APPLICATION XTENDER

PROGRAM EVALUATION AND AUDIT

METROPOLITAN COUNCIL

March 2015

INTRODUCTION

Background

The Application Xtender program was implemented in 2007 to aid in the efficient management and security of electronic documents across the Metropolitan Council. Implementation of the system has been voluntary and use has gradually spread across many Council departments, including the Central Corridor Project Office and Community Development. The program also includes workflow functionality which is currently used in two departments. A document management team and document management policy were both created in 2011, at which time the implementation of Application Xtender was accelerated.

Purpose

The purpose of the audit is to assess the implementation of Application Xtender, with a focus on access management. The audit will identify potential risks and control weaknesses and recommend solutions to mitigate risks or strengthen controls where necessary.

Scope

Testing of access controls was limited to the 2014 calendar year.

Methodology

- Interviews of Document Management, Information Services and related staff
- Review of application users and entitlements
- Review of existing provisioning process
- Testing of employee access and privileged account use

Assurances

This audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and the U. S. Government Accountability Office's *Government Auditing Standards*.

OBSERVATIONS

An informal process has been developed to manage identity and access rights in Application Xtender.

When the audit began, a majority of the provisioning process occurred as an application was being developed, but an ongoing process for provisioning user identities and access rights was not in place. A process has since been developed by document management staff. First, application owners responsible for managing access for each business unit have been identified and a routing process for access requests through the agency intranet has been developed. Routing goes to an employee's supervising manager and the application owner for approval prior to being routed to Information Services (IS). Second, document management staff checks with application owners to review the appropriateness of access permissions and intends to perform this review on a yearly basis. Third, staff has begun checking offboarding lists to better ensure employees who have retired or transferred have their permissions changed. While these processes have been put into practice, they have not yet been formalized in written policies or procedures. These procedures mitigate the risk of granting unnecessary access to employees who don't need it for their work and the risk of maintaining access when it is no longer needed.

Privileged accounts are used in scanning software and custom programming from the vendor.

Privileged accounts are used to administer IT systems, and thus have greater entitlements than typical accounts used by employees to view or create documents. Privileged accounts need to be managed carefully since they are able to bypass access controls and make changes to the system. When privileged account use was reviewed, approximately 92% of activities were related to scanning processes or custom programming by the third-party vendor responsible for system support. When possible, custom work by the vendor should use a least-privileged approach to mitigate the risk of potential vulnerabilities that come from use of privileged accounts.

A generic privileged account was used by document management staff, and to a lesser extent, the third-party vendor, for system maintenance and support.

The activities of privileged accounts were audited to understand why they were used and who was using them. Many different activities are captured in the audit trail, from log-ins and log-outs, to the creation, viewing and deletion of documents. Less than 1% of audited activities related to privileged accounts were traced to document management staff and the third-party vendor for system support. Use of this account by the vendor is the result of their employees not being made full administrators in order to limit what they can do in the system. The use of the generic privileged account is less auditable than having each employee have their own admin account. A least-privileged approach is desirable for vendor access, but accounts that directly identify the individual making the changes are more appropriate for both the vendor and document management staff to use.

Audit trail was incomplete for privileged accounts.

Use of the generic privileged account decreased the ability for individuals to be identified from the audit trail. Activities from this account could not be traced back to the party using the account in approximately 2% of cases. In these cases, it was unclear whether document management staff or the vendor used the account. Logs from the system that enable remote access were kept for two days, which also contributed to gaps in the audit trail. However, even if activity could be traced back to either party, use of the generic account would make it difficult to identify the actual individual who made the change.

The generic privileged account that was used by the vendor to resolve an issue with an application resulted in additional gaps in the audit trail. The intention was to have a Metropolitan Council employee change the account to a more appropriate account soon after the fix. The change didn't occur and the account remained active for 38 days. As a result, documents viewed during this time for an application containing sensitive documents could not be traced back to the individual viewing the document. Document Management staff discovered the issue when reviewing email messages describing the fix, at which time the issue was resolved. There is no evidence of any inappropriate activity as a result of the fix, but the generic privileged account should not have been used and controls were not in place catch the issue in a timely manner. The creation of formal policies or procedures for the management, use, and oversight of privileged accounts for Application Xtender and a defined process for approval and documentation of the maintenance activities of the vendor would have identified the issue and allowed staff to take appropriate action in a timely manner.

Employee use of Application Xtender was also reviewed. A generic username was returned in audit logs of employee activities, making it difficult for audit to identify who accessed documents in a limited number of circumstances. This was eventually resolved in each case and thus poses no risk. In some cases a user's last name did not populate correctly in the tool used to manage access in Application Xtender. In these cases a generic username was returned in reports instead of a last name specific to the individual. All cases were eventually traced back to specific individual users by cross referencing other audit tables. The risk of incomplete audit logs was resolved, but user information should be manually updated so users can be easily identified in a single audit table.

CONCLUSIONS

Steps have been taken to develop an ongoing process for provisioning access to Application Xtender. These steps include a routing process for requests and approvals, periodic review of access rights, and periodic review of retired and transferred employees. Written policies or procedures for these steps, including a risk assessment, employee responsibilities, and appropriate documentation will increase the probability that only approved employees can access documents.

