AUDIT REPORT
Denver County Court
IT General Controls

August 2018

Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O'Brien, CPA
Denver Auditor

The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies and contractors for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor, and the public to improve all aspects of Denver's government.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City's finances and operations, including the reliability of the City's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

Timothy M. O'Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

Audit Management

Timothy M. O'Brien, CPA, Auditor
Valerie Walling, CPA, CMC®, Deputy Auditor
Heidi O'Neil, CPA, CGMA, Director of Financial Audits
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Manager

Audit Team

Nicholas Jimroglou, CISA, Lead IT Auditor
Karin Doughty, CISA, Senior IT Auditor
Brian Cheli, CISA, CISSP, Senior IT Auditor

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000 ◆ Fax (720) 913-5247

Or download and view an electronic copy by visiting our website at: www.denvergov.org/auditor
Audit report year: **2018**

Timothy M. O'Brien, CPA
Auditor

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202
720-913-5000 • Fax 720-913-5253 • www.denvergov.org/auditor

August 16, 2018

AUDITOR'S REPORT

We have completed an audit of Denver County Court's information technology general controls. As described in the attached report, our audit revealed that Denver County Court's IT department needs to update its policies and procedures, improve data center security, and enhance the backup and recovery process.

Through stronger policies and procedures, Denver County Court's IT infrastructure will be able to ensure data is protected and information technology is operating as efficiently and effectively as possible. Our report lists several related recommendations. In addition, we identified security related findings which have been communicated separately to management of Denver County Court for their remediation.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, *General Powers and Duties of Auditor*, and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We extend appreciation to Technology Services, Denver County Court, and the personnel who assisted and cooperated with us during the audit.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

Denver County Court IT General Controls

August 2018

Objective

The objective of the audit was to evaluate the operating effectiveness of the internal controls for Denver County Court's information technology.

Background

Denver County Court is Denver's judicial branch of government and handles a variety of cases including civil, small claims, traffic, and criminal cases. Denver County Court's IT department manages and maintains Denver County Court's IT infrastructure, systems, and data, all while providing 24/7 helpdesk support.

REPORT HIGHLIGHTS

Highlights

We identified opportunities to improve the information technology general controls in place at Denver County Court. Our audit included a review of the controls over user access, backup and recovery, change management, and those at the data center. We noted opportunities for improvement in three areas: One, the existing policies and procedures can be strengthened by updating them to reflect current practices and to more clearly identify the existing control framework. Two, the data center environmental controls are lacking, putting vital Court data at risk for destruction in the event of water or fire damage. Finally, the backup processes were not based on best practices, putting critical Court data at risk for loss or theft.

For a copy of this report, visit www.denvergov.org/auditor or contact the Auditor's Office at 720.913.5000.

TABLE OF CONTENTS

BACKGROUND

Overview of Denver County Court

Denver County Court is Denver's judicial branch of government and handles a variety of cases including civil, small claims, traffic, and criminal cases. Presiding over and managing these cases are 17 judges, 15 magistrates, and 245 staff members, all of whom are supported by an internal IT department. This is somewhat unique as most City departments and agencies use Technology Services to manage their IT processes and infrastructure. The Court IT department started out by providing the capability to develop the following applications that we reviewed:

THEMIS is the Court developed case management system. This software is used by Court staff to manage all Court cases. This functionality includes tracking fines, fees, judgements, and details related to the case and communicates the judges' entry to the Receipting System in real time. From 2013 through 2016, Denver County Court handled an average of over 248,000 cases per year. These cases are tracked through THEMIS.

The Receipting System is the Court developed cash receipting system. This software is used by Court staff to manage all payments received. Cashiers do not have to make judgements about where to allocate the fees they collect. This is automatically prioritized in the THEMIS system. When cashiers update the payment in the receipting system, THEMIS is automatically updated. For example, settlement payments to plaintiffs, and victims' compensation or victims' assistance payments are of higher priority in THEMIS than payments due to the County Court or the City.

The Accounting System is the Court developed accounts payable system. This software is used by Court accounting staff to issue payments for bond and restitution checks. When the receipting system processes a restitution payment, the accounting system automatically prepares a check that moves to the queue for payment.

