

EveryMatrix Disaster Recovery Plan

Code: P10-01

Change Control

Version	Date	Name	Role	Comment
2.0	01.07.2021	Dmytro Lanovskyi	CISO	Initial draft

Sign-off / Approval

Version	Date	Name	Role	Comment
2.0	23.03.2021	Rafael Campuzano	Group CTO	Approved

Filename, Location, Owner, and Classification

File Name	Disaster Recovery Plan v2.0.pdf
File Location	Confluence
Owner	EveryMatrix Group CTO
Classification	Confidential

Document Distribution

Role	Name	Organization
EveryMatrix Employees	EveryMatrix Employees	EveryMatrix Group

References

Reference	Version	Section/Control/Requirement
ISO/IEC 27001:2013	Second Edition – 01.10.2013	A.17
ISO/IEC 20000-1:2018	2018	clauses 7.5.4.e) & 8.7.2
ISO/IEC 20000-1:2018	2018	clauses 8.5.1

Contents

Change Control	2
Sign-off / Approval	2
Filename, Location, Owner, and Classification	2
Document Distribution	2
References	2
Contents	3
1. Introduction	5
1.1. Purpose.....	5
1.2. Scope and Assumptions	5
1.3. Reference documents	5
1.4. Terms and definitions.....	6
1.5. Contents and Plan Objectives	6
2. Contacts, Roles and Responsibilities.....	7
3. EveryMatrix System Description.....	7
4. System Recovery Phases.....	9
4.1. Planning and Preparation.....	9
4.2. Invocation and Notification.....	10
4.3. Recovery.....	10
4.4. Reconstitution	10
4.5. Timeline for Recovery	10
5. Disaster Recovery Scenarios	11
5.1. Top Risks.....	11
5.2. Loss of Romanian Datacenter	11
6. Disaster Recovery Environment.....	11
6.1. Google Cloud	11
6.2. Servers.....	12
6.3. Applications	12
6.4. Endpoints and Configurations.....	12
6.5. Backups.....	12
7. Disaster Recovery Procedures	13

7.1.	Invocation Criteria and Procedures.....	13
7.2.	Outage Notification and Evaluation	13
7.3.	Recovery Procedure	14
7.4.	Reconstitution Validation, Cleanup and Deactivation	14
8.	Disaster Recovery Plan Testing	15
8.1.	Purpose, scope and users.....	15
8.2.	Implementation of exercising and testing	15
8.3.	Review of results	16

1. Introduction

1.1. Purpose

This Disaster Recovery Plan (DRP) covers all the steps required in order to restore all EveryMatrix services provided to its clients in the event of a disaster within the Recovery Time Objective (RTO). This plan aims to minimize the impact of a disaster by ensuring recovery tasks are effective, methodical and thorough which should reduce mistakes and omissions. The aim is to meet both the agreed RTO as well as the Recovery Point Objective (RPO).

1.2. Scope and Assumptions

This document is applied to all processes and activities of the SMS.

The requirements of this document apply to all EveryMatrix employees, as well as all external parties who have a role in the SMS.

This Disaster Recovery Plan covers documentation and procedures regarding the EveryMatrix product provided to its clients. The scenarios that this plan covers take into consideration any event that would prevent EveryMatrix from providing the EveryMatrix product to the clients for a prolonged period.

Normally we consider RTO 12h and RPO 1h as regular values, but if there is a business need, we can adapt the Disaster Recovery Plan accordingly.

This plan does not address short-term disruptions lasting less than the RTO or the loss of only data at the EveryMatrix Romanian datacenter. This plan focuses primarily on the recovery of IT infrastructure (hardware, software and applications) to restore operations of the EveryMatrix product supplied to the clients. This Disaster Recovery should therefore be part of a larger Business Continuity Plan (BCP) that addresses areas such as data loss, finance, personnel and other emergency plans.

It is assumed that current backups of the system software and data are intact and available in the off-site Disaster Recovery Environment.

Lastly, this plan assumes that key EveryMatrix personnel have been identified and trained in their emergency response and recovery roles and they are available to activate the EveryMatrix Disaster Recovery Plan.

