that must be fulfilled and respective deadlines:	The ability to access Assessment Systems AWS environment, restore capability to customers, maintain operational capability and notify customers and partners of events during recovery/restore processes.
Minimum capacity that is required immediately after the disaster:	Service up and running non-clustered.
Period after which the normal operational level must be resumed:	8 hours

Roles and contact information

<i>Role in recovery</i>	<i>Name</i>	<i>Job title / organization / unit</i>	<i>Mobile phone</i>	<i>Landline phone</i>	<i>E-mail</i>
ASC	Nate Thompson	Vice President	651.2834327	651.383.4311	nate@assess.com
ASC	David Weiss	President	612-418-3312	651.625.0342	dweiss@assess.com
ASC	Jane Zirbes	Director of Operations		651.383.4311	jzirbes@assess.com
Softur	Mikolaj Buda	Tech Lead	+48 517915417		mbuda@assess.com
Softur	Lukasz Kregiel	Dev Ops Lead	+48 663 277 751		lkregiel@assess.com
Mundrisoft	Pramod Waikar	Lead Dev Ops	+91 95030 03183		pramodw@mundrisoft.com
Percona	Audrey Swagerty	Technical Account Manager	+1-702-406-0715	+1 888-401-3401. Ext: 031	audrey.swagerty@percona.com
OAC	Brandon Contons	IT Account Manager			bcontons@oactechnology.com
Mundrisoft	Hitesh Bedmutha	FastTest dev lead	+91-8087-688-594		hbedmutha@assess.com

Security Committee:

Nathan Thompson

Jane Zirbes

Mikolaj Buda

Lukasz Kregiel

Ryan Elmer (TBD - will be new Boulay representative)

Larry Smith

Executive Committee

David Weiss

Nathan Thompson

Authorizations in a crisis

Role in recovery / job title	Authorizations
Lukasz Kregiel	Authorized to take all steps specified in this Disaster Recovery Plan in order to recover the IT infrastructure / IT services
Mikolaj Buda	Authorized to take all steps specified in this Disaster Recovery Plan in order to recover the IT infrastructure / IT services
Nathan Thompson	Authorized to communicate with clients, suppliers, and vendors
Jane Zirbes	Authorized to cooperate with Suppliers and Vendors
Jorie Boswell	Authorized to communicate with clients

Necessary resources

The following resources will be used for the recovery of this activity:

Name of resource	Description	Amount	When the resource is necessary	Person responsible for obtaining the resource
<i>People:</i>				
ASC Security Committee	Primary POC for event.	Group or individual based on severity	Based on level of severity	Security Committee lead
<i>Applications / databases:</i>				
FastTest	Web based assessment platform		Based on service level agreements	Nate Thompson
Ada	Web based assessment platform		Based on service level agreements	Nate Thompson
<i>Data in electronic form:</i>				
ASC Policies in Google Drive	Business Continuity, Incident Response and Disaster	As needed	Once DR is initiated	Security Committee

	Recovery Plan documents			
<i>Communication channels:</i>				
Slack	Internal messaging app		As needed	
ASC email	Email System		As needed	
<i>Other equipment:</i>				
RDS Snapshot				
<i>Facilities and infrastructure:</i>				
Remote Worksites				
<i>External services:</i>				
AWS				
Percona				
Mundrisoft				
OAC				
Softur				

Recovery steps for the IT infrastructure / IT services

Example Scenario for AWS Infrastructure

#	Step Name	Step Description	Responsible Party	Est. Execution Time
1	Storage Layer Recovery	Verify existence of document copies in S3 bucket in separate region (OHIO)	Infrastructure Support	5 minutes