Denver County Court's IT department has 10 full-time staff, including IT systems administrators, developers, and an IT Director. Together they manage and maintain Denver County Court's IT infrastructure, systems, and data, all while providing helpdesk support 24 hours per day, 7 days per week. These services include development of the software used by the Court. Software development requires a very specific set of internal controls that are called change management controls. When an organization has the ability to make changes directly to the underlying software code it has the ability to change how transactions are processed. The ability to make these types of changes requires controls to verify that only properly approved and tested changes are put into the actual operating version of the software being used. The next major function of the IT team is to manage user access. User access includes the processes to approve, apply, verify and remove individual users' access to all of the systems used by the Court including email, THEMIS, the receipting system and the accounting system, among others. User access requires controls to make sure that users only have the ability to perform the duties required by their job and that these duties do not create the potential for a single user to create, approve and complete any single transaction. The IT department is responsible for key IT operations including backup of all data files and managing the physical access to critical IT hardware such as servers and network devices, which are housed in the Court data center.

OBJECTIVE

The objective of the audit was to evaluate the operating effectiveness of the internal controls for Denver County Court's information technology department for change management, user access, data backup and the data center.

SCOPE

The scope of this audit focused on Denver County Court's case management, accounting and receipting systems covering the period of 2016 through 2017. Specifically, the audit reviewed access controls, change management, backup and recovery, and the security and environmental controls for the data center.

METHODOLOGY

We applied multiple methodologies to gather and analyze information pertinent to the audit objective and scope, which included the following:

- Interviewing personnel from Denver County Court's IT department to gain an understanding of their roles and responsibilities
- Reviewing and assessing relevant policies and procedures related to user access, change management, backup and recovery, and data center security and environmental controls
- Assessing the IT general controls in place for the key applications that handle court cases and finances
- Observing and reviewing data center security and environmental controls
- Testing of a random sample of transactions to determine whether the existing controls are functioning appropriately
- Performing walkthroughs of key processes with personnel from Denver County Court's IT department

FINDING

The Internal Control Structure of Denver County Court's Information Technology Systems and Data Should Be Improved

In assessing the internal control structure for Denver County Court's systems and data, we identified three areas for improvement. First, several policies and procedures should be enhanced in user access, system backups, and change management. Second, we found several opportunities to strengthen the backup processes, which mitigate the risk of losing vital Court data. Third, we have several suggestions for improving the environmental controls for the data center. By implementing the resulting recommendations, the Court's IT department will greatly reduce the likelihood that the Court will be faced with infrastructure damage or loss or exposure of information.

Policies and Procedures Need Improvement

In assessing the policies and procedures that are used to operate the Court's IT systems and data, we identified areas where Denver County Court's IT department can enhance its internal control structure. Specifically, we identified ways to improve user access, system backups, and change management policies to align with standards issued by the National Institute of Standards and Technology (NIST).[1] We identified the following concerns with the current policies and procedures:

1. The backup policies do not include requirements for backup of the source code for the Court's case management accounting, receipting, and other Court-developed software.
2. The backup policies do not describe the media type used for backups or the media backup rotation cycles.
3. The backup policy does not reference the current offsite backup storage provider.
4. The user access policies do not include the timeframe to communicate changes in user access to the Court's IT department.
5. The user access policies do not include a requirement that user access changes should be provided via email and include the details of the requested changes to a user's access.
6. The user access policies do not address exceptions to the termination policy.
7. The password policy does not cover all relevant applications.
8. The user access policies and procedures do not include the details for handling contractor user access with a review process to remove such access when the contractor no longer needs it.
9. The change management policies do not address the documentation details and timelines for emergency changes to the applications.
10. The Court does not have a written policy and procedure in place for physical access to the data center or for monitoring for water or fire damage to the data center.

[1] The National Institute of Standards and Technology, or NIST, is a part of the U.S. Department of Commerce. The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

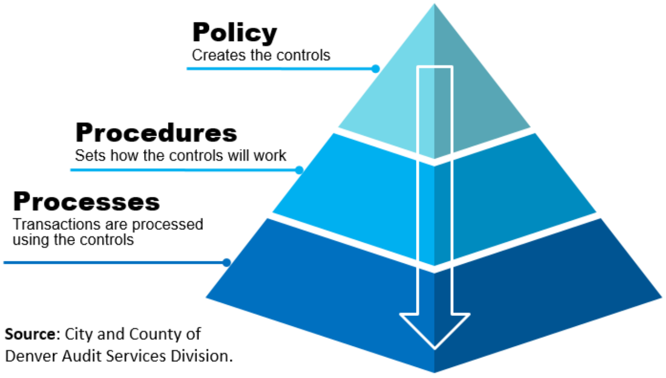
NIST Special Publication 800-53, Revision 4, provides guidance on securing and reviewing user access and implementing changes into production. For securing and reviewing user access, the guidance specifies that organizations should document adding, changing, or removing user access to individuals. It also specifies that organizations should develop, document, and disseminate an access control policy. For implementing changes into production, the guidance specifies that organizations should have appropriate segregation of duties so that the individuals developing code are independent from those with the ability to implement the code into production.

