Audit of System Backup and Recovery Controls for the City of Milwaukee Datacenters

MARTIN MATSON
City Comptroller

AYCHA SIRVANCI, CPA
Audit Manager
City of Milwaukee, Wisconsin

July 2014

TABLE OF CONTENTS

Martin Matson
Comptroller

John M. Egan, CPA
Deputy Comptroller

Glenn Steinbrecher, CPA
Special Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Office of the Comptroller

July 31, 2014

Honorable Tom Barrett, Mayor
The Members of the Common Council
City of Milwaukee
Milwaukee, WI 53202

Dear Mayor Barrett and Council Members:

The attached report summarizes the results of our Audit of System Backup and Recovery Controls for the City of Milwaukee datacenters. The scope of the audit included the six City-owned and operated datacenters. The objectives of the audit were the following: assess whether datacenter controls over the system-backup process are performed in accordance with policy, procedures, and best practice; verify whether the backup tapes include the operating system, applications, database, and support files required for a full system restoration; determine whether a full system-restoration test has been performed within the past two years; and assess the datacenters' capacity for a timely and full system restoration in the event of a business disruption or disaster.

Overall, the audit concluded that the internal controls in place over the system backup and recovery controls for the City of Milwaukee datacenters are adequately designed and operating effectively. However, for some of the controls cited within this report, gaps exist in the control design or operational effectiveness that exposes certain datacenters to risk. This report only provides summary information on datacenter activities in order to protect the confidential and sensitive nature of City datacenter operations. Detailed findings and recommendations were sent to all datacenter managers and a written management response was received indicating their agreement. The report identifies seven recommendations to address these issues.

Audit findings are discussed in the Audit Conclusions and Recommendations section of this report. Appreciation is expressed for the cooperation extended to the auditors by the management and staff of the City's datacenters.

Sincerely,

Aycha Sirvanci

Aycha Sirvanci, CPA
Audit Manager

AS:gjl

I. Audit Scope and Objectives

The scope of the audit included the controls over the system backup and recovery process for the six City-owned and operated datacenters. The audit focused on the internal controls over the system-backup process, administered by the datacenters, including the secure, offsite storage of data. In addition, the audit focused on the datacenters' capacity for a timely and accurate system restoration, including operating systems, applications, databases, and supporting files in the event of an actual business disruption or disaster event. Lastly, the audit focused on the adequacy of the datacenters' overall information technology (IT) governance process.

The datacenters, within this audit's scope, included: the Information Technology Management Division (ITMD); the Police and Fire Departments (who share one datacenter); Department of Public Works -Water Works; Municipal Court; the Library; and the Assessor's Office. The audit, executed during April and May of 2014, covered the datacenters' activities for the past twelve months. The City's PeopleSoft application was outside of this audit's scope because this system is hosted by an offsite vendor. The City's networking and switch closets, and third party vendors that provide data-processing services, were outside of this audit's scope, as well. The City Public Health Laboratory datacenter was audited in February 2014, and therefore excluded. Furthermore, the audit did not include an evaluation, or testing, of the City's Business Continuity Plan or Disaster Recovery Plan.

System backup and recovery controls are considered standard provisions to provide reasonable assurance that a datacenter will be able to recover from loss or destruction of data-processing facilities, hardware, software, or data. These continuation provisions include the retention of copies of data files and software, arrangements for access to backup hardware on short notice, and tested recovery plans.

The audit evaluated the datacenters using the criteria of backup-control standards, as established by the Information Systems Auditing and Control Association.

The audit's methodology included developing an understanding of each datacenter's process and internal controls for the periodic backup of system files, offsite storage, physical security, and system-restoration testing, as well as security-access measures surrounding the backup software. The audit procedures were developed to evaluate the processes and controls, in order to meet the audit's objectives. These procedures included process walk-throughs, inspection of relevant control documentation, system hardware and software analysis, security-configuration reviews, and detailed tests of controls. Specific procedures and tests were conducted to:

- Assess whether each datacenter complies with policy, procedures, and best practice;
- Determine if a sample of performed daily backups ensures proper documentation, frequency, and inclusion of the operating system, applications, database, and support files deemed necessary for a full system restoration;
- Verify that the backup-tape process is automated and pre-programmed to run on a regular schedule, whereby issuing automated success or failure notifications to the system manager;
- Confirm that access to backup-tape software is restricted to authorized personnel only and that system access is granted using a least-privilege criteria, based on job-level responsibilities;
- Examine the adequacy of a system-restoration test performed every two years; and
- Assess the adequacy of each datacenter's IT governance process.