2	Database Layer Recovery	<ul style="list-style-type: none"> a. Provision a new RDS instance in OHIO region based on current set-up configuration: db.m4.xlarge instances hosting SQL Server Standard 2016. b. Restore the storage volume from latest replicated snapshot and attach it to the instance provisioned on (a). c. Set the provisioned RDS instance with Multi-AZ replication option set to ACTIVE or ON. 	Infrastructure Support	30 minutes
3	Web Layer Recovery	<ul style="list-style-type: none"> a. Provision 3 new EC2 instances in OHIO region based on current set-up configuration: r4.xlarge instances hosting Windows Server 2016 b. Restore the storage volume from latest replicated snapshots and attach them to the instances provisioned on (a). 	Infrastructure Support	20 minutes
4	Security Group Configuration	<p>Recreate relevant security groups for each of the layers:</p> <ul style="list-style-type: none"> - Web layer security group. - Load balancer layer security group. - Database layer security group. - Cache layer security group. 	Infrastructure Support	10 minutes
5	Load Balancer Configuration	<p>Recreates the Application Load balancer in the new Region, OHIO, and targets it to the 3 EC2 instances restored in numeral (3), Web Server Layer Recovery.</p> <p>Once load balancer is targeting the new EC2 instances, the security certificate for the Company domain is associated to the new load balancer to ensure that all communications between the client and the new servers are encrypted.</p>	Infrastructure Support	10 minutes
6	Domain/Hosted Zone Configuration	<p>Once load balancer set-up is completed, proceed to update the domain/hosted zone parameters for the Company domain (backup domain hosted in Amazon Route 53 DNS service) to point to the address provided by the new load balancer.</p>	Infrastructure Support	15 minutes

		This change may take time to further propagate worldwide, but as most DNS servers managing/targeting said domain are maintained within the AWS network, change should start being visible to the US region within the first few minutes after it is applied.		
7	Cache Cluster Layer Recreation:	<p>Proceed to recreate the Cache Cluster layer by launching a new cluster in the OHIO region, US-EAST-2, via the Amazon ElastiCache service.</p> <p>Said cache cluster is created with 3 nodes distributed in separate Availability Zones in the following manner.</p>	Infrastructure Support	20 minutes
8	Application Configuration Adjustments	<p>Application support team executes the following changes to the application configuration in each of the servers:</p> <ol style="list-style-type: none"> Adjust web application configuration to fit new web servers' set-up. Adjust web application configuration to be able to connect to the new database instance restored in (2) Database Layer Recovery. Adjust web application configuration to be able to connect to the passive-side S3 storage bucket instance restored in (1) Storage Layer Recovery. Adjust web application configuration to be able to connect to the newly provisioned Cache cluster from (7) Cache Cluster Layer Recreation. 	Application Support	45 minutes
9	Cache Refresh Process	Application Support team launches the cache refresh process to refresh recreated Cache cluster, as to be able to provide a responsive end-user experience.	Application Support	15 minutes
10	VERIFY COMPLETION	Once all steps are completed, team verifies usage and functionality of the application by connecting via the company domain.	Company IT	10 minutes

Ada Recovery Process:

#	Step Name	Step Description	Responsible Party	Est. Execution Time
---	-----------	------------------	-------------------	---------------------

1	Snapshot current production RDS server	In case of anything, it's always a good idea to take snapshot of current RDS server.	AWS Admin	15 minutes
2	What needs to be restored and from when?	Find out, what exactly needs to be restored - whole server, some databases (there is a couple) or maybe just some single entries (because they were overwritten by mistake) and from when (backup from yesterday?, from few day ago?)	Admin/Developers	15 minutes
3	Restore RDS backup as a new server	Set up new RDS server from backup	AWS Admin	15 minutes
4	Restore data	Get data from restored database (using mysqldump, raw mysql client or any other mysql client) and restore them to production RDS https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html	AWS Admin	Depends on what needs to be restored
5	Test & clean up	Test that restoration has fixed an issue/issues and remove RDS instance, which has been created from backup.	AWS Admin/Developers/Testers	15 minutes
6				
7				
8				
9				
10				

This activity should be recovered and documented in the following way:

Recovery procedures (main steps / individual tasks)	Persons responsible for implementation	Communication (content, to whom)	Implementation record (date / time)
[name of step no. 1]			
[task no. 1.1]			
[task no. 1.2]			
...			
[name of step no. 2]			
[task no. 2.1]			
[task no. 2.2]			
...			

Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Record of recovery step implementation (record in paper form)	Archive location	[job title]	Records are printed out and stored in a locked drawer or cabinet and accessible in Google Drive.	3 years

Communication Plan

If an incident occurs, follow this plan.

1. Determine if client uses the affected software
2. Determine appropriate contact at the client
3. Inform the contact of the incident and resolution, and efforts to prevent next time

Validity and document management

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of corrective actions based on conducted exercises
- number of corrective actions based on implementation of the plan in a crisis
- in the case of a crisis, whether the recovery was completed within the recovery time objective

Version History:

Version	Modified Date	Approved Date	Author	Reason/Comments
1.0.0	October 2018		Assessment Systems	Document Origination
2.0.0	June 2020		Assessment Systems	Updating to current team