NIST Special Publication 800-34, Revision 1, provides guidance on the policy requirements for backup methods and offsite storage. Policies should specify the minimum frequency and scope of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency with which new information is introduced. Data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. Data may be backed up on magnetic disk, tape, or optical disks, such as compact disks (CDs). The specific method chosen for conducting backups should be based on system and data availability and integrity requirements. These methods may include electronic vaulting, network storage, and tape library systems.

Insufficient Policies and Procedures Jeopardize the Confidentiality, Integrity, and Availability of Data

As Figure 1 shows, policies provide the overall structure for the specific actions and functions that need to occur. Procedures document the detailed steps needed to implement the policies into the way the processes work. A lack of policies and procedures for IT controls jeopardizes the confidentiality, integrity, and availability of the entire organization's information systems and data because there is no consistency in how critical functions are performed.

Figure 1: How Policies, Procedures and Processes Interact


Policy
Creates the controls
Procedures
Sets how the controls will work
Processes
Transactions are processed using the controls

Source: City and County of Denver Audit Services Division.

Further, weak policies and procedures that do not provide enough guidance could lead to unauthorized individuals gaining access to critical data. For example, in 2012, Memorial Healthcare Systems, a non-profit hospital chain based in Miami, Florida, reported that former employees had improperly accessed electronic protected health information. Investigators determined that inadequate access control policies for protected data, failure to remove access of former employees, and failure to review logs and access records led to the unauthorized access of the names, birth dates, and Social Security numbers of approximately 80,000 people. As a result, some of the data was used to commit identity theft, and the organization paid a $5.5 million HIPAA breach settlement and agreed to implement a corrective action plan.[2]

Incomplete system backup policies and procedures create a risk that critical data may be lost due to data corruption or data loss caused by computer viruses. For example, the police

[2] "Poor Management Leads to $5.5 Million HIPAA Penalty," Aldrin Brown, Channel Futures, accessed June 19, 2018, http://www.channelfutures.com/strategy/poor-access-management-leads-55-million-hipaa-penalty.

department for Cockrell Hill, Texas, lost eight years' worth of digital evidence because of a ransomware attack. Data could not be recovered from backups, as the backup procedure kicked in shortly after the ransomware took root and backed-up copies of the files, but they were already infected. The department was forced to recover the lost data using their existing hard-copy documentation.[3]

Finally, a lack of change management and IT operations policies and procedures could result in downtime and loss of critical systems and data. For example, a Tesla employee recently admitted to circumventing change management practices, making changes to computer code of the company's manufacturing operating system and exporting large amounts of highly sensitive data.[4] If appropriate controls had been in place over the code review and approval process, along with appropriate segregation of duties, there is a likelihood that this unauthorized activity would have been detected sooner.

RECOMMENDATION 1.1

Update Existing Policies and Procedures Using the NIST Framework – The Denver County Court's IT department should update its IT policies and procedures for user access and change management based on the National Institute of Standards and Technology's 800-53 standard and the system backup policies and procedures based on the National Institute of Standards and Technology's 800-34 standards as soon as possible. These updated policies and procedures should address the following areas:

1. Reflect the current operational practices
2. Clearly identify each control in place
3. Specify who performs each control
4. Describe how the performance of each control should be documented
5. Establish the retention period for control documentation

Agency Response: Agree, Implementation Date – June 1, 2019

Environmental Controls over the Denver County Court's Data Center Can Be Strengthened

A data center is a central repository that houses computing facilities like servers, routers, switches, and firewalls, as well as supporting components like backup equipment, fire suppression facilities, and air conditioning. Auditors tested the controls related to environmental protection of the data center and identified several issues that could cause the loss of critical data. The Court's critical judicial records and processed financial transactions are stored in physical computer servers, which are kept in the Court's data center.