A process was not in place to approve the maintenance activities of vendors and manage privileged accounts in Application Xtender, which contributed to incomplete audit trails. Privileged accounts pose more risk since they can bypass existing access controls and make changes to the system. As a result, a process to provision access, manage and monitor privileged accounts is recommended to reduce risk to an acceptable level.

RECOMMENDATIONS

Program Evaluation and Audit recommendations are categorized according to the level of risk they pose for the Council. The categories are:

- **Essential** – Steps must be taken to avoid the emergence of critical risks to the Council or to add great value to the Council and its programs. Essential recommendations are tracked through the Audit Database and status is reported twice annually to the Council's Audit Committee.
- **Significant** – Adds value to programs or initiatives of the Council, but is not necessary to avoid major control risks or other critical risk exposures. Significant recommendations are also tracked with status reports to the Council's Audit Committee.
- **Considerations** – Recommendation would be beneficial, but may be subject to being set aside in favor of higher priority activities for the Council, or may require collaboration with another program area or division. Considerations are not tracked or reported. Their implementation is solely at the hands of management.
- **Verbal Recommendation** – An issue was found that bears mentioning, but is not sufficient to constitute a control risk or other repercussions to warrant inclusion in the written report. Verbal recommendations are documented in the file, but are not tracked or reported regularly.

1. **(Essential) Develop a written process for managing privileged accounts in the following areas:**

   - Provisioning process for vendor accounts according to the least-privileges necessary to perform their specific duties. Develop naming conventions for each account so a specific user can be easily identified from the sign-on credentials.
   - Periodic auditing of privileged account users and monitoring of account activities. Ensure audit logs are archived long enough to satisfy monitoring and audit requirements.
   - Require the vendor to use the least-privileges necessary when completing custom work on the Application Xtender system
   - Adequate documentation of approval, privileged account users and other processes as necessary to demonstrate compliance with procedures

   Management Response: *Concur with the audit recommendation. Enterprise Content Management staff have already taken steps to minimize the use of privileged accounts by the vendor; this includes communication in early February reiterating requirements to utilize existing Active Directory accounts for system access and maintenance. Enterprise Content Management and Information Services staff will further define and document processes to manage privileged accounts to include:*

   - *Review of current Active Directory account privileges for the external vendor, and standardize naming conventions as necessary*
   - *Development of an ongoing report to provide audit information to appropriate Council staff as needed. Audit logs/data are currently available for extraction to satisfy monitoring and audit requirements.*
   - *Review access levels of the service account to determine the least privileges necessary to accommodate system functionality*
   - *Create documentation to describe the approval and management of privileged account users including the reset of system passwords as required to maintain a secure environment*

Staff Responsible: *Carah Koch, Shankar Veluvali (Other ECM and IS staff yet to be determined)*

Timetable: *Completion-3rd quarter 2015*

2. (Essential) Develop a process for approval and documentation of maintenance activities for vendors prior to deployment in the system.

Management Response: *Concur with the audit recommendation. Enterprise Content Management and Information Services staff will review current maintenance agreements and further define and document a process for the management of ongoing vendor maintenance activities. This will include:*

- *Development and documentation of vendor test ID scenarios, and the implementation of time out features for their ongoing maintenance*
- *Review of existing and future password maintenance roles for Council staff*

Staff Responsible: *Carah Koch, Shankar Veluvali (Other ECM and IS staff yet to be determined)*

Timetable: *Completion- 3rd quarter 2015*

3. (Significant) Formalize the provisioning process for employees in written procedures. It is recommended that procedures include the following:

- How requests are made and routed for different types of identities
- Approval process, including an evaluation of employees role and adequacy of rights
- Documentation of access requests, approvals, start/end dates and other details
- Onboarding and offboarding responsibilities and procedures
- Periodic review of user access
- Adequate documentation of processes as necessary to demonstrate compliance with procedures

Management Response: *Concur with the audit recommendation. Enterprise Content Management and Information Services staff will continue to develop internal procedures and documentation to fulfill these recommendations. These efforts will include:*

- *Enterprise Content Management staff currently review access on a quarterly basis, and work with managers and supervisors to insure that access remains current. Communication with Human Resources staff will take place to review onboarding and offboarding procedures to support formalized communication to supervisory and management staff.*
- *Documentation of existing user access procedures and processes and publication of MetNet for internal staff review*

Staff Responsible: *Carah Koch, Shankar Veluvali, Nancy Jennings (Other ECM, HR, and IS staff yet to be determined), as well as Council Supervisors and Managers*

Timetable: *Completion- 3rd quarter 2015*

4. (Significant) Manually update Active Directory so all users can be easily identified in a single audit table.

Management Response: *Concur with the audit recommendation. Enterprise Content Management staff will review Active Directory data in Application Xtender and update user names as appropriate.*

Staff Responsible: *Carah Koch*

Timetable: *Completion-2nd quarter*

390 Robert Street North
St Paul, MN 55101-1805

651.602.1000
TTY 651.291.0904
public.info@metc.state.mn.us
metrocouncil.org