1.3. Reference documents

The following referenced documents are indispensable for the application of this procedure:

- *ISO/IEC 27001:2013 – Information Technology – Security Techniques - Information Security Management Systems – Requirements*
- *ISO/IEC 20000-1:2018, clauses 7.5.4.e) & 8.7.2*

1.4. Terms and definitions

The terms used in this document are defined within:

- *ISO/IEC 27000:2018 – Information Technology – Security Techniques - Information Security Management Systems – Overview and vocabulary*

1.5. Contents and Plan Objectives

Section	Content
Contacts, Roles and Responsibilities	List of EveryMatrix contacts, how to contact them and what responsibilities they will have as part of this plan. They will be provided with guidance for the restoration of the EveryMatrix services during a long period of service interruption. Also, this plan aims to ensure coordination with other external personnel and vendors associated with the execution of this plan.
System Description - EveryMatrix	Description of the EveryMatrix Applications and how they are currently deployed and running in production
Overview of the Four Phases	The four system recovery phases are: 1. Planning and Preparation Phase 2. Invocation and Notification Phase 3. Recovery Phase 4. Reconstitution
Disaster Recovery Scenarios	Description of the main Disaster Recovery Scenario covered by this plan – loss of the GTS datacenter in Bucharest, Romania
Disaster Recovery Environment	Information of the alternate site and its configuration for the EveryMatrix System and its dependencies.
Disaster Recovery Procedures	Activation Criteria and Procedures Outage Evaluation and Notification Recovery Procedures Recovery Notification and Escalation Reconstitution Validation, Cleanup and Deactivation
Disaster Recovery Plan Testing	Details of plan's periodic revision and testing
Appendix 1 - Asset list	Application inventory for EveryMatrix including key configuration items, data files, published endpoints and interconnection information.
Appendix 2 - Detailed Recovery Procedures	Keystroke-level recovery steps Required configuration settings or changes Recovery of data from backup files Other system recovery procedure, as appropriate
Appendix 3 - Disaster Recovery Environment Configuration	Google Kubernetes Engine

2. Contacts, Roles and Responsibilities

Role Name	Description
Disaster Recovery Owner (DRO)	Responsible for the content of the Disaster Recovery Plan (DRP). Sets and main objectives such as the RTO and RPO of the DRP. Need to be consulted before any changes are made to the DRP.
Disaster Recovery Commander (DRC)	Accountable for all aspects of a disaster response. Ensure availability of required resources. Delegates tasks to the DRRs and makes sure all areas of work are covered.
Disaster Recovery Responder (DRR)	Responsible to carrying out certain aspects of the DRP. Reports to the DRC.
Disaster Recovery Administrators (DRA)	Support the DRRs and DRC in any way possible. Responsible for sending out any communications required during the Invocation and Communication phase, the Recovery Phase and the Reconstitution phase. Act as scribes during the Disaster Recovery phase.
Disaster Recovery Stakeholder (DRS)	Need to be kept informed of progress via one-way communication. Anyone or any group who are affected by the outcome of the DRP and/or need to be kept up to date.