[3] "Police lost 8 years of evidence in ransomware attack," Darlene Storm, Computerworld, accessed July 2, 2018, https://www.computerworld.com/article/3163046/security/police-lost-8-years-of-evidence-in-ransomware-attack.html.

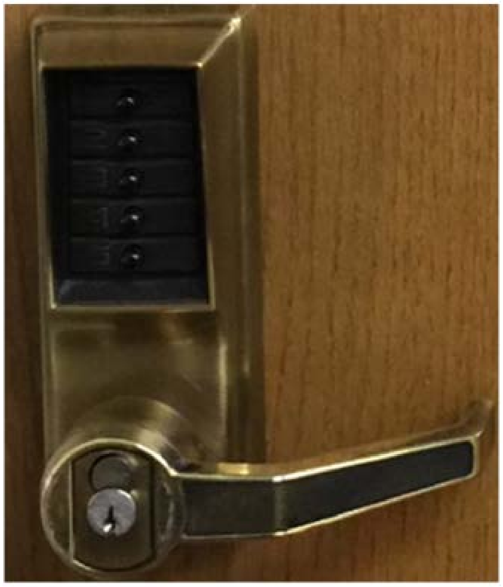
[4] "Elon Musk: Tesla Worker Admitted to Sabotage", Chris Isidore, Julia Horowitz, CNN Tech, accessed June 25, 2018, http://money.cnn.com/2018/06/19/technology/tesla-fire-musk-note/index.html.

Environmental controls mitigate data loss by ensuring that computer servers are protected from excessive heat, water damage, and fire hazard and supplied with the appropriate power. Environmental controls are essential to data center operations because of the sensitivity and high cost of the critical IT infrastructure. These controls include:

1. Sufficient air conditioning to prevent computer or network hardware form overheating
2. Water detection controls to alert IT staff in the event of water damage to critical hardware
3. Humidity monitoring controls to alert IT staff in the event humidity levels exceed the optimal level required by the critical hardware
4. Fire detection and suppression systems to identify and extinguish possible fires
5. Providing uninterrupted power to critical hardware from an uninterruptible power supply using a combination of battery backup and a separate emergency generator
6. Location of system components to minimize potential damage from water, fire, or other environmental threats

The Court's data center lacks many critical environmental controls, including for water, humidity, and fire detection and suppression controls. Specifically, there are no water or humidity monitoring systems. IT staff would only become aware of water or humidity problems when critical hardware became too damaged to function. Additionally, the data center does not have a smoke detector. The fire suppression system is limited to a wall-mounted, hand-operated fire extinguisher, which at the time of our observation was more than one year past its tested certification for operation. In addition, the location of the fire extinguisher might make it inaccessible during a fire because a user would need to pass the server rack to reach it. Finally, because the data center is secured with a combination key and keyless entry system, accessing the data center requires knowledge of the cipher lock code, which is limited to certain personnel due to legitimate security concerns. See Figure 2 for an example of a cipher lock. Therefore, in the event of a fire or water event, only certain facility staff would be able to enter the data center to respond to such emergency conditions.

Figure 2: Cipher Lock Example



Source: City and County of Denver Audit Services Division

NIST offers extensive guidance on the steps necessary to ensure environmental protection of sensitive IT equipment. If environmental protections are not used, critical IT equipment and data may be lost.

RECOMMENDATION 1.2

Relocate Data Center – Denver County Court's IT department should work with Technology Services to move the Court's computer servers to the City's existing data center colocation facilities as soon as possible.

Agency Response: Disagree

The Denver County Court's IT Backup Process Can Be Strengthened

Auditors also detected weaknesses in the process used for backup and recovery of Court data. Court data contains a wide range of critical information, such as the judge's ruling and details for a case, Court records, fines, financial information, personal information, and criminal records. We identified the following problems with the current backup process:

1. Backups containing sensitive personally identifiable information, such as Social Security numbers, were not encrypted to protect confidentiality of the information while stored offsite.
2. The media type[5] being used for backup is fragile and subject to loss of data in the event of improper physical handling.
3. Complete restoration of data from the backup media has not been tested.
4. There are not enough sets of backup media available to provide a sufficient rotation process for backups.

The following paragraphs explain the significance of these weaknesses in the backup process.

