



WEM No-Code

Modeler Production disaster recovery exercise

Amsterdam
14th April 2025

Elia Ebbing – CTO
Douwe Roelofsen – COO
Pieter Emmelot – DevOps Engineer
Lilach Pollak – Information security team leader



Introduction

In an effort to validate WEM no-code's Incident Response Plan, WEM no-code will conduct a tabletop exercise to examine processes and procedures associated with the implementation of the Incident Response Plan. This discussion-based exercise will be a 3-hour event that will begin at March 3th 2pm and will last until March 3th 5pm.

The exercise is designed to facilitate communication among select personnel regarding the implementation of recovery operations following an event causing the outage of mission critical systems managed by WEM no-code. This exercise is designed to improve the readiness of the WEM no-code and help validate existing Incident Response Plan procedures.

Participants should come to the exercise prepared to discuss high-level issues related to the recovery of mission critical systems at WEM no-code. To achieve the exercise's stated objectives, discussion will focus on the following WEM no-code's contingency planning elements:

- What would be done to recover each class of system (e.g., Messaging, Web) impacted by a security event?
- How will system recovery be accomplished and what is the priority/optimal chronology of restoration?
- What is the time required for restoration and how can this be optimized?
- What are the expected results and action items that will assist system teams and improve readiness after the exercise?

Participants may choose to bring back-up reference material that will aid in answering the above questions.

Concept of Operations

A tabletop exercise is a discussion-based event in which participants meet in a "classroom" or collaborative remote setting to address the actions they would take in response to an emergency situation. Tabletops are an effective initial step for personnel to discuss the full range of issues related to a crisis scenario. These exercises provide an excellent forum to



examine roles and responsibilities, unearth interdependencies, and evaluate plans.

Participants will be presented with a scenario affecting the availability and continuity of business critical systems. A facilitator will help guide discussion by asking questions designed to address the exercise's objectives. The facilitator may choose to inject modifications to the scenario to further stimulate discussion. Participants will also be encouraged to ask one another questions.

Objectives

The exercise objectives are as follows:

- Validate the team's ability to recover IT operations at alternate facility
- Validate the accuracy of recovery procedures documented in the Incident Response Plan
- Identify areas of the contingency plan that need to be revised.

Scenario

At 2:00 AM on September 20th, 2025, the WEM modeler production environment becomes unavailable due to a critical infrastructure failure at our cloud provider, TransIP. Despite being hosted across multiple data centers, the issue impacts both locations, leading to a complete outage. Our uptime monitoring system immediately detects the problem and triggers alerts. Following an initial investigation, the DevOps team determines that the most effective course of action is to rebuild the WEM modeler production environment on an alternative cloud provider, Microsoft Azure, to restore service availability.

Discussion Questions

The following questions are designed to be used by the facilitator to guide the discussion and ensure the pre-defined objectives are met; depending on the flow of the exercise, the facilitator may elect to use these questions or other questions to ensure participants meet the objectives through the discussion:

1. How quickly did we detect the outage, and were the right people alerted in time?
2. What is our internal incident classification for this type of outage, and who has the authority to declare a major incident or disaster?
3. How do we inform affected clients and partners about the outage, and what information do we provide initially?



4. Who is responsible for internal and external communication, and what are the expectations for status updates during the incident?
5. What are the steps required to rebuild the WEM modeler production environment in Azure, and do we have up-to-date documentation and automation to support this?
6. How long would it take to restore a functional modeler environment on Azure, and what are the key dependencies or risks during that process?
7. What impact does this outage have on clients currently working in the modeler, and what is our plan to minimize data loss or work disruption?
8. Do clients have alternative ways to access their data or applications during this outage? If not, should we offer temporary access to backups or staging environments?
9. Once service is restored in Azure, how do we verify integrity, performance, and client access before officially announcing recovery?
10. What long-term improvements should we consider to reduce dependency on a single provider and improve our multi-cloud or DR strategy?

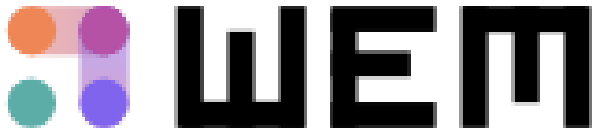
Debrief/Hotwash Questions

An after action report identifying strengths and areas where improvements might be made will be provided after the exercise. The following questions are designed to obtain input into the after action report from participants.

1. Are there any other issues you would like to discuss that were not raised?
2. What are the strengths of the contingency plan? What areas require closer examination?
3. Was the exercise beneficial? Did it help prepare you for follow-up testing?
4. What did you gain from the exercise?
5. How can we improve future exercises and tests?

Discussion Findings

The Modeler Production disaster recovery exercise provided information on the DR procedure for the Modeler environment. An important benefit of the exercise was the opportunity for participants to raise important questions, concerns, and issues. At the conclusion of the exercise, participants were asked to complete an evaluation form regarding the information provided, additional information needed, and their thoughts on the event and topics, to be included in the after action report.



The discussion findings from the exercise along with any necessary recommended actions are as follows:

General Findings

The exercise provided an excellent opportunity for participants to the Business Continuity and Disaster Recovery Plan. As a result of the exercise, participants left with a heightened awareness of the Business Continuity and Disaster Recovery Plan.

The monitoring system functioned as expected, ensuring timely alerts and proper escalation. Backups were available, and the system configuration and deployment are largely automated through our CI/CD pipeline. However, the pipeline is closely tied to our current cloud provider (TransIP), and switching to a different provider requires manual adjustments that depend on the specialized knowledge of a few key personnel. This creates a risk of delays during recovery. Additionally, the time required to fully provision a new environment and restore operations on a different platform remains uncertain.

Specific Findings

Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:

1. Observation:

The monitoring and alerting system reliably detects outages and notifies the appropriate team members.

Recommendation:

Maintain current monitoring setup and regularly test alert flows to ensure continued reliability.

2. Observation:

Backups are available, and our infrastructure is deployed using automation via CI/CD.

Recommendation:

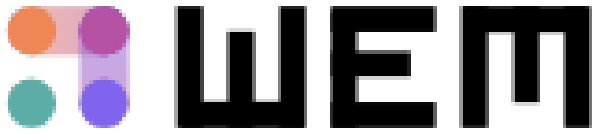
Continue maintaining regular backups and review automation scripts periodically to ensure they remain up to date.

3. Observation:

The CI/CD pipeline is tightly integrated with TransIP, and migrating to another provider requires manual intervention by a small group of experts.

Recommendation:

Decouple the CI/CD process from provider-specific configurations where possible, and cross-train additional team members to reduce reliance on key personnel.



4. Observation:

The timeline for setting up a fully functional environment on a new cloud platform is currently unknown.

Recommendation:

Conduct a timed dry run of the full migration process to another provider (e.g., Azure) and document the steps, estimated durations, and potential blockers to improve preparedness and confidence in disaster recovery.