



Will Tetsell, City Auditor
Internal Audit Department
350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-2056

October 20, 2015

Mayor Betsy Hodges, City Council Members and City Coordinator Spencer Cronk,

Attached is the City of Minneapolis Internal Audit Department's Records Management audit report. The objective of this audit was to access and address the risks involved in collecting, creating, receiving, maintaining or disseminating data while adhering to the various statutes, acts, and City of Minneapolis (City) policies.

We found that the City had a variety of strengths and opportunities in how it manages data. Four findings are noted in the report; two of which include several sub-findings that were themed into categories to help the audience organize the contents of the report.

The City did have the institutional knowledge needed to manage government records risks; however, those key stakeholders (City Clerk, City Attorney, Information Technology, etc.) lacked the resources needed to address these issues.

Furthermore, the current program was disjointed, with various policies and projects put forward independently by a single stakeholder group. Perhaps the greatest opportunity is to provide a framework for increased collaboration and accountability among the various stakeholders.

A current example of such collaboration: the Records and Information Management Division of the Clerk's Office and the Records Information Unit of the Police Department had been collaborating to improve business processes around public data requests for accident reports. This partnership had also included Information Technology and the City Attorney's Office and was resulting in new processes which the stakeholders expect to significantly reduce staff time related to this process.

The attached report details risks, that if adequately addressed, could strengthen the City's aptitude and ability to strengthen its records management processes.

Sincerely,

A handwritten signature in black ink that reads "Will Tetsell". The signature is written in a cursive, flowing style.

Will Tetsell, City Auditor

Records Management Audit

City of Minneapolis – Internal Audit Department
October 20, 2015



Contents	Page
• Background	4
• Objective, Scope and Methodology	5
• Audit Results and Recommendations	6
• Acknowledgements	15
• Appendix A: ARMA Information Governance Maturity Model.....	16
• Appendix B: Audit of the Minneapolis Parks and Recreation Board	19
• Appendix C: Office of City Clerk Response	20



Internal Audit Department
350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-2056

Date: October 20, 2015

To: City Clerk, City Coordinator, City Council, Department Heads, Mayor's Office, Park and Recreation Board

Re: Records Management Audit

Background

Information is a strategic asset that allows the City of Minneapolis (City) to function effectively. The City maintained records to document business decisions and activities, provide information to public officials and act as a check on the honesty, integrity and completeness of official actions.

Government data (data) is defined as all data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or condition of use (Minnesota Statutes, section 13.02, subd. 7). As technology continues to advance and individuals change the media formats of conducting government business, the City needs to be aware of the risks of maintaining official documentation per statutory requirements.

City Information was subject to requirements governing both its use (i.e., the purposes for which it can be collected and used) and management (including how long it is kept, how it is secured and who may access it). All Minnesota government entities' data practices were given general guidance and basic legal framework by three laws.

- The Official Records Act (Minnesota Statutes, section 15.17) required government entities to make and preserve records to document official activities.
- The Records Management Statute (Minnesota Statutes, section 138.17) required the maintenance of official records for required time periods as defined by retention schedules and the disposal of records in a specific process depending on the types of data it contains.
- The Government Data Practices Act (Minnesota Statutes, Chapter 13) provided rights for public and data subjects, classified data that is not public, required data on individuals to be accurate, complete, current and secure, and provided penalties for violations.

In addition to this general legal framework, numerous federal and state laws and regulations imposed management requirements on specific types of information, such as personnel files, health information, financial records, and security information.

The Government Data Practices Act required entities to assign a responsible authority to oversee data practices decisions and policies. The City assigned this authority to the City Clerk and his designees. The City Clerk also developed a Records & Information Management (RIM) Division and established a network of liaisons within each department in the City. RIM provided guidance on the management of government records, validated compliance with necessary laws and regulations, and coordinated with Department Liaisons to help the City meet data practice obligations.

Objective, Scope and Approach

This audit was conducted as part of the Internal Audit Department's Fiscal Year 2015 Annual Audit Plan, as presented to the Audit Committee. Records management risks were identified as part of the annual risk assessment discussion with the Office of the City Clerk, City Attorney and City Coordinator.