3. EveryMatrix System Description

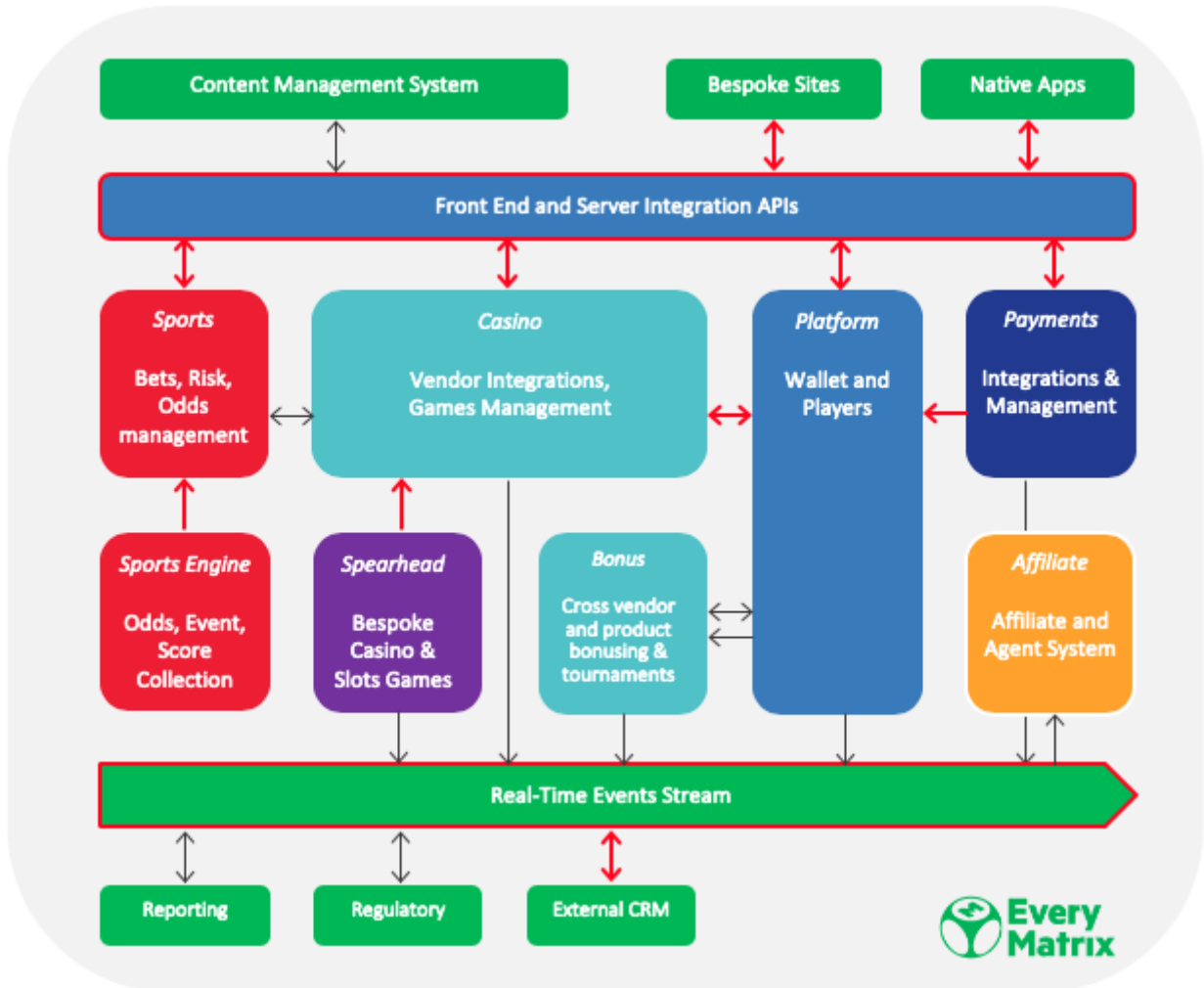
EveryMatrix delivers a modular and API-driven product suite for Wallet and PAM (Player Account Management), Casino, Bonus Engine, Sports Betting, Payments, Affiliates Management, Reporting System, Frontend web and mobile applications and Games Provider. The modular platform architecture allows partial (where the client opts for one or more of the EveryMatrix software services) or full integrations (where EveryMatrix offers a turnkey solution and provides everything from the back-office to front-end solutions).

In any case, all those EveryMatrix products are provided on a Software-as-a-Service basis, with platform hosting and maintenance managed by EveryMatrix.

These are the products (modules) of which EveryMatrix is comprised of:

- **CasinoEngine** – Casino gaming aggregator
- **BonusEngine** – Bonus and Promotions system
- **OddsMatrix** – Sports Betting platform
- **GamMatrix** – Wallet and Player Account Management system
- **MoneyMatrix** – Payment processing, KYC, & PSP aggregator
- **PartnerMatrix** – Affiliate & Agent management
- **RGSMatrix** (including Spearhead and Armadillo) – Bespoke game development studios and platform
- **DataHub** – cross-product data aggregation, reporting, feeds
- **FrontEnd** – CMS based and bespoke web and mobile app frontends

The following diagram presents a high-level overview of all those modules and how those are interconnected. All exposed APIs that can be used for the different levels of integrations are marked with red borders:



APIs which are exclusively concerned with server-to-server activities – e.g., directly adjusting a player's account balance – are not exposed directly to public access and require suitable server authentication tokens to operate. In all cases, access is provided using HTTP as the transport layer, using REST-style API signatures. The data transfer medium is JSON. Where direct-to-client push data is offered (e.g., live client account balances), HTTP SSE (Server-Sent Events) is the protocol used.