Backups Not Encrypted – Denver County Court's IT department currently uses three sets of external hard drives as its primary backup media. The Court's data, which includes sensitive personally identifiable information, is backed up to these hard drives. Some of this data is classified under the Criminal Justice Information Services (CJIS) Security Policy, which requires strict standards for how this data is handled.[6] The CJIS Security Policy requires that this type of data should be stored using encryption to protect the confidentiality of the data. However, these backups are not currently being encrypted, putting this data at risk of exposure should the backups be lost or stolen.

Hard Drives Too Delicate for Safe Transport – Hard drives provide an inexpensive way to quickly backup and store large data sets. However, they are not designed to be used as a primary data medium that is routinely transported offsite due to their delicate nature. Hard drives use a magnetized spinning disk, which is read by a head. The disk and the head are only 0.3 microns apart—thinner than a human hair. Physical shock to a hard drive can cause the head to bounce on the disk, potentially resulting in a loss of data. Hard drives are also at risk of degaussing, which happens when the data that is stored using a magnetized disk becomes demagnetized, thus losing all of the data on the hard drive.

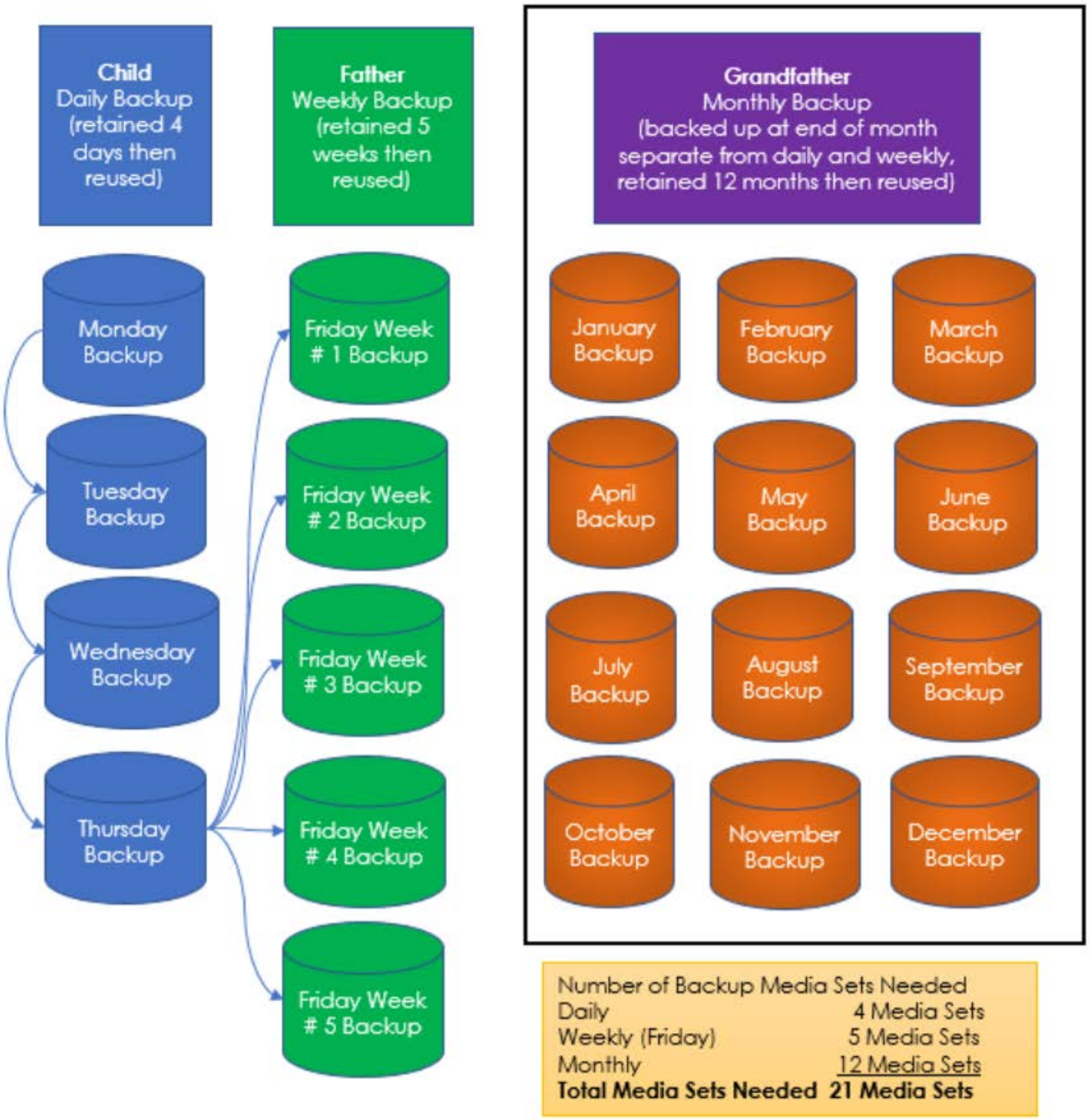
[5] Media types include diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks.