Objective

The objective of the audit was to assess the effectiveness of the City's adherence to the Minnesota Government Data Practices Act, Minnesota Records Management Statute, Minnesota Official Records Act—and related City policies and procedures. The audit also evaluated the lifecycle of City Information, and assessed the processes in place to identify and remediate risks associated with information management. This was done through an evaluation of the City's records management program, including awareness, training, policies and the efficiency and effectiveness of the City's ability to execute appropriate records management practices based on the Information Governance Maturity Model promulgated by ARMA International, a professional association focused on information governance.

Scope

The audit scope included current records management practices and data from fiscal year 2015, which included:

- Records liaison roles, responsibilities and accountability for data decision-making, management and security.
- Policies and procedures supporting the governance of records collection, maintenance, usage and dissemination.
- Data element identification and classification.
- Access to data being appropriately provisioned, managed and based on a business justification.
- Adherence to data retention legal requirements and removal practices.

Approach

To accomplish our audit objective, we performed the following steps:

- Conducted interviews with City Clerk staff, Information Technology staff and Records Management Department Liaisons throughout the City.
- Evaluated applicable federal and state laws.
- Reviewed City policies and procedures.
- Tested a sample of users across three applications with access to private information.
- Reviewed a sample of terminated users.

Audit Results and Recommendations

The City's adherence to data practice and records management laws and City policies needed improvement. There were opportunities for improvement to the City's information asset management, data access and request management to manage records management risks. Without sound practices, the City may not be able to accurately and effectively ensure security of private information, validate compliance with laws and regulations and respond to requests for documentation resulting in potential legal consequences.

As the City leveraged new technologies and new ways of conducting its business, the types of data generated—and the challenges associated with managing it—evolved and will continue to evolve. Existing procedures may no longer address the challenges of the current context. The City needs to be aware of the challenges of managing its data per statutory requirements and the risks of failing to do so.

Finding 1: Records Management

The City did not have an adequate records management governance structure to provide an accountability framework of records management practices that encompass the full data life cycle. This includes defined responsibilities, documented policies and procedures and compliance monitoring.

Generally Accepted Recordkeeping Principles® (Principles) were developed and promulgated by ARMA International to help organizations address the need of information governance. Internal Audit reviewed the Principles, and using the Maturity Model, identified that the City was in 'sub-standard' or 'in development' status for the eight Principles of an effective information governance structure (see Appendix A). This rating represents a program with numerous gaps that leave the City vulnerable to legal or regulatory risks because its records management practices are incomplete or only marginally effective.

Internal Audit reviewed the ten policies and procedures identified by the Clerk's RIM Division as the current records management policies. It was noted that of the ten, only one had been updated in the past two years. There was no process in place for the team to review and communicate changes of these policies to the departments. Without policies and procedures, departments cannot be held accountable, which created a lack of consistency in practices throughout the City. In 2003, City Council adopted an Enterprise Information Management policy to create a standardized framework for governing information assets across the enterprise. Despite the adoption of this policy, it was never fully implemented or adhered to by departments.

Records Management Recommendations:

- The City Clerk's RIM Division should use the ARMA International Principles to develop an effective records management framework.
- The City Clerk's RIM Division should review records management policies and procedures on a consistent basis and ensure departments are aware of any changes.

Records Management Management Response: Office of the City Clerk

The Clerk's Office agrees with the Auditor's findings as to the importance of an effective information governance program and the factual description of the state of the enterprise. Currently, the City operates with a number of independent policies, various undefined roles and responsibilities and without clear channels of communication. To be effective, the program must be actively managed and maintained over time by an entity with sufficient authority and accountability for the overall effectiveness of the program. We agree with the audit's recommendations and propose the following corrective actions:

- The City should enact an ordinance establishing the policy framework for the information governance program, which would provide the authority and structure for appropriate policies

and procedures, clear standards and accountability. The information governance program should be overseen by a council committee that could provide proper assurance that such a multidisciplinary, enterprise-wide program is appropriately reviewed, updated and maintained.