Technologies, Robustness and Scalability

Every component or set of nodes in which the solution is made is deployed in HA mode or is defined with local redundancy. For instance, the number of backend application servers are always defined in such a way that is ready to support double of the peak traffic, so that, even in the case of having 50% of the servers failing, the traffic can be handled (there are always more than 2 servers deployed). Databases are set up in cluster mode, or as a master-replica, with failover mechanisms to avoid downtime in case of failure. The load balancers are constantly querying the health-check methods, to react and remove from the traffic flows those servers that are suffering any kind of problem.

The technology stack varies according to products, although we have a certain amount of standardization of core infrastructure technology (e.g., Kubernetes is our standard orchestration platform.)

Key technologies used across the Group are:

- **Linux** and **Windows** OS, depending on the application or component
- **Proxmox** for virtualization
- **OpenStack/OpenNebula** for VMs orchestration
- **Kubernetes** and **Rancher** for containers orchestration.
- **New Relic, Grafana** (Telegram, Prometheus, Influx) and **Nagios** for monitoring
- **ELK** (Elasticsearch/Logstash/Kibana) for logs and some reporting
- **Apache Kafka** – for event streaming
- **RabbitMQ** – for message passing (the choice of whether to use Kafka or Rabbit for a given requirement is based on the required message delivery semantics and throughput requirements - i.e., each serves its own architectural purpose, and we choose appropriately.)
- **PostgreSQL** – this is our preferred open-source database solution.
- **MySQL** – we also currently support MS-SQL, but in general, are migrating instances to PostgreSQL.
- **In addition**, where required we also make use of Redis, VoltDB (for grid storage/computing in sports risk management,) MongoDB, Microsoft SQL Server (in the legacy GamMatrix platform, being deprecated by the replacement GM platform described above,) Apache Avro, and KSQL.
- **Programming languages:**
 - C#/.NET for Casino, MoneyMatrix and GamMatrix. All .NET applications are on a migration path to .NET Core, to allow for more hosting flexibility (i.e., non-Windows hosts) and containerisation. All new .NET developments (such as the next generation GamMatrix) are already developed using .NET Core.
 - Java for OddsMatrix, DataMatrix and SpearHead/RGSMMatrix
 - PHP for PartnerMatrix
 - Javascript (reactjs) for FrontEnd

4. System Recovery Phases

This Disaster Recovery Plan (DRP) had been split into four phases pertaining to a disaster. The first phase is the most important phase, it occurs before a disaster strikes and directly impacts the efficacy of the other three phases.

4.1. Planning and Preparation

The planning phase should include all tasks that can be done in advance that will reduce the Recovery Time Objective (RTO) from when the disaster strikes and lower the Recovery Point Objective (RPO) in terms of lost transactions after a disaster. The results of this phase are documented in the Disaster Recovery Environment section and Appendix 3.

EveryMatrix tests the contingency plan at least yearly by doing a dry run of what would happen in case the primary datacenter suffers a catastrophic or partial failure. This is done by running the disaster recovery procedures and making sure everything can be restored according to the predefined plan.

4.2. Invocation and Notification

The Invocation and Notification phase is intended to define what needs to be done once a severe EveryMatrix service outage has been detected. The Invocation phase is to ensure procedures of this DRP are correctly initiated and executed when a qualifying event occurs. Therefore, this phase contains criteria for the activation of this plan, steps to be taken to activate it and how to communicate at each step along the way. It also contains information regarding how and from whom to get approval before activating this plan.

