Frequently Asked Questions

xMatters Business Continuity, Disaster Recovery and Pandemic Preparedness

July 2020
Information Assurance Team

Does xMatters have a documented Business Continuity Plan?

Yes, as part of ISO 27001 certified controls, xMatters has a documented Business Continuity Plan (BCP). This covers the ongoing operations of the cloud environment and corporate activities should a disaster, pandemic, or any other catastrophic event occur. The xMatters BCP also describes the procedures to recover and sustain its business operations, based on an annual Business Impact Analysis (BIA), which includes the identification of critical resources and an assessment of potential disruption impacts, allowable availability thresholds, and recovery priorities.

The operational risks outlined in the plan provide xMatters with a comprehensive assessment of its business continuity posture and prioritization.

Cloud operations continuity is supported by a Disaster Recovery Plan (DRP), which evaluates various scenarios and completes datacenter failover tests. These tests are conducted daily, and reports are generated every quarter (available for clients upon request).

Does the plan include a formal annual executive management review?

Yes. The xMatters BCP, BIA and DRP are reviewed, at least annually, by the xMatters Information Security Management System Steering Committee, and validated on a semi-annual basis during its ISO 27001 assessment (external and internal audits).

Can you describe the Business Continuity Plan?

1 – Datacenter Failover Tests
The xMatters BCP describes the recovery resources, procedures, and priorities necessary to provide seamless customer access if a disaster occurs that impacts customer data at the data center(s).

The BCP is integrated with a DRP to remedy client access to data available through geographic diversity between data center pairs ('active-active'). This is achieved by segmenting and compartmentalizing the continuity management needs into sections and regions, as described below:

- **European Union:** London, UK (europe-west2), and Germany (europe-west3).
- **Asia-Pacific:** Sydney, Australia (australia-southeast1), and Singapore (asia-southeast1).

- **North America:** Moncks Corner, South Carolina (us-east1), and Council Bluffs, Iowa (us-central1).

Both data centers in a pair are always active and have identical processing capabilities, and each data center can support the combined production load of the pair. The main levels of continuity management are detailed in the BCP, which addresses the xMatters corporate operation, system operations, and technical support.

The specific requirements of continuity management policies and procedures are also outlined in the BCP, as well as exemption requirements, infraction consequences, applicability, and training requirements.

Continuity management is a risk-based approach to managing risks/issues that can cause interruption/disruption to business operations or service delivery operations. Managing risk/issues includes determining the most common causes of interruption/disruption, and having prepared plans for the treatment of risks/issues.

Recovery Time Object (RTO) is set to 30 minutes, Recovery Point Objective (RPO) is set to 24 hours.

2 – Work from Home (“WFH”) Risk Analysis

xMatter's Information assurance team has conducted a detailed Risk Analysis based on the possibility that the work from home scenario could be extended for a longer period of time. We believe that the necessary arrangements and controls have been deployed for a secure WFH set up and we believe we will be able to consistently deliver our services with the same quality.

3 - Critical suppliers

We have identified all essential suppliers and service providers, and we have assessed them with the objective to evaluate their continuity and preparedness plans. We have a process in place to constantly monitor our critical suppliers and we are working closely with our suppliers to secure guarantees around delays and disruption in their services.

4 - Technical Support and Operations

As part of our Business Impact Analysis, we have also identified our critical business functions and we have prepared and implemented a Continuity Plan applied to roles based on criticality. Based on the current set up and service analysis, we do not anticipate any impact or delays that might affect clients. Operations and Technical Support professionals are physically segregated. Additionally, different business functions can temporarily support these teams, if necessary, since cross-training is already in place to ensure critical functions continue with minimal disruptions.

Do continuity business procedures include cloud specific information security activities and processes (for example, vulnerability management, IDS, capacity management)?

Yes. If a primary data center becomes unavailable, the secondary data center will resume the functions with live data and capabilities.

Do formal business continuity procedures include the continuity of IT operations and support?

Yes. The xMatters corporate network is also included in the BCP, including 24/7 technical support with offices located in different time zones.

Does the response and recovery include specific roles and responsibilities?

Yes. All xMatters policies and procedures include the specific roles and responsibilities for those who are involved in executing it.

Is a critical vendor list made available to clients?

Yes. The list is available to clients upon request.

Does xMatters assess the business continuity preparedness of critical vendors?

Yes. The Supplier Assessment and Monitoring Process (SOP A15) is also part of ISO 27001 controls. All critical vendors are reviewed on an annual basis.

If you require any further information, please do not hesitate to contact security@xmatters.com.