- The City Clerk's RIM Division should review existing policies relating to information governance against the current environment, considering legal and regulatory requirements, best practices such as ARMA International's Principles, and the City's technology, processes and capabilities. These policies should be updated and harmonized.
- The City Clerk's RIM Division will collaborate with each City Department to develop appropriate department-specific procedures, retention schedules and training.

Finding 2: Information Asset Management

The City did not have adequate and effective controls to appropriately manage data as a public asset. Well-governed data is critical to the success of the City.

2.1 Data Inventory

The City did not have a data inventory that identified all private and confidential information maintained or collected by the City departments. This was in violation of Minnesota State Statutes requirements as defined in section 13.025 subdivision 1, which required the responsible authority to prepare and update annually an inventory identifying private and confidential information maintained by the City. This inventory would allow the City to ensure appropriate controls are applied to the protected data from the moment it is created until its disposition. In addition, as part of Minnesota Statutes, section 13.05, subdivision 5, departments were responsible for validating that data that is private is only accessible by persons whose work assignment required access to such data. Because the City did not have the necessary data identified, Internal Audit was unable to verify that necessary security monitoring controls are in place.

Data Inventory Recommendations:

- The City Clerk's RIM Division should create and implement processes to annually update an inventory identifying all private and confidential information.
- The City Clerk's RIM Division, in coordination with the departments, should implement a periodic review of private and confidential information to determine whether the information is necessary to City business purposes and eliminate the collection of unnecessary data.

Data Inventory Management Response: Office of the City Clerk

The Clerk's Office agrees with the Auditor's findings and recommendations. This inventory is statutorily required and, while the City's current records retention schedules partially meet this requirement, many of these schedules are incomplete or out-of-date.

The City Clerk's RIM Division is in the process of developing a data inventory in the format suggested by the State's Information and Policy Analysis Division (IPAD). This inventory will bring the City into compliance with Minnesota law. In addition, the City Clerk's RIM Division will collaborate with the Information Technology Department to identify and leverage opportunities to track the classifications of electronic data (e.g., private, confidential) in electronic systems, where appropriate and practicable. These opportunities will facilitate improved electronic management and appropriate security.

2.2 Records Storage

The City maintained two locations for physical record storage: the Clock Tower in City Hall and a storage facility in the Leamington ramp. The City Clerk's RIM Division managed the records within these designated locations. Throughout the City, departments were using empty conference rooms and other locations to store physical records.

Internal Audit noted the Clerk's Office storage was restricted to authorized personnel, though lacked physical access controls. Additionally, there was no complete mapping or tracking of the records within the Clerk's Office storage facility, making it difficult to identify the full scope of records the facility contains and where in the facility a particular record may be located. Due to the decentralized nature of the remaining records throughout the City, offsite locations were not reviewed. These decentralized storage locations posed security and access risks as controls may not have been in place for those employees that did not have a work-related reason to access private data that could potentially be located within these locations. Based on discussions with Records Management Department Liaisons, some departments maintained records in multiple locations and Department Liaisons were uncertain what data should reside in departments and what should be sent to or managed by the Clerk's Office. The City Clerk's Office did not monitor or manage—and was frequently unaware of—departmental storage locations, which hampered its ability to plan for future storage space needs. This could have exposed the City to data practices and legal discovery risks.

Based on discussions with Information Technology staff and Records Management Department Liaisons, it was noted that the City did not have sufficient policies and procedures around the organization and storage of electronic data. Many departments noted that electronic information had never been considered in the record destruction process or multiple versions of documents were maintained for fear of deleting the wrong one. In addition, the systems used by departments did not have retention functionality built into them and therefore data was kept in perpetuity unless departments worked with Information Technology to complete a clean-up process.

Records Storage Recommendations:

- The City Clerk's RIM Division should create policies and procedures for departments to use to determine where and how to store physical records.
- The City Clerk's RIM Division and IT should create policies and procedures around the organization and management of electronic data. In addition, as new systems are implemented, records management functionality (including retention, accessibility, protection and disposition) should be incorporated as able.
- The City Clerk's RIM Division should conduct an enterprise-wide evaluation of physical record storage needs and develop a capacity to handle the City's inventory of physical records.
- The City Clerk's Records and Information Management Division should strengthen the central records center infrastructure to allow more efficient access and management, and more effective use of existing storage space.