The objectives of the audit were to:

- ➢ Assess whether the datacenter controls over tape backup, offsite storage and system restoration procedures are performed in accordance with City policy and best practice;
- ➢ Verify whether the backup-tapes include the operating system, applications, database, and support files required for a full system restoration;
- ➢ Determine whether a full system-restoration test has been performed within the past two years; and
- ➢ Assess each datacenter's capacity for a timely and fully functional system restoration in the event of a business disruption or disaster and the adequacy of the datacenter policy and procedures.

The audit was conducted in accordance with generally accepted government auditing standards (GAGAS). Those standards require that the audit obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. The Audit Division believes that the evidence obtained provides a reasonable basis for the audit's findings and conclusions based on the audit objectives.

II. Organization and Fiscal Impact

The City's IT governance is centralized under the ITMD within the City's Department of Administration. While IT services are primarily based in ITMD, there are five other separate datacenters serving the City; and these IT entities have individually operating domains, applications, and databases. These datacenters are comprised of the Police and Fire Department, Municipal Court, Water Department, Library, and Assessor's Office.

The City's datacenters utilize servers ranging from a Z-series mainframe to Intel servers. The servers are deployed on Windows Server, Linux, and Unix-based operating systems. The servers run applications, such as property assessment, tax collection, water billing, legislative tracking, and municipal-court violations, as well as Police/Fire dispatching, and records management. The City owns its own wide area network (WAN), which is centralized, maintained, and managed (including firewalls) by ITMD. This WAN connects 5,000+ City workstations with its several City datacenters.

The mission of each datacenter is to support and maintain its respective department's information, processing systems (including financial and operational applications), desktop operations, and departmental networks. The ITMD provides hardware support for the City's Internet site and web-based applications while ensuring the security of City networks, systems, and data. It also operates a centralized system that maintains and provides data which support critical departmental activities. The datacenters are City owned and operated facilities, used to house computer systems and associated components, such as telecommunications and storage systems. They include backup-power supplies, redundant data communications connections, environmental controls, and various security devices in highly secured rooms.

City datacenters must provide internal and external users with the capacity for data confidentiality, data integrity, and data availability. Data confidentiality means that appropriate controls should be in place to authorize and authenticate users, based on job-level responsibilities and the least-privilege access principle. Data integrity involves the accuracy of the system's reported results. Data availability involves the ability to access data easily, where and when needed, and, most importantly, to minimize or eliminate system downtime, business disruption, or a disaster event, all of which could lead to lost productivity and service interruptions to citizens and City personnel.

A datacenter's capacity for data availability and continuity involves the proficiency to restore lost data easily and to minimize or eliminate system downtime and from a business disruption event that could lead to lost productivity, costly data recovery, and severe service interruptions to citizens. It is essential for the City's datacenters to have the capacity for a timely and fully functional system restoration of the operating system, applications, database, and supporting files, in the event of an actual business disruption or disaster event. The datacenters are the foundation for City operations and for supporting critical citizen services. Thus, data availability and continuity are essential for meeting program missions, objectives, and goals.

III. Audit Conclusions and Recommendations

With regard to the exceptions noted during the audit, this report only provides summary information on datacenter activities, in order to protect the confidential and sensitive nature of City datacenter operations.

Overall, the audit concluded that the internal controls in place over the datacenters are adequately designed and operating effectively. However, for some controls, cited within this report, there are gaps in the control design or operational effectiveness that expose certain datacenters to risk. With regard to exception monitoring and documentation, four datacenters had processing exceptions, ranging from moderate to low risk, and one datacenter was not able to produce the appropriate documentation of daily backup activity. Access controls over the backup-software systems are in compliance with City Password Policy, except where only one shared user-access account for backup-software access existed within each of five datacenters. In addition, five datacenters do not have an adequate written policy and procedure, governing the backup requirements and timelines, and one datacenter is non-compliant with the City’s Cloud Computing Policy. The IT governance process over the datacenters is adequate, with the exception of four datacenters requiring some improvement in periodic system-restoration testing and one datacenter requiring a Class ABC fire extinguisher. This report identifies the following seven recommendations to address these issues and the number of datacenters impacted. As previously noted, there are a total of six City owned and operated datacenters.

1. Four datacenters should monitor the daily-exception report to identify the nature of all exceptions noted and eliminate them from the report.
2. One datacenter should create and maintain documentation of system-backup activity.
3. Five datacenters should create datacenter policy that governs and addresses essential system backup and recovery elements.
4. Five datacenters should configure each Administrator’s access to have a unique user ID and password for the backup software.
5. One datacenter should obtain the review and approval of the Chief Information Officer regarding the use of a cloud-based backup solution.
6. Four datacenters should perform the datacenter system-restoration test every two years.
7. One datacenter should obtain a Class ABC fire extinguisher for the datacenter and have the required inspections performed annually.