[6] Criminal Justice Information Services, or CJIS, is a division of the U.S. Federal Bureau of Investigation. The mission of CJIS is to equip law enforcement, national security, and the intelligence community with criminal justice information necessary to protect the United States while preserving civil liberties.

No Testing of Backup Integrity – The Court's IT department has not specifically tested the completeness and integrity of the backups by using the backup media to restore all the data to determine if the backups will allow for the full recovery of the Court's systems. CJIS recommends testing backup data quarterly to gain assurance that their process is working effectively. Without this testing, it is impossible to ensure that data could be recovered in the event that the data needs to be restored from the backup media.

FIGURE 3. Grandfather/Father/Child Backup Media Strategy

How the Grandfather - Father - Child Backup Strategy Works



Number of Backup Media Sets Needed	
Daily	4 Media Sets
Weekly (Friday)	5 Media Sets
Monthly	12 Media Sets
Total Media Sets Needed	**21 Media Sets**

Source: City and County of Denver Audit Services Division.

Two sets of hard drives remain in the data center to be used during the daily backup process. Auditors determined that two remaining hard drives are not sufficient to prevent the risk of media failure or malware corrupting the existing backups. The SANS Institute provides guidance on the best practices for backup media rotation strategies.[7] This best practice describes how often data should be backed up and how many different sets of backup media should be used and is referred to as the Grandfather/Father/Child data media rotation strategy. Figure 3 shows how this media rotation strategy works, requiring a minimum of 21 sets of backup media to fully implement.

The Court's IT department relies upon the local daily backups as its primary recovery process and has not fully matured its operational processes based on current technical solutions. There are two primary ways that data can be backed up. The first is the use of a physical media, which is the way the Court is currently performing backups using portable hard drive. The second way is to use a cloud based method whereby the backups are recorded into an online system or services. The cloud based backup solutions provide benefits over physical media because data can be stored offsite daily and eliminate the need to maintain and track multiple sets of physical media. The primary problem with using online backup is making sure there is sufficient bandwidth to send the data.

RECOMMENDATION 1.3

Update Backup Process – Denver County Court's IT department should use an online backup solution or set up a physical backup solution on a nightly basis using the best practice Grandfather/Father/Child backup rotations as soon as possible.

Agency Response: Agree, Implementation Date – June 1, 2019

[7] The SANS Institute is a private for-profit company that specializes in information security and cybersecurity training. SANS stands for SysAdmin, Audit, Network and Security.

RECOMMENDATIONS

We make the following recommendations to Denver County Court:

1.1 **Update Existing Policies and Procedures Using the NIST Framework** – The Denver County Court's IT department should update its IT policies and procedures for user access and change management based on the National Institute of Standards and Technology's 800-53 standard and the system backup policies and procedures based on the National Institute of Standards and Technology's 800-34 standards as soon as possible. These updated policies and procedures should address the following areas:

1. Reflect the current operational practices
2. Clearly identify each control in place
3. Specify who performs each control
4. Describe how the performance of each control should be documented
5. Establish the retention period for control documentation

Auditee Response: Agree, Implementation Date – June 1, 2019

Auditee Narrative*: The Court has developed a comprehensive Change Management tracking policy and improvements to existing user access policies. These improvements will support the National Institute of Standards and Technology's 800-53.*

The Court will improve current backup policies to align with the National Institute of Standards and Technology's 800-34 standards. The Court's focus is transitioning to Cloud based backup technology and real-time disaster recovery. Which would enable the Court to continue to operate in the event of a Denver based disaster. The Court does not want to rely on an onsite data center or physical media. A cloud solution will support the Citywide initiative of Continuity of Operations Plan (COOP).

1.2 **Relocate Data Center** – Denver County Court's IT department should work with Technology Services to move the Court's computer servers to the City's existing data center colocation facilities as soon as possible.