Records Storage Management Response: Office of the City Clerk

The Clerk's Office agrees with the Auditor's findings and recommendations regarding physical and electronic records storage. While some in-departmental storage is appropriate because the materials must be frequently accessed, at least a portion is forced due to space constraints in the central records warehouse.

2.3 Records Disposition

The City did not have consistent data destruction processes in place, which could result in unauthorized access to information, or in records destroyed without authority from the Records Disposition Panel, violating Minnesota Statutes, section 138.225.

Some City Information (records) must be maintained for a specific period (the retention period). As defined in Minnesota Statutes, section 138.17, subdivision 7, the State through the Minnesota Records Disposition Panel must approve the period for which a record must be retained, which was achieved by the City's Record Retention Schedules. When a Department Destruction Form was completed by the department, it allowed the City Clerk's Office the ability to track records that were destroyed, as well as monitor if records were being destroyed within the approved time periods.

Per the City policy, a department was to use the approved City Record Retention Schedules to determine when a record was eligible for destruction. In the event that destruction took place, a Department Destruction Form was required to be completed and sent to the Clerk's Office. Based on discussions with the City Clerk's RIM Division, this was not a consistent practice across City departments and some forms were completed at a high level, and provided insufficient documentation of the record destruction.

Based on discussions with the City Clerk and Records Management Department Liaisons, the current City Record Retention Schedules were not easy to use and/or understand. Many departments stated it was easier to maintain data than risk destroying something that was not eligible for destruction. Internal Audit notes that on average the schedules had not been updated since 2006. Many departments seemed unaware of the authority and partnership required of the Clerk's Office to update and maintain these schedules to reflect the most accurate information for their data.

Records Disposition Recommendations:

- The City Clerk's RIM Division should update and maintain the record retention schedules.
- The City Clerk's Office should provide periodic training and guidance on the requirements and available resources regarding record and data destruction and record retention schedules.
- The City Clerk's RIM Division should periodically review the timeliness of Department Destruction Form submissions, and address incomplete form submissions through feedback to departments providing such forms.
- The City Clerk's RIM Division should update and maintain policies and procedures for departments around destruction of record and non-record information.

Records Disposition Management Response: Office of the City Clerk

The Clerk's Office agrees with the Auditor's findings and recommendations regarding records disposition and the City's records retention schedules. Many of the City's records retention schedules are outdated and difficult to use. This complexity leads to non-compliance which exacerbates the storage issues described in Finding 2.2. The City Clerk's RIM Division proposes to overhaul, update and simplify the City's records retention schedules, transitioning to a modern schedule which comports with best practices. The RIM Division will work with Information Technology and City Departments to identify and remediate expired records and information.

2.4 Records Management Monitoring

The City Clerk did not have a process to ensure compliance with records management policies among City departments. Departmental non-compliance with (or inconsistent interpretation of) policy requirements, may create inconsistency in City records management practices. The City could face potential reputational and legal consequences from inappropriate destruction, inaccurate retention or insufficient protection of data.

Minnesota State Statutes, section 13.03 and 13.05, imposed specific duties on government entities relative to data requests, classification of government data, and the collection, storage, use, dissemination and proper disposal of government data. The responsible authority was assigned responsibility for data practices decisions and policies and had the ability to appoint designees. Within the City of Minneapolis, the City Clerk was assigned as the responsible authority and had designated liaison(s) within each department to help facilitate the records management processes. The City Records Management Policy did not provide clear authority for the responsible authority to oversee or audit department records management processes. There were no accountability tools or ongoing monitoring performed to validate compliance with state statutes among the City departments. Internal Audit conducted surveys with 19 of the 21 liaisons and noted inconsistent practices in terms of records retention practices, request fulfillment and data disposition.

Records Management Monitoring Recommendations:

- The City Clerk's RIM Division should create accountability tools and an ongoing monitoring program, including scheduled updates to policies and procedures, onboarding and ongoing training and periodic auditing. This will allow the City Clerk to validate that departments are aware of and in compliance with internal and external records management requirements.
- The City should clarify the authority of the responsible authority to create and implement the accountability tools and monitoring program described above.