4.3. Recovery

Once the plan has been activated, the recovery phase implements the procedures to restore the EveryMatrix system and repair damages. Once completed, the EveryMatrix service provided to the clients will function as described in the System Description section.

4.4. Reconstitution

The reconstitution phase is comprised of testing and validation that the original system capabilities have been restored as well as the steps required to deactivate the DRP. System owners are required to test functionality and data integrity before validating that the original system is recovered. The steps to deactivation incorporate notifying those that require it that the system is operational again as well as finalizing post-disaster tasks such as updating of documentation, conducting a postmortem and updates to the Disaster Recovery Plan itself.

4.5. Timeline for Recovery

The above recovery phases encompass multiple procedures, therefore, to determine how long it will take to restore all EveryMatrix services, a timeline breakdown for each process involved must be done.

EveryMatrix commits to recovering EveryMatrix solution adhering to the following timeline:

1. Disaster detection – 30 min
2. Registering a P1 incident – 15 min ([SLA for Incident Management](#))
3. Contacting an on-call person – 15 min ([Operations Schedule](#))
4. Holding an emergency meeting to investigate the problem – 30 min
5. Activating the Disaster Recovery Plan if recovery ETA is more than the determined RTO – 30 min
6. Preparing the Disaster Recovery environment – 2 hours
7. Deploying EveryMatrix Applications – 2 hours
8. Testing the Disaster Recovery environment (regression, load, stress testing) – 5 hours
9. Switching all operations to the Disaster Recovery environment – 1 hour

In total, the recovery process is expected to take up to 12 hours.

5. Disaster Recovery Scenarios

5.1. Top Risks

1. Cyber-attacks, state-sponsored or criminal
2. Major IT interruptions due to malfunction or human error
3. Acts of Nature such as earthquake or flooding
4. Failure of national infrastructure at a country level
5. Extreme violence such as riots or revolution
6. Terrorist attack
7. Pandemic, often spreading very quickly

Since EveryMatrix has applications hosted in EveryMatrix datacenter in Romania, the loss of this datacenter would constitute a disaster.

5.2. Loss of Romanian Datacenter

In case EveryMatrix datacenter in Romania is affected by, but not limited to, the above-stated disasters and, therefore, is lost, services that are hosted in it will be restored in Google Cloud using database backups, build scripts and redeploy of the application code from a copy of main source code repository and database backup files.

6. Disaster Recovery Environment

In preparation for the different Disaster Recovery scenarios, infrastructure, data and applications have been set up in advance in order to speed on the time to recovery in the case of a disaster.

Some of the prerequisites for safe usage of the disaster recovery environment:

1. The data for all databases can be restored from the backups.
2. The disaster recovery environment should be deployed 1 week after the deployment to the production environment to make sure that all the deploy scripts still work.
3. The disaster recovery environment IPs should be whitelisted by the clients.

6.1. Google Cloud

Google Cloud has been chosen to provide the infrastructure which includes all hardware and networking (Infrastructure as a Service) as well as a few managed services from Google Cloud. By using a cloud provider, one has the ability to scale up quickly without having to make emergency hardware purchases or keep extra capacity onsite "just in case".

GKE (Google Kubernetes Engine) will be used to create identical Kubernetes clusters as the Production ones.

6.2. Servers

All servers are listed in Appendix 1.

6.3. Applications

EveryMatrix maintains a set of scripts to reproduce the infrastructure of the solution in Google Cloud, as well as keeping a pre-installation of the most critical or time-consuming elements, to act quickly in the case the Disaster Recovery Plan is activated.

All applications can be installed using code repositories stored in GIT and the corresponding Continuous Integration (CI) tool, GitLab. These scripts and pre-installations will cover the entire turnkey solution. Games are also configured in these scripts but added to them with less periodicity than EveryMatrix critical components. Once the Ansible scripts are run, all versions are to be verified and deploy the latest one for each application.

The list of critical components to be deployed are documented in Appendix 1 – EveryMatrix Asset List.

6.4. Endpoints and Configurations

EveryMatrix API Endpoints necessary for the clients' connections will not change DNS names, only the IPs of the endpoints. The Unified Configuration System (UCS) configurations also do not require updating. All external endpoints required for the EveryMatrix-Client Disaster Recovery environments connection will be documented in Appendix 1 — External Endpoints along with the list of their consumers.