Auditee Response: Disagree

Auditee Narrative*: The Court will not relocate our data center. The Court will continue to make improvements the data center.*

The improvements include but are not limited to: the physical security, notification alerts for temperature, humidity monitoring, access controls, logging and fire/water prevention.

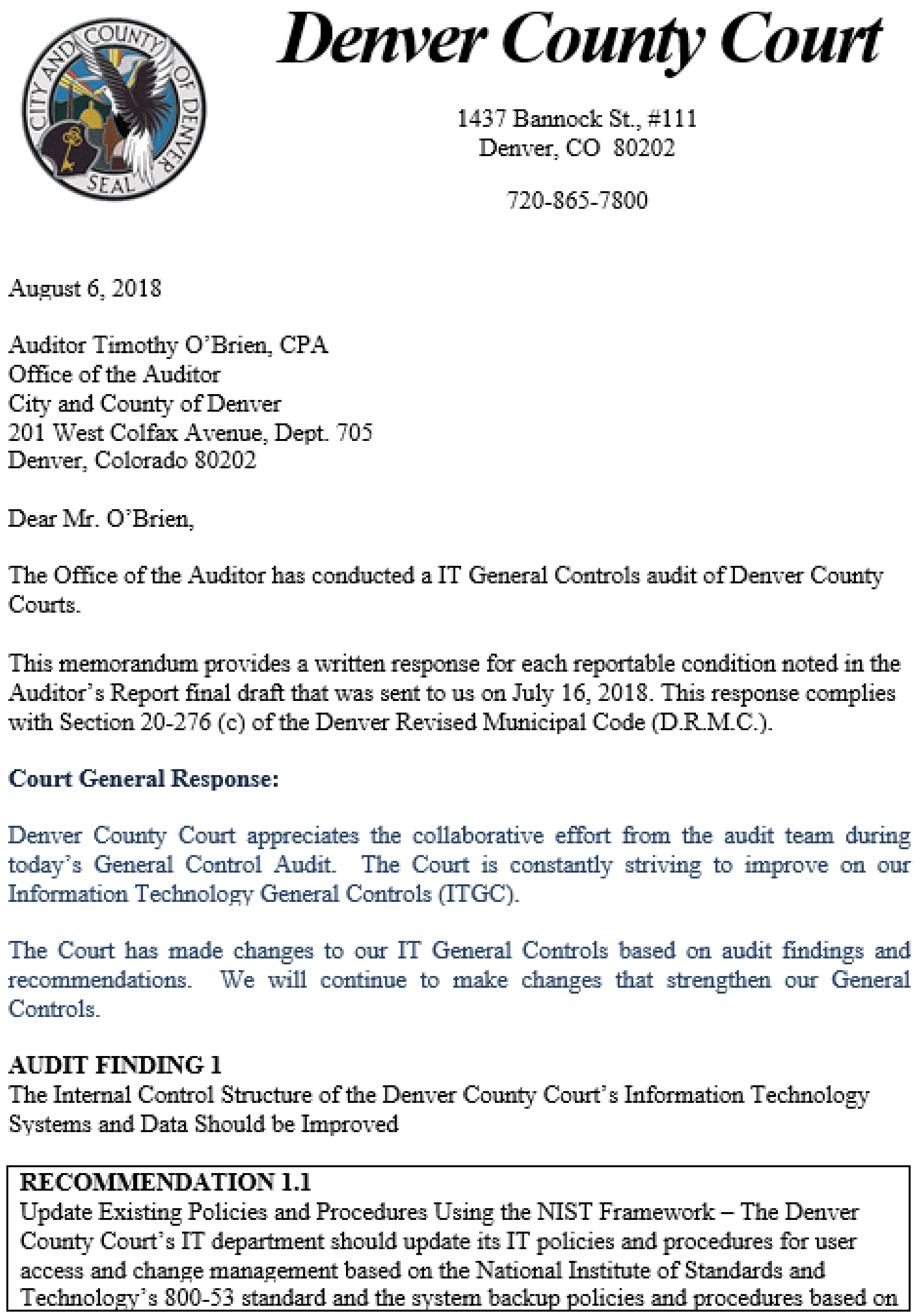
1.3 **Update Backup Process** – Denver County Court's IT department should use online backup solution or set up a physical backup solution on a nightly basis using the best practice Grandfather/Father/Child backup rotations as soon as possible.