Records Management Monitoring Management Response: Office of the City Clerk

The Clerk's Office agrees with the Auditor's findings and recommendations regarding the lack of compliance monitoring related to the RIM program. Departments are largely left on their own to manage information, notifying the Clerk's Office at their discretion. There is no affirmative audit or review.

As discussed in the response to Finding 1, the City should enact an ordinance establishing a framework for information governance that clarifies roles and responsibilities. This should explicitly include the role of the responsible authority to validate departmental compliance, develop an audit and accountability program and develop training, guidance and awareness materials.

Finding 3: Data Access

The City did not have adequate security controls for electronic data access management.

3.1 Application Access

As noted in Finding 2, the City did not have a formal process to identify and locate confidential, private and sensitive information. The Information Technology Department was responsible for securing systems and applications but was reliant on the departments to notify them of special needs for the information they maintain within their applications. Without this identification, there were no means to determine and provide appropriate levels of protection.

Testing of a sample of user accounts with access to confidential, private or sensitive information across two applications (MINS and KIVA) identified 14 of 25 (56%) accounts where access was determined to be inappropriate based on their current role.

The City did not operate on a least-privilege model, which is the ability to access data only by those employees with business justification. Typically, departments requested setting up new users with similar access to an existing City employee and there was no process to verify that any unnecessary access was not provisioned. There was no consistent periodic review of a user's access to applications and data within the City, nor was there a good means to identify when someone has transferred roles or terminated their employment with the City. This could have led to users maintaining unnecessary and/or unauthorized access to sensitive information.

Application Access Recommendations:

- As noted in Finding 2.1, City Clerk's RIM Division should create a data inventory, in addition, the Information Technology Department, City Clerk's Office and City Departments should develop a framework to better define appropriate requirements and limitations regarding access to confidential, private and other sensitive information.
- The City Clerk's RIM Division, the Information Technology Department and Human Resources Department should establish procedures to validate that user access is closely tied to an individual's role and job duties and that user's access rights are timely updated to reflect any changes of employment, role or duties.

Application Access Management Response: Office of the City Clerk

The Clerk's Office agrees with the Auditor's findings and recommendations regarding application access controls. As discussed in the response to Finding 2.1, City Clerk's RIM Division is working to create a data inventory and proposes to collaborate with IT to leverage opportunities to track the classifications of electronic data in electronic systems.

Application Access Management Response: Information Technology

IT is in agreement with the recommendations. We believe an enterprise policy framework around information security and risk management is needed to clearly articulate expectations and assign accountability for safeguarding private government information. We also recognize that IT industry trends are changing how, what and where City employees use technology to work with City data. In response, we have a strategy to evolve our security services to expand protections beyond the traditional IT perimeter. But effectiveness of these protections will depend on an enterprise policy framework that strikes the right balance between risk and productivity to govern how far beyond City-implemented controls employees will be allowed to go.

3.2 Terminated Users

Testing of user accounts within applications hosting confidential, private and sensitive information identified 740 accounts across three applications assigned to persons no longer employed with the City. As part of the off-boarding process, all access, both physical and logical, to city resources should be removed. Allowing terminated user accounts to remain active created the risk that confidential, private or sensitive information could have been accessed by unauthorized users. Of the 740 accounts, 704 were PeopleSoft users. PeopleSoft

allowed users to login through a web-portal that doesn't federate to Active Directory, resulting in the potential that these terminated users could have logged in to the PeopleSoft application from an external network rather than the City's network with their employee credentials.

Terminated User Recommendations:

- HR off-boarding policies and procedures should be reevaluated and stronger IT processes and controls should be in place to ensure users are removed in a timely manner. Periodic system reviews should be conducted to detect accounts belonging to terminated users.

Terminated User Management Response: Office of the City Clerk

The Clerk's Office agrees with the Auditor's findings as regarding the importance of managing access as part of the off-boarding process. The Clerk's Office sees this as part of a broader need to proactively manage information in the custody of the terminated or transitioning employee. The framework discussed in the response to Finding 1 should incorporate off-boarding policies and procedures that ensure access is secured and that government devices, records and information in possession of the off-boarding employee are properly managed.