Example: games.prod.EveryMatrix.com is the production-used gamelaunch URL. The endpoint will remain the same during Disaster recovery, but the DNS record will be changed to use the IP address of the GKE Ingress.

6.5. Backups

As well as the servers and applications, what is also required are copies of the databases which will need to be restored in order to run the EveryMatrix product and meet the Recover Point Objective (RPO).

Backups are performed for all databases daily (frequency may vary in accordance with RPO, we are considering 12h hours max, in this case). This backup includes all databases of the turnkey solution. Network Attached Storage (NAS) is used in order to store local backup data (there is also a remote backup in google cloud, as part of the disaster recovery site). Periodic restores are performed according to the internal procedures in order to ensure data integrity.

For systems that are under the Automated Operation policy EveryMatrix ensures that the systems automated build scripts (Terraform, Ansible, Configuration Parameters for these scripts) are stored in a source control system and versioned accordingly. The source control systems are backed up daily. Configuration databases are also backed up daily.

All the backups are copied to the secondary disaster recovery location in Google Cloud to have them available in case the primary location fails or is not accessible, and the Disaster Recovery Plan needs to be activated.

GitLab Repository

The main GitLab instance is running on a dedicated machine in the datacenter. Therefore, another GitLab instance deployed in AWS stores the source code of EveryMatrix solution as well as all scripts required to recreate the environment. Besides, it is also regularly backed up to the Google Cloud Storage, with backup execution taking place daily at 00:00 UTC.

7. Disaster Recovery Procedures

7.1. Invocation Criteria and Procedures

The EveryMatrix Disaster Recovery Plan shall be activated if one more of the following criteria are met:

1. The type of outage indicates that the EveryMatrix system will be down for more than 12 hours (the Recovery Time Objective (RTO)).
2. EveryMatrix datacenter in Romania is damaged and may not be available for 12 hours.
3. Internet connectivity to the EveryMatrix datacenter in Romania may not be available for 12 hours.
4. An earthquake, terrorist attack, flood or any other force majeure that has a high potential for causing an outage in Romania that is expected to last more than 12 hours

The following roles defined below may activate the DRP if one or more of the above criteria are met:

1. DR Owner for the client and EveryMatrix
2. DR Commander for EveryMatrix

7.2. Outage Notification and Evaluation

The first step after activation of the DRP is to notify the appropriate business and technical personnel from both EveryMatrix and the clients/operators. Contact information is included in the Contact List as well as who needs to be only notified and who must be called to work.

EveryMatrix's Disaster Recovery Commander (DRC) must ensure that the clients are informed both via an email and phone call that a major service outage has been detected, and that EveryMatrix is activating this DRP. The DRC must ensure that the EveryMatrix Incident Management team are notifying people needed to carry out the procedures outlined in the DRP using a combination of Instant Messenger and phone, depending on response. A new chat group should also be set up dedicated to communication regarding this disaster. The EveryMatrix Incident Management team will also need to inform EveryMatrix management and product owners via email notification following the standard operating procedures for handling major incidents.

After the notifications have been sent out, an initial assessment of the outage is required to be provided to the DRC in order to facilitate the invocation of the DRP.

The Outage Notification and Evaluation are done as per the agreed Incident Management/Problem Management procedures of handling A(P1) type incidents. The only difference is that the contact list should reflect the contact list in this document.

7.3. Recovery Procedure

If the criteria for invoking the DR Plan have been met, the evaluation of what has been affected has been completed, and all relevant parties have been notified that this DR Plan is to begin, then the following steps must be carried out precisely in the order described below to resume the EveryMatrix service for the clients within the RTO and without losing more data than agreed by the RPO.

