## CASE STUDY

# Bank of Israel: Addressing Disaster Recovery and High Availability Challenges with Continuity Software

Sponsored by: Continuity Software

Dan Yachin
August 2009

52 Begin Road Sonol Tower Tel Aviv, 67137 Israel Tel. +972 3 68 71 727 Fax. +972 3 68 71 720 www.idc.co.il

## IN THIS CASE STUDY

This case study looks at Bank of Israel's (BOI) disaster recovery (DR) and high availability challenges surrounding the need to protect and ensure the continuous availability and performance of its critical data center operations. The study analyzes the benefits gained by BOI by implementing Continuity Software's solutions, which are aimed at allowing organizations to continuously assess their DR readiness, avoid system downtime, data loss or data corruption, as well as ensuring regulatory compliance.

## SITUATION OVERVIEW

### Introduction: Bank of Israel Overview

The Bank of Israel (BOI) is the central bank of Israel. Founded in 1954, BOI serves various functions, including the following:

- Regulating and directing monetary policy
- Providing economic advice to the government
- Managing the foreign exchange reserves and foreign currency market
- Monitoring and analyzing foreign exchange activity
- Banking supervision
- Promoting financial stability
- Issuing currency
- Banking for the government and the banks
- Representing Israel in international institutions

In light of the national importance of ensuring the continuous availability and performance of its data center and systems, BOI has made substantial efforts in recent years to improve its IT infrastructure. As part of these efforts, significant investments were made in securing the bank's DR readiness and addressing high availability needs.

BOI's data center architecture consists of production and DR sites. The production site includes a central storage array and servers hosting the different databases and applications. Each production server is comprised of two clustered servers, and a mirrored storage array is deployed at the DR site. To synchronize the production site with the DR site, BOI uses synchronous remote data replication. Additional data protection and recovery solutions (e.g., backup, replication and snapshot, and management solutions) are used for the production servers.

## Challenge

Given the critical nature of its data center operations, BOI has defined strict Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO refers to the acceptable amount of time to restore operations; RPO refers to the amount of data that can be lost without significantly affecting the organization. RTO and RPO therefore define an organization's backup, replication, and other DR requirements.

BOI requires frequent testing of DR readiness to make sure its systems are consistently and properly backed up in the DR site. Traditionally, such DR testing is performed by manually looking for configuration mismatches between the two sites in specific applications, fixing any mismatches accordingly, running scripts, and implementing the required updates. As a result, common drawbacks of the manual approach include operational disruption, inability to cover the entire environment, and lack of real-time information.

In the case of BOI, the initial demand has been to test DR readiness every several months. However, it was soon realized that DR testing involves significant operational disruption. As each test required the arrival of the IT infrastructure teams to the DR site, setting up the site, and the arrival of users and conducting multiple tests, it resulted in considerable time consumption, as well as concerns over the effect of the DR testing on the production systems. In addition, each test required that the DR site would stop functioning as a backup site until the test is over, potentially exposing BOI to recoverability problems in the event of an actual DR situation.

On the other hand, the need to perform DR tests has only been increasing in frequency due to the dynamic nature of BOI's data center, which has grown in scale and complexity over the years. As a result, BOI has been increasingly challenged with the potential for configuration gaps between the production and DR sites. In this situation, the need to continuously ensure that changes made in the production servers will be properly replicated in the DR and high availability servers has become even more important.

To address these concerns, BOI has decided to look for solutions to ensure readiness and compatibility between the production and DR sites consistently and automatically. Continuity Software's RecoverGuard solution was chosen as most suitable for the bank's demands at both the storage and system level, as well as in terms of time and ease of implementation.

## Solution

Continuity Software's RecoverGuard is aimed at mitigating data protection, DR, and high availability concerns. This is done by detecting replication infrastructure gaps and configuration vulnerabilities between a customer's primary production and disaster recovery localized solution and/or remote sites. RecoverGuard's key features include:

**IT discovery and scanning.** An automatic, agentless tool used to non-disruptively and continually scan an IT environment and collect critical configuration data from key IT assets, including storage, servers, and databases.