Terminated User Management Response: Information Technology & Human Resources

IT and HR are in agreement with the recommendations. IT currently is working with HR to automate notifications and workflows for promptly removing access when a worker changes jobs in the City or leaves City employment. We are also preparing new onboarding procedures that will capture more information about what a new employee needs access to. Though the primary goal of this tactic is to get that employee set up to work as quickly as possible, we also need this information to help make sure all access is removed when that employee leaves. Achieving success with this tactic will depend on gaining visibility into the applications and access administration processes that the IT department does not currently support.

3.3 Data Breach Protocol

In the event of a data breach, departments did not have procedures to report and respond to incidents of misuse, unauthorized disclosure or access. Minnesota Statutes, section 13.055 required notification to impacted individuals and that an investigation be conducted. The investigation should determine the cause of the breach, and enforce any necessary disciplinary action if City employees or contractors are found guilty of an unauthorized acquisition with the intent of using the data for nongovernmental purposes.

Data Breach Recommendations:

- The City should create and implement an incident response plan to facilitate a consistent, central process for reporting and responding to unauthorized disclosure, access or misuse of confidential, private and other sensitive data.

Data Breach Management Response: Office of the City Clerk

The Clerk's Office agrees with the Auditor's findings regarding the City's lack of an incident response plan in the event of a data breach. The framework discussed in the response to Finding 1 should incorporate an incident response plan. This plan should address the appropriate immediate response, assessment, investigation and notification and should consider all applicable laws including the Minnesota Government Data Practices Act, HIPAA and the Payment Card Industry Data Security Standards.

Data Breach Management Response: Information Technology

IT is finalizing our incident response plan for investigating suspected breach incidents detected by our security monitoring operations and acceptable-use observations. This plan includes preservation of such evidence we can find to indicate a successful breach. We welcome this recommendation to collaborate with the City Clerk and other stakeholders to develop the organizational response plan should a successful breach of IT protections be discovered. We also recognize that not all breaches will occur because IT systems are compromised, and not all systems are capable of monitoring user behavior for suspected misuse. We believe the organizational response plan should include a procedure for reporting and investigating suspected breaches resulting from misuse of authorized access.

3.4 Device Security

The City did not have encrypted devices, including mobile devices such as laptops, tablets, smart phones and removable storage media, so in the event that a device was lost or stolen, or data was compromised, there were no security measures to prevent external parties from accessing the information.

Device Security Recommendations:

- The Information Technology Department should implement a program to secure mobile devices that may contain sensitive information, such as by encryption or equivalent measures. Because the City did not have a formal process to identify and locate confidential, private and other sensitive information, all City laptops should be encrypted.

Device Security Management Response: Office of City Clerk

The Clerk's Office agrees with the Auditor's findings regarding the importance of appropriate security for mobile devices. This issue is related to the lack of an effective governance program discussed in Finding 1 because there are limited standards regarding where data can be stored. The framework discussed in the response to Finding 1 should incorporate standards for appropriate storage for private, confidential and sensitive information.

Device Security Management Response: Information Technology

IT has a plan in place to implement encryption on City-issued laptops when we take ownership of these devices from Unisys. This will roll out sometime after the first of the year when we are confident we have the tools and processes in place to support it. IT has limited control over how other categories of mobile device are secured with encryption, such as tablets and smartphones that could contain sensitive City data. IT also cannot control how City data would be protected when workers choose to access it from personal computers, tablets and smartphones. We believe it is important that an enterprise policy framework addresses acceptable use of personally-owned computing devices to access and store City data.

Finding 4: Request Management

The City Clerk's RIM Division did not have a central or consistent process to track the intake and fulfillment of public information requests made under the Minnesota Government Data Practices Act, Minnesota Statutes, chapter 13. The City lacked the ability to track volume and fulfillment timing of requests and was thus unable to validate that departments were effectively meeting statutory requirements regarding timing and disclosure. Because responses were not consistently centrally coordinated or reviewed, the City was unable to ensure that responses were appropriate and that redaction or exceptions were consistently applied.