The identified exceptions, along with their corresponding recommendations for improvement, have been communicated to the appropriate City personnel and implementation is underway. Additional details regarding the recommendations for improvement are provided in the remaining sections of this report.

A. Backup-Exception Monitoring and Documentation

Backup-Exception Monitoring

Based on City datacenter policy and best practice, the Administrator should review the backup success or failure status on a daily basis and take timely action to identify and resolve exceptions. If reported exceptions are designated as being truly false positives, then eliminating the false positives from the exception report will indicate only true exceptions that need further research and resolution. For some datacenters, additional research and monitoring is needed to determine whether these exceptions can be identified with certainty, resolved, and eliminated from the daily-exception report.

After a sample of fifteen days of system backups were tested for proper backup evidence, the exception reports revealed that four datacenters had daily processing exceptions, ranging from moderate to low risk. Some exceptions occurred repetitively and without timely Administrator research and resolution.

Recommendation 1: Four datacenters should monitor the daily-exception report to identify the nature of all exceptions noted and eliminate them from the report.

The objective of monitoring is to identify the root cause of the exceptions and eliminate them from future reports. If necessary, the backup-software vendor should be consulted with to obtain configuration information on how to resolve false positives and prevent them in the future. The exception-reporting process is most effective and efficient when only true exceptions, in need of timely research and resolution, are reported.

Documentation of Backup Activity

Backups of the operating system, applications, database, and support files should be performed daily, while documentation of these backups should be retained for at least three months. Daily success or failure notices should be generated as well. Documentation that verifies whether backup exceptions are resolved on a timely basis should be maintained, along with verification of offsite data storage. One of the key responsibilities of a database administrator is to prepare for the possibility of media, hardware, and software failure, as well as to recover databases after a disaster. Should any of these failures occur, the major objective is to ensure that the databases are available to users within an acceptable timeframe, while still ensuring that there is no permanent loss of data.[1]

[1] *Information Systems Audit and Control Association Journal, Volume 1* (2012), 1.

One datacenter was not able to produce documentation of daily backup activity, offsite storage, or daily exception-monitoring reports for the past twelve months. It could not be determined that all of the required backup activity had taken place due to the lack of documentation. The datacenter began using the Carbonite Server Backup software in early 2014. Prior to the initial use of the Carbonite Server Backup software, documentation of daily backup activity was not available at the time of the audit. Furthermore, after the conversion to Carbonite, the software has not been able to produce appropriate documentation of daily backup activity and success or failure exception notices. The datacenter management is currently working with the vendor to resolve the matter.

Recommendation 2: One datacenter should create and maintain documentation of system-backup activity.

The documentation should include backup activity for the past three months, evidence of offsite storage, and whether the backup-storage medium includes the operating system, applications, database, and support files required for a full system restoration. Additionally, the documentation should include whether daily success or failure notices were generated and whether backup exceptions were resolved on a timely basis.

B. Policies and Procedures

Policy and Procedure

The City's datacenters should have a written policy that governs activities, requirements, and timelines. Management should deploy control activities through policies that establish what is expected and through procedures that put policy into action.

Points of Focus[2]

- Establish policies and procedures to support deployment of management's directives. Controls are built into business processes through specific policies and procedures.

[2] *An Overview of the COSO 2013 Framework, Principle Number 12 Policy – Points of Focus* (August 8, 2013).

- Establish responsibility and accountability for executing policies and procedures. Management assigns responsibility and accountability for the controls in the business unit or function where the risk resides.
- Responsible personnel perform controls in a timely manner.
- Responsible personnel take corrective action by investigating and acting on matters identified as being a result of executing the control.
- Competent personnel, who possess sufficient authority, perform controls with diligence and sustained focus.
- Management periodically reassesses policies and procedures, in order to determine the continued relevance of established controls, and provides updates when necessary.

Five datacenters do not have a written policy governing the datacenter's backup activities, requirements, and timelines. Not utilizing a well-developed system of control-related policies, procedures, and best practices risks the consistent completion of Management's goals, objectives, and required operations, as well as the disruption of critical City services to its citizens and personnel.

Recommendation 3: Five datacenters should create datacenter policy that governs and addresses essential system backup and recovery elements.

Policy Essentials:

- Designated frequency of backups.
- Designated retention period of backed-up data.
- The requirement of offsite tape and disk storage at a defined distance from the primary datacenter.
- The access and protection of tapes and disks in offsite storage facilities.
- The requirement of determining what is backed up, such as the operating system, applications, database(s), and support files.
- Requirement for documented backup procedures.
- Backup-exception monitoring, follow up, and resolution.
- The requirement of system-recovery tests every two years, in accordance with best practice and the requirement for documented system-recovery test results.