**Gap detection engine.** Identifies and reports on more than 3,000 known gaps and vulnerabilities in an IT infrastructure (it then delivers alerts in a predetermined fashion – via email or by sending alerts to enterprise ticket management systems, thus allowing the customer to take immediate action to ensure ongoing data protection, disaster recoverability, and business continuity).

**Visualization and reports.** Allows customers to drill further down into the IT infrastructure configuration status, as well as the previously discovered data protection and disaster recovery gaps (i.e., SLA compliance and exceptions, change and audit reports, configuration changes trend analysis, and business services recoverability status).

**Optimization.** Leverages the data center topology map to detect under/over utilized assets, allowing organizations to fine-tune resources and fully exploit infrastructure value.

In addition, RecoverGuard identifies and addresses gaps that are unique to VMware and other virtualization environments. Other capabilities include host configuration gap detection; integration with Configuration Management Databases of leading vendors and ticket management systems; support for all major platforms, including all open operating systems and storage systems (e.g. EMC, HDS, IBM, HP and NetApp) and their respective replication capabilities. Future releases are planned to add support for leading host-based replication solutions, including Oracle Data Guard, EMC RecoverPoint and Symantec VVR.

The product's latest version 4.0 includes the HA/DR System Configuration Validation feature, which allows HA/DR environments to be kept in sync with production environments. Other capabilities include:

- Community-driven gap knowledge base updated regularly
- Continuous verification of IT changes
- Policy-driven SLA management that allows measuring and analyzing RPO
- Identification of deviations from industry best practices as well as regularly updated recommendations on industry and vendor-based best practices
- Continuous assessment of business continuity risk level through centralized dashboard

In addition to RecoverGuard, Continuity Software provides DR Assurance, a Web-based service that remotely monitors customers who use RecoverGuard for disaster recovery and high availability vulnerabilities. The service includes monthly Web meetings to review and resolve such issues as they arise, as well as continuous vulnerability notifications.

## Results and Benefits

After deployment, RecoverGuard initiated a scan of BOI's IT infrastructure to obtain DR and high availability-related configuration data from the different infrastructure components. Configuration gaps were then detected, prioritized, and reported, allowing the BOI IT team to immediately mitigate critical problems posing the greatest risk to critical business services. The product is now set to continuously identify and report DR gaps as they emerge.

According to BOI, with RecoverGuard in place, the uncertainty factor has been significantly mitigated and the customer now feels more confident that the IT infrastructure configuration is aligned to the HA/DR recovery goals. Other key benefits include having a single system for centrally storing and accessing comprehensive configuration data on the entire IT environment – from the storage array to the file system level in a given server, on any other IT resource defined on the cluster. In terms of high availability benefits, BOI notes that RecoverGuard identified several cases of misconfiguration at the production server cluster, which might have led to failure if undetected.

In addition to RecoverGuard, BOI has been using Continuity Software's DR Assurance service. The service provides quarterly reports that summarize all events, configuration gaps, and errors, as well as recommendations on how to improve the efficiency of the DR and data protection operations and processes, and achieve improved security and DR readiness. This includes, for example, recommendations on how to duplicate database control files, when to take snapshots, how many snapshots to take, etc.

# CONCLUSION

Despite heavy investments in building and maintaining disaster recovery and high availability environments, many organizations are struggling to ensure that their objectives are met in a consistent manner. The BOI case study illustrates this problem. Given the criticality of BOI's data center operations, the bank has defined strict DR objectives, which to a large extent could not be met, due to an inability to effectively test their DR readiness. By using Continuity Software's solutions, BOI has been able to identify configuration gaps between its production and DR sites, and keep track of data protection gaps caused by the frequent configuration changes in the production site. Thus, it has been able to ensure its ability to maintain its objectives while improving the effectiveness of its DR operations.

## Copyright Notice