Minnesota Statutes, section 13.03, subdivision 2 required the responsible authority to establish procedures that ensured that data requests are received and complied with accurately and promptly. Minnesota Statutes, section 13.04, subdivision 3 set further time limits for responding to individuals who are the subjects of the information inquiry. The City Clerk's RIM Division did not have the ability to monitor the volume and/or completion of data requests, resulting in an inability to ensure that requests were fulfilled in a timely manner. The City Clerk's RIM Division was unable to effectively track details of the requests once sent to the departments. Unless notified by a department, the City Clerk's RIM Division was not aware of what response was sent to the requestor, when it was sent, or whether the request was successfully completed. Instead, they relied on the Department Liaisons to coordinate responses with their respective departments. Internal Audit conducted surveys with 19 of the 21 Department Liaisons and noted a wide range of request fulfillment practices.

In most departments, there was no formal process to review the response before information was released. While all liaisons were aware of who to contact with questions and concerns in regards to public versus not-public information, specific request fulfillment practices varied. In addition, there was no coordination when fulfilling and releasing records that span across departments. This could have led to inconsistent application of the law or incomplete redaction in the response to a single request, for example, where one department identified something as private while another included it as a part of their response.

Although the future impact of data requests is unpredictable, the ability to better monitor and track fulfillment progress enables the City to apply exceptions and redactions consistently, identify problematic request types to better focus training efforts and resources and avoid violations of legal requirements.

Request Management Recommendations:

- The City Clerk's RIM Division should develop consistent review and authorization procedures for all departments to follow before releasing information to the public as part of data requests.
- The City Clerk's RIM Division should implement a process to allow central tracking of data requests of all City departments, from intake through fulfillment.
- The City Clerk's RIM Division should establish a monitoring program to evaluate data gathered from the above process and identify departments who are struggling to fulfill data requests or may need additional training or resources.

Request Management Management Response: Office of City Clerk

The Clerk's Office agrees with the Auditor's findings and recommendations regarding management of requests for public information. The appropriate provision of information in response to public information requests under Minnesota law is a critical component of the City's commitment to government transparency. The current system is not only unable to centrally track requests but also risks inconsistent treatment of requests or application of law by responders.

The City Clerk's RIM Division will implement a centralized data practices request management solution that allows for submission, fulfillment and reporting of requests and the RIM Division will collaborate with each City Department to develop a program of training and monitoring related to the City's responsibilities under the Minnesota Government Data Practices Act.

Acknowledgments

The City of Minneapolis Internal Audit team would like to acknowledge the time, effort and partnership put forth from the City Clerk's Office and Information Technology Department. Their enthusiasm and collaboration were very helpful in completing this audit. In addition, the Department Liaisons were also extremely helpful in providing information about their individual departments as well as being accommodating with meetings and timely with responses.

Appendix A – ARMA Information Governance Maturity Model

To address the needs and concerns around information governance, ARMA International developed and promulgated the Generally Accepted Recordkeeping Principles. The Principles were intended to help guide organizations on the creation of a high-level framework of good data management practices. Internal Audit reviewed the “Information Governance Maturity Model” (IGMM) and identified the following rankings for the City’s current data governance framework. The IGMM was developed by ARMA to help organizations gauge the effectiveness of their recordkeeping processes. Data is one of the most strategic assets the City possesses and having a sound framework of governance allows the City to meet the demands of ever-growing data volume and issues of transparency. In addition, the gaps that needed to be addressed to reach an essential level (3 of 5) were included to show some of the improvements that needed to be made to allow the City to have a more effective framework to mitigate data governance and records management risks.

The Principle	Maturity Level	Gaps for Level 3 (Essential)
<p>Accountability A senior executive (or person of comparable authority) shall oversee the information governance program and delegate responsibility for records and information management to appropriate individuals. The organization adopts policies and procedures to guide personnel and ensure that the program can be audited.</p>	<p>In Development (2 of 5)</p>	<p>Senior management lacked awareness and engagement of the records management program.</p> <p>The Clerk's RIM Division envisioned establishing a broader-based information governance program to direct various data-driven processes throughout the City.</p> <p>The City needed more consideration around electronic records as part of the records management program.</p> <p>The City lacked defined specific goals related to accountability.</p>
<p>Transparency An organization’s business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and the documentation shall be available to all personnel and appropriate interested parties.</p>	<p>In Development (2 of 5)</p>	<p>City employees were not educated on the importance of transparency and the specifics of the City's commitment to transparency.</p> <p>The records management processes were not consistently documented.</p> <p>Transparency in records management was not taken seriously and data was not readily and systematically available when needed.</p> <p>The City lacks specific goals related to information governance transparency.</p>

