MERCURY™

Disaster Recovery Planning Focus Area

Document Information

Document title:	Control Objectives – Disaster Recovery Planning Focus Area
Document file name:	Control Objectives - DRP Focus Area - v2
Revision number:	2
Issued by:	Ron Wilson
Issue Date:	10/21/2004
Status:	Draft

Document Approvals

IT Process Owner	Signature	Date
SOX IT Program Owner	Signature	Date
Chief Information Officer	Signature	Date

Table of Contents

DS4—ENSURE CONTINUOUS SERVICE

COBIT DESCRIPTION:

Managing continuous service includes the ability to recover from a disaster. Controls need to be in place to manage various disaster scenarios, from backup and recovery to full business continuity. Actions performed in this area align with the control activities and monitoring components of COSO. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For instance, the inability to recover from a disaster after year-end could prevent the organization from producing financial reports that are supported with source documentation and details of transactions that make up financial reporting balances.

MERCURY PROCESS DESCRIPTION

Mercury Interactive protects its business processes and data through backup and restore procedures as detailed in the Backup and Offsite storage procedures (referenced elsewhere in this document). These backups use industry standard software and servers as described in the Global Backup Procedure (GTO-PRC-039), the Global Backup Policy (GTO-POL-039), and the Global Backup Standard (GTO-STD-039), to back up and restore critical business applications and data.

The primary business applications addressed in this document are Lawson, Aviv, and Siebel 7.5. Business data that is not backed up falls into one of the following categories:

- The data can be estimated, or,
- The data is transferred and resides in an application that is in scope for Disaster Recovery Planning, or,
- The data is not needed for financial reporting.

Using Veritas software or other industry-standard backup software, stored on IBM or other industry-standard tape backup media, incremental backups are performed daily. Full backups are performed weekly. Each tape is clearly labeled and inventoried. Each backup is verified for both media and content by the Backup and Storage Administrators per the Global Backup Procedure (GTO-PRC-039), the Global Backup Policy (GTO-POL-039), and the Global Backup Standard (GTO-STD-039). In the United States, the daily backups are stored locally at the Humboldt data center in Sunnyvale, California. In Israel, the daily backups are stored at the Mercury corporate offices in Yehud. In both instances, the tapes are stored in an environmentally secure (fireproof and waterproof) vault. On a weekly basis, Iron Mountain Data Systems located at 29555 Kohoutek Way, Union City, California collects the weekly Mountain View tapes and stores them off-site at their secure location. In Israel, DataBank, located at 7 Hamasger Street, Tel Aviv, Israel, (office and vault), collects the weekly backup tapes and stores them off-site at their secure location. Retention logs are written and reviewed by the Backup and Storage Administrators on a weekly basis to ensure that the correct data is being backed up. In the event of a backup failure, a new backup is scheduled and an incident logged as per the Incident Management process (detailed in Control Objectives – Operations document). Changes to the backup schedules, applications, or data being backed up are approved by the Regional Operations Manager based on the recommendations of the Business Applications Owner or regulatory/compliance requirements as dictated by the Legal department. Backup tapes are retained for seven years.

There are three basic situations where data needs to be restored:

- Accidental deletion
- Data corruption
- Forensic activity

When data needs to be restored, it is restored as per one of the following:

- System recovery—restores everything including systems, applications, data and equipment
- Application recovery—restores the applications onto the server
- Data recovery—restores data to the location it was residing

These restoration scenarios are supported by the following policies, procedures, and standards:

- GTO-PRC-001 Aviv DRP
- GTO-PRC-002 Lawson DRP
- GTO-PRC-003 Siebel 7.5 DRP
- GTO-PRC-044 Yearly off-site storage assessment
- GTO-PRC-039 Global Backup Procedure
- GTO-POL-039 Global Backup Policy
- GTO-STD-039 Global Backup Standard
- GTO-PRC-040 Send/receive Backups from Offsite storage
- GTO-PRC-061 Annual test of DRP procedures

Complete onsite restore procedures are reviewed annually. A printed copy of the procedures is located in the fireproof vault with the backup tapes and a soft copy online through the IT Portal.

In the event of a disaster at a Mercury office containing one or more business critical applications, the affected business critical application can be restored at one of the following alternate Mercury offices: Yehud, Israel; Sunnyvale, California; Boulder, Colorado or Surrey, United Kingdom. In the event that the required hardware is not available, Mercury maintains favorable relationships with vendors allowing them to order and take possession of the required resources and bring the environment up within one week at an alternate site.

Note: Five of the nine control objectives for DS4 are out of scope as outlined in the IT planning document. These control objectives pertain to business continuity planning, which is out of scope per PCAOB guidance. This document addresses the remaining control objectives.