Loss of EveryMatrix Services hosted in GTS Datacenter in Bucharest, Romania, and full restoration in the Disaster Recovery Environment

1. Activate the pre-installed infrastructure and adjust needed resources in Google Cloud.
2. Run the Terraform scripts for all EM Application servers which are listed in Appendix 1, using the terraform plan to make sure that the Google Cloud Platform (GCP) instances exist, are up-to-date and are using the current configuration.
3. Bootstrap on all the required VM instances using the Terraform scripts as described above in the Disaster Recovery Environment section.
4. Verify by using the Google Cloud Platform (GCP) Console that all servers exist and are now up and running.
5. Test the correct setup of the infrastructure.
6. Run the pipelines to deploy the packages into the DR infrastructure.
7. Restore databases from backups.
8. Verify that all applications are up and running and that they have correctly registered themselves with Kubernetes and passed the Kubernetes health checks.
9. Update the external DNS records according to the IPs in the Google Cloud.
10. Perform the testing of the Disaster Recovery Environment.
11. Switch the traffic interchanged with payment vendors to the new setup (DNS changes in most of the cases) and whitelisting of IPs.
12. Enable backup jobs for the Disaster Recovery Environment.

7.4. Reconstitution Validation, Cleanup and Deactivation

Restoring EveryMatrix Services hosted in GTS Datacenter in Bucharest, Romania

The reconstitution phase is comprised of testing and validation that the original system capabilities have been restored upon the recovery of the affected datacenter after the disaster. It also covers the steps required to deactivate the DRP.

Plan of action

1. Check if all the applications are up and running.
2. Update the new production databases using the latest backups from the Disaster Recovery Environment.
3. Stop the EveryMatrix Applications in the Disaster Recovery Environment.
4. Take a differential backup since the last full backup, copy it to Production and restore it for the Production databases.
5. Run final tests on the new Production Environment.
6. Switch DNS endpoints of EveryMatrix services back to the Production Environment.
7. Perform testing of the Production Environment (synchronous and asynchronous systems)

8. Disaster Recovery Plan Testing

8.1. Purpose, scope and users

The purpose of the DRP testing is to ensure that the plan can meet the stated purpose of this plan, restoring the EveryMatrix system for the clients within the Recovery Time Objective (RTO). Without testing, the plan may fail to include all necessary requirements, procedures or correct order of tasks.

The DRP will be tested without the clients' or GSP's involvement, meaning EveryMatrix is responsible to test the full restoration of the EveryMatrix Service and can run it in a standalone configuration.

Users of this document are all persons with a role in the DR Plan.

8.2. Implementation of exercising and testing

Disaster Recovery exercising and testing is implemented in EveryMatrix in the following way:

- Period: at least annually
- A person responsible for coordination and implementation of exercising and testing: CISO
- Exercising and testing objectives are the following:
 - to check whether the plan is accurate, solutions are in place, and resources provided to:
 - implement the recovery plan for each activity
 - check whether employees responsible for recovery are familiar with plan details
 - check the implementation of all steps specified by the plan
 - ensure all necessary resources (including recovery data)
 - enable communication and warning procedures between individual team members, towards other recovery teams, Incident Management Team, and other interested parties
 - to create comments or suggestions in order to improve the plan
- Exercising and testing scope: EveryMatrix turnkey solution
- One of the following exercising and testing methods shall be selected:
 - Desk Check - checking the plan by means of auditing, validation and verification techniques; conducted with plan author and moderator

- Plan Walkthrough - checking the plan by means of team interaction; conducted with the main plan participants and the moderator, whose interaction is tested in a joint meeting
 - Simulation - testing all interrelated plans (including supplier procedures) with real information resources, but with no need of relocation to the alternative site; conducted with all necessary employees, suppliers and the moderator
 - Functional testing - activities are relocated to the alternative site in a controlled (announced) exercise; all necessary employees, suppliers, the moderator and observers take part
 - Full testing - all activities are relocated from the original site to the alternative site (announced or unannounced); all necessary employees, suppliers, the moderator, observers and auditors take part
- Will exercising and testing be announced: YES
 - Scenario upon which the testing and exercising will be based: Loss of EveryMatrix Services hosted in GTS Datacenter in Bucharest, Romania

8.3. Review of results

The CISO reviews the results of exercising and testing and prepares an Exercising and Testing Report.

In the Report, appropriate corrective actions must be initiated, as well as other recommendations for improvement.