<p>Integrity An information governance program shall be constructed so the information generated by or managed for the organization has a reasonable and suitable guarantee of authenticity and reliability.</p>	<p>Sub-Standard (1 of 5)</p>	<p>The City did not have a formal process to ensure that the required level of authenticity and chain of custody could be applied to its systems and processes.</p> <p>The City did not have defined goals related to integrity.</p>
<p>Protection An information governance program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection.</p>	<p>Sub-Standard (1 of 5)</p>	<p>The City lacked a formal written policy for protecting data, as well as centralized access controls.</p> <p>Confidentiality and privacy considerations were not well-defined within the City.</p> <p>Training for employees was not consistently available.</p> <p>Records and information audits were not conducted.</p> <p>The City did not have specific goals related to records and information protection.</p>
<p>Compliance An information governance program shall be constructed to comply with applicable laws and other binding authorities, as well as with the organization’s policies.</p>	<p>Sub-Standard (1 of 5)</p>	<p>Compliance was not highly valued and measurable, and suitable records and information were potentially not maintained.</p> <p>Data was not systematically managed. Departments within the City managed data as they saw fit based upon their understanding of their responsibilities, duties, and what the appropriate requirements were.</p> <p>There was no generally understood process for imposing legal, audit, or other information production processes. The hold process was not integrated into the City's information management and discovery processes for the critical systems.</p> <p>The City had significant exposure to adverse consequences from poor</p>

		compliance practices.
<p>Availability An organization shall maintain records and information in a manner that ensures timely, efficient, and accurate retrieval of needed information.</p>	<p>In Development (2 of 5)</p>	<p>The records and other information lacked finding aids.</p> <p>There was no standard imposed across departments on where and how to store official records.</p> <p>The City's systems and infrastructure did not contribute to the availability of records.</p>
<p>Retention An organization shall maintain its records and information for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements.</p>	<p>In Development (2 of 5)</p>	<p>The retention schedule and policies were not regularly updated or maintained.</p> <p>Education and training about the retention policies was not available causing employees to either keep everything or dispose of records and information based on their own business needs, rather than City requirements.</p> <p>The City did not have specific goals related to retention.</p>
<p>Disposition An organization shall provide secure and appropriate disposition for records and information that are no longer required to be maintained by applicable laws and the organization's policies.</p>	<p>In Development (2 of 5)</p>	<p>There was neither enforcement nor auditing of dispositions.</p> <p>Although policies and procedures existed, they were not standard across the departments.</p> <p>The City did not have specific goals related to disposition.</p>

Appendix B

Records Management Audit of the Minneapolis Parks and Recreation Board

Due to the smaller breadth and complexity of the Minneapolis Parks and Recreation Board (MPRB), a limited-scope audit covering the following areas was completed:

- Request management.
- Policies and procedures.
- Data Inventory.
- Record disposition.

No reportable findings were discovered in the audit of the MPRB.

Office of City Clerk Response

The Clerk's Office recognizes and appreciates the work of the Internal Audit Department and understands the seriousness of the findings. We are in overall agreement with the Auditor's assessment. The audit reveals a number of gaps and weaknesses in the City's existing information governance and records management programs. It also provides a starting point from which to develop, implement, and evaluate an effective, revitalized information governance program, providing a firm foundation for a path forward. The Records and Information Management (RIM) Division of the Clerk's Office looks forward to further developing and presenting plans to address the findings in this audit.

The Clerk's Office takes the results of this audit very seriously. An effective information governance program is critical in order for the City to function effectively as an enterprise, to protect private data, and to comply with obligations under Federal and State law. The Clerk's Office appreciates the time and effort of the Internal Audit team in producing this report and the attention of the Audit Committee.