COBIT CONTROL OBJECTIVE 4 – The IT Organization's Members Responsible For Disaster Continuity Plans Have Been Trained Regarding The Procedures To Be Followed In Case Of An Incident Or Disaster

Mercury Control Description

IT personnel (the backup team), as assigned by Regional Operations Managers, have been trained in both onsite and offsite backup and restore procedures for the three primary business

applications, Lawson, Aviv, and Siebel 7.5. These applications are located in corporate data centers located in Sunnyvale, California and Yehud, Israel. The policies, backup and restore procedures and equipment configurations are documented and available to all assigned employees, in print at the restore location and online at the IT Portal

Risk Area

None

Mitigating Approach
Not applicable

COBIT CONTROL OBJECTIVE 5 – IT Management Has Ensured That The Continuity Plan Is Adequately Tested, At Least Annually, And That Any Deficiencies Are Addressed Within A Reasonable Period Of Time

Mercury Control Description

The Regional Operations Managers ensure that the backup and restore plan is tested annually with the active participation of the backup team member(s) for each business application at each site. The plan is reviewed annually. Deficiencies are addressed as they are identified and the plan is updated by the Regional Operations Managers in conjunction with the local application and network managers. Procedures are updated to correct deficiencies and stored with the backup media and at the individual restore sites.

Risk Area

Offsite restore procedures have not been tested.

Mitigating Approach
Onsite restore procedures have been tested; our offsite procedures and hardware requirements are identical to the onsite procedures and hardware requirements.

COBIT CONTROL OBJECTIVE 6 – Where New Risks Are Identified, Appropriate Changes Are Made To The Business Continuity And Disaster Recovery Plans

Mercury Control Description

As we learn about new risks, Regional Operations Managers review the existing DRP plan and update it and all effected procedures on an ongoing basis. The backup team is then trained on the updated DRP plan.

New risks are identified and assessed in one of the following ways:

- Annual Security assessment
- During the System Design Life Cycle
- Management direction of significant business changes

During the System Design Life Cycle (SDLC) process, a Security and Business Risk Assessment is done to determine the necessary disaster recovery requirements. Once the assessment is completed, the Global Security and Risk team works with the Global IT Operations group to define, design and develop an appropriate DRP solution as needed. The DRP documentation is then updated and training is provided as needed.

Risk Area
None

Mitigating Approach
Not applicable

APPENDIX

SFA—Off-Site Store Visit Report—Iron Mountain

Document Title	Mercury off-Site Storage – Visit Site Procedure
Document Number	001
Related Documents	Off-Site visit yearly Procedure \ Backup tapes delivery procedure \Backup tapes delivery weekly report

Off-site Storage Company: Iron Mountain

Scheduled:
Tuesday, September 07, 2004

Visit done by:
Erez Batat

Steps and Question Reviewed during visit:

- **Off-site company service description**
    - **Company Details**:
        - Company name: **IronMountain**

      Business Address:
      29555 Kohoutek Way
      Union City, CA 94587

      Business: (510) 489-5100
      Business Fax: (510) 487-3647

      E-mail: Sherrie.rae@ironmountain.com
      E-mail Display As: Sheri Rogers (Sherrie.rae@ironmountain.com)
      Sheri Rogers - AE - x305

      Full Name: Sheri Rogers
      Sherrie.rae@ironmountain.com

- **Physical layout of the facility**
    - **Description of the environment**
        - IronMountain is located in an industrial area in Union City, off of the 880 highway.
        - The place is located on ground floor. There is one entrance in the front as well as a back entrance for trucks.
        - The storage rooms are accessible through the front entrance after sign-in and authentication.
        - The place is manned 21 hours a day. During other hours, a security company is called to respond within 3-5 minutes.
    - **Check for Obstacle in physical layout**
      None
    - **Access to the facility**
        - Access is through two heavy doors protected with alarms. The two doors cannot be opened at the same time, to create a video surveillance protected corridor.

- All visitors must sign-in in order to get access. The visit must be pre-scheduled and all the names must be communicated by an individual who is registered with the company as a trusted authority.

  - **Distance from Mercury building**
    Distance is 21 miles.

  - **CSVC, guards, and other physical controls**
    The place is manned 21 hours a day. There are bars on the windows. CSVC is available and used.

- **What is the availability of the bonded \ vault \ Safe to transport service?**
  - **Is the facility close on weekend, holidays and dose it operates during specific hours of the day?**
    Closed on holidays and weekends, but the access procedure to the tapes is valid 24/7.

  - **What is the emergency routine for return delivery media tape?**
    Call the 800 number, whoever has the appropriate access level can order a tape by number (currently Ron, Jacky and Charlie).

  - **Can the Media accessed in the necessary time frame?**
    Tape will arrive within 2-4 hours.

- **Facility Safety and security conditions**
  - **Fire detection and suppression system**
    Gas based suppression system (FM-200)

  - **Dose the facility provide temperature and humidity monitoring and control?**
    Yes. Temperature is keep between 68 and 71 degrees. Humidity levels are monitored. System is alerting in cases of change.