- Recovery procedures, resources, options, vendors, and service-level agreements (if applicable).

The datacenter policy should address the required frequency of backups, what systems, applications, and databases are to be backed up, offsite storage, a requirement for written backup procedures, and a required recovery test performed every two years.

Password Policy

City Password Policy requires Administrators to have individual user accounts and passwords, when accessing the backup software.[3] The best-practice approach is for Administrators to possess separate user ID's and passwords, while performing their individual job responsibilities. This approach is beneficial for user-activity tracking and job accountability, as well as allowing for easy termination of system-user access when an employee leaves City service.

Five datacenters have from two to four Administrators sharing one user account and password for the backup-software access, which is non-compliant with City Password Policy and best practice. System activity cannot be tracked for each individual user, and the practice of shared user accounts and passwords is in violation of City Password Policy.

Recommendation 4: Five datacenters should configure each Administrator's access to have a unique user ID and password for the backup software.

Cloud Computing Policy

Selected relevant portions of the City of Milwaukee Cloud Computing Policy, dated March 2014, are shown below:

> *Purpose:*
> *This Cloud Computing Policy is meant to ensure that cloud services are NOT used without the IT Management or CIO's knowledge. It is imperative that employees NOT open cloud services accounts or enter into cloud service contracts for the storage, manipulation, or exchange of city-related communications or city-owned data without the IT Management/CIO's input. This is necessary to protect the integrity and confidentiality of data and the security of the network.*

[3] *City of Milwaukee Password Policy* (June 11, 2011).

One datacenter uses the Carbonite Server Backup software and is non-compliant with the City of Milwaukee's Cloud Computing Policy because it has not been reviewed and approved by the Chief Information Officer. Sensitive information may not be adequately protected, leading to a breach of confidential data and a violation of the City's information security standards and policy. The Cloud Computing Policy was adopted by the Common Council on March 6, 2014. The datacenter began using the Carbonite Server Backup software on March 3, 2014. Thus, the Carbonite software was already being utilized when the new Cloud Computing Policy was adopted, but the datacenter personnel were not aware of this new policy.

Recommendation 5: One datacenter should obtain the review and approval of the Chief Information Officer regarding the use of a cloud-based backup solution.

Sufficient system documentation and evidence should be provided so that a thorough review process can be completed. Documentation of the review's outcome should also be retained for future audit purposes.

C. System Recovery Controls

System Restoration Test

Best practice criteria indicate that a system-restoration test should be performed by the datacenter every two years. The frequency of contingency-plan testing will vary depending on the essentialness of the entity's operations. Generally, contingency plans for particularly critical functions should be fully tested every two years, whenever significant changes to the plan have been made or when significant turnover of key people has occurred. It is important for top management to assess the risks of contingency-plan problems then develop and document a policy regarding the frequency and extent of such testing. Additionally, the nature and extent of system-recovery testing should be documented.

Computer backup and recovery controls are the provisions to deliver reasonable assurance that an organization will be able to recover from loss or destruction of data-processing facilities, hardware, software, or data. These continuation provisions include the retention of copies of data files and software, arrangements for access to backup hardware on short notice, and tested recovery plans.

For four datacenters, a system-restoration test has not been performed in the past two years, in accordance with the recommended best practice approach outlined in the *Federal Information System Control Audit Manual*.[4]

Recommendation 6: Four datacenters should perform the datacenter system-restoration test every two years.

A system-restoration test in the test environment should be performed every two years to accomplish the following:

1) Verify that all files needed to restore the system to full production mode are backed up and available;
2) Demonstrate that recovery activity can be completed within the time constraints required by City personnel and citizens who depend on the system; and
3) Assess that datacenter personnel possess the necessary training and resources to ensure continuity of operations after a business disruption or disaster event.

D. Environmental Controls

Datacenter Fire Suppression

Best practice suggests that each City-owned datacenter contain an annually-inspected Class ABC fire extinguisher within its server room. Currently, in the event of a datacenter fire, a method to reduce and extinguish the fire is not readily available for one datacenter. This could result in damage and loss of essential datacenter operations and data, which are vital to the City of Milwaukee and its citizens.

One datacenter does not have a Class ABC fire extinguisher located within its server room, and does not comply with the best practice approach for fire suppression.

[4] *GAO – Federal Information System Control Audit Manual* (February 2009), page 333.

Recommendation 7: One datacenter should obtain a Class ABC fire extinguisher for the datacenter and have the required inspections performed annually.

A chemical-based fire suppression system for information technology hardware and software is consistent with best practice.