Auditee Response: Agree, Implementation Date – June 1, 2019

Auditee Narrative*: The Court is focused on transitioning to cloud-based technology and real-time disaster recovery. The Court does not want to rely on the onsite data center in the event of a Denver disaster. A cloud solution will support the citywide initiative of Continuity of Operations Plan (COOP). COOP is a United States federal government initiative, required by U.S. Presidential Policy Directive 40 (PPD-40), to ensure that agencies are able to continue performance of essential functions under a broad range of circumstances.*

The cloud solution will replace the need for physical backups and support the Grandfather/Father/Child backup rotations.

AGENCY RESPONSE



Denver County Court

1437 Bannock St., #111
Denver, CO 80202

720-865-7800

August 6, 2018

Auditor Timothy O'Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O'Brien,

The Office of the Auditor has conducted a IT General Controls audit of Denver County Courts.

This memorandum provides a written response for each reportable condition noted in the Auditor's Report final draft that was sent to us on July 16, 2018. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

Court General Response:

Denver County Court appreciates the collaborative effort from the audit team during today's General Control Audit. The Court is constantly striving to improve on our Information Technology General Controls (ITGC).

The Court has made changes to our IT General Controls based on audit findings and recommendations. We will continue to make changes that strengthen our General Controls.

AUDIT FINDING 1
The Internal Control Structure of the Denver County Court's Information Technology Systems and Data Should be Improved

RECOMMENDATION 1.1
Update Existing Policies and Procedures Using the NIST Framework – The Denver County Court's IT department should update its IT policies and procedures for user access and change management based on the National Institute of Standards and Technology's 800-53 standard and the system backup policies and procedures based on

the National Institute of Standards and Technology's 800-34 standards as soon as possible. These updated policies and procedures should address the following areas:

1. Reflect the current operational practices
2. Clearly identify each control in place
3. Specify who performs each control
4. Describe how the performance of each control should be documented
5. Establish the retention period for control documentation.

Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	August 30th 2018 – 800-53 June 1st 2019 – 800-34	Kris Griffin 720-865-7703

Narrative for Recommendation 1.1

The Court has developed a comprehensive Change Management tracking policy and improvements to existing user access policies. These improvements will support the National Institute of Standards and Technology's 800-53.

The Court will improve current backup policies to align with the National Institute of Standards and Technology's 800-34 standards. The Court's focus is transitioning to Cloud based backup technology and real-time disaster recovery. Which would enable the Court to continue to operate in the event of a Denver based disaster. The Court does not want to rely on an onsite data center or physical media. A cloud solution will support the Citywide initiative of Continuity of Operations Plan (COOP).

RECOMMENDATION 1.2

Relocate Data Center – The Denver County Court's IT department should work with Technology Services to move the Court's computer servers to the City's existing data center colocation facilities as soon as possible.

Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Disagree	N/A	Kris Griffin 720-865-7703

Narrative for Recommendation 1.2

The Court will not relocate our data center. The Court will continue to make improvements the data center.

The improvements include but are not limited to: the physical security, notification alerts for temperature, humidity monitoring, access controls, logging and fire/water prevention.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 1.3</b>
Update Backup Process – The Denver County Court's IT department should use online backup solution or set up a physical backup solution on a nightly basis using the best practice Grandfather/Father/Child backup rotations as soon as possible.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>June 1st, 2019</td><td>Kris Griffin 720-865-7703</td></tr>
</table>

Narrative for Recommendation 1.3

The Court is focused on transitioning to cloud-based technology and real-time disaster recovery. The Court does not want to rely on the onsite data center in the event of a Denver disaster. A cloud solution will support the citywide initiative of Continuity of Operations Plan (COOP). COOP is a United States federal government initiative, required by U.S. Presidential Policy Directive 40 (PPD-40), to ensure that agencies are able to continue performance of essential functions under a broad range of circumstances.

The cloud solution will replace the need for physical backups and support the Grandfather/Father/Child backup rotations.

Please contact Kris Griffin at 720-865-7703 with any questions.

Sincerely,

Kris A. Griffin
Court IT Director

cc: Valerie Walling, Deputy Auditor, CPA,CMC
Kevin Sear, Audit Manager, CPA, CISA, CFE, CIA, CGMA
Theresa Spahn, Presiding Judge
Terrie Langham, Denver County Court Administrator