  - **Media transportation condition**
    - IronMountain has vans that transport the Media; the vans are recent models that are regularly maintained.
    - All employees sign “driver rules document” and “DataBank NDA - non disclosure agreement”
    - All IronMountain vans are fitted with a steel safe locking system

  - **Intrusion detection**
    - Windows are equipped with pressure based alarm
    - Video cameras are monitoring access to the building
    - Bars on all windows.
    - Badges for all employee

  - **Access control**
    - You must swipe your badge to get access to the storage room. All entrances are logged.
    - Entrances not scheduled/expected are triggering alerts .
    - No two customers are allowed to visit at the same time

  - **How do our tapes secured from other clients? Is confusion possible?**
    No. A scanner is verifying the correct box is delivered. The container is scanned five times during the transfer process.

- **Organizational policies and procedures**
  - **Does the company have employee screening procedures**
    Yes, detailed screening procedures are performed including random drug tests.

  - **Does the company provide adequate segregation of duties?**
    Yes. Monitoring is done by people different than the transporters and account reps.

  - **Does the company have an adequate security policy?**
    yes.

  - **Does the company follow change control procedures?**
    Yes, for process changes.

Written By: Erez Batat

SFA—Off-Site Store Visit Report—DataBank

Mercury Off-Site Storage - Visit Site Report

Document Title	Mercury off-Site Storage – Visit Site Procedure
Document Number	001
Related Documents	Off-Site visit yearly Procedure \ Backup tapes delivery procedure \Backup tapes delivery weekly report

Off-site Storage Company: DataBank Israel

Scheduled:
May 18 2004

Visit done by:
Shlomo Boussidan

Steps and Question Reviewed during visit:

- **Off-site company service description**

  - **Company Details**:
    - Company name: **DataBank**
    - Address: **7 Hamasger St. Or Yehuda 60223** (office and vault)
      - **Tel Aviv Office, 24 Saadia Gaon St. Tel Aviv**
    -
    - Phone: +**972 3 634 4088**
    - Fax**: +972 3 634 4078**
    - email : info@databank.co.il
    - Website: www.databank.co.il
    - Contact persons:
      - **Anthony Harris**, +972-56-816-206, mail: Anthony@databank.co.il

- **Evan Lever**, +972-56-816-207, mail: evan@databank.co.il

Company Profile:
DataBank protects business data and providing specialized offsite backup tape storage and messenger service and insurance against permanent loss of data in case of disaster occur or files lost. The service that DataBank provides is considered a normal business practice used by companies around the world. DataBank founded in May 2002, and had 10 employees and strict confidentiality structure and agreements with all its staff and clients ensuring that their data will be secured in the correct and confidential manner. DataBank services over 170 Customers. DataBank is also software source code escrow agent have escrow agreements in place with companies in the UK, Germany, Switzerland, USA and Israel.

- **Physical layout of the facility**
  - **Description of the environment**:
    - DataBank locates in industrial and business aria in Or Yehuda, the vault facility locates in the Building shelter (the same building of the office in Or Yehuda). The building managed by Security Company 24/7. Company name "Spekurity", Phone: 03-538 2222.
    - The vault is connected directly to the security company via a secured telephone line backed up with a radio transmitter.
    - During the evenings and weekends, if the vault door is opened, the security company calls a list of numbers to identify if there is a problem
  - **Access to the facility**:
    - Access is from the underground parking. Special aria is restricted for DataBank and bordered in front of the entrance of the Vault.
  - **Check for Obstacle in physical layout**. No obstacle
    - Distance from Mercury building: 5 KM ~

- **Availability of the bonded \ vault \ Safe to transport service**
  - **Is the facility close on weekend, holidays and dose it operates during specific hours of the day?**
    - The Facility working 6 days a week working hours (closed on Saturday). For special cases DataBank can be reach by one of the mobiles listed above.
  - **What is the emergency routine for return delivery media tape?**
    - Any hour during the week media can be delivered.
    - A call from Mercury Authorized Person for taking Media would be done by Shlomo Boussidan & Alex Gurevich) Any other person who call to take any Media will be confirm by return call from Data Bank to Shlomo Boussidan and sending Mail request to info@databank.co.il .
  - **Can the Media accessed in the necessary time frame?**
    - DataBank committed to deliver any Media in their Facility not more then 3 hour.

- **Facility Safety and security conditions**
  - **Intrusion detection**
    - **The vault has the following internal security devices**
      - Seismic Detectors to detect vibration
      - Motion Detectors
      - Reinforced magnetic sensor on the entry doors to the vault
      - Pama entry code control system
      - Temperature detectors
  - **Fire detection and suppression system:**
    - Smoke Detectors – FM200 Gas System
  - **Access control**
    - The Vault has restricted access. The codes and combinations are only known by 2 directors and the vault manager of the Company
    - Employees are only permitted in the vault under the supervision of the directors or the vault manager
    - The Vault door is a reinforced steel bank room vault door with a double combination locking system

- The DataBank Or-Yehuda building is shared with its onsite Security Company “Spekurity” ensuring onsite response 24/7. The vault and surrounding areas are monitored by CCTV in the Spekurity Control Room.

- **Media transportation condition**:
  - DataBank had vans that transport the Media, the vans are recent models that are regularly maintained.
  - All employees sign “driver rules document” and “DataBank NDA - non disclosure agreement”
  - All DataBank vans are fitted with a steel safe locking system.

Written By: Harry Magnan