CITY OF VANCOUVER
INTERNAL AUDIT REPORT
Shadow IT Audit

Distribution:

Audit Committee	Tadhg Healy - Chief Technology Officer
Auditor General	Leo de Sousa - Director, Enterprise Technology
External Auditor	

EXECUTIVE SUMMARY

March 22, 2022

The audit assessed the effectiveness of processes in place to manage shadow IT. Shadow IT is the use of software or hardware without the knowledge of Technology Services. Users may be motivated to use shadow IT systems due to the innovative functionality that solutions provide. However, shadow IT may unintentionally introduce excessive cybersecurity, information privacy and compliance risks to the City.

Opportunities exist to further develop processes and to implement tools that minimize the risks and manage the potential value brought on by shadow IT. Shadow IT is a growing issue given the ease of acquisition and increasing availability of cloud-based solutions.

At the time of the audit, Technology Services was in the process of exploring solutions to better detect shadow IT and developing a process to handle unapproved IT purchases. To further these efforts, the following are the more significant findings and recommendations:

F.1 Define the process for removal of high-risk shadow IT

The Technology Lifecycle policy states that technologies that introduce an unacceptable level of risk to the City may be removed or disabled. However, the process for how technologies are removed is not defined. A documented process for removal of shadow IT, with defined risk assessment criteria, to inform the Risk Management Committee for review and decision-making would assist Technology Services in implementing the policy.

F.2 Communicate requirements for maintaining shadow IT systems

Risks from shadow IT systems could arise from inadequate maintenance of software. To reduce this risk, City departmental directors and managers should be educated on processes for adequately maintaining shadow IT. Examples of processes include user access management, data backup processes, and patch management.

F.3 Implement a shadow IT detection tool

With the number of users and endpoint devices managed by Technology Services, tools to detect shadow IT usage would enhance monitoring, identification, and risk assessment. Enhanced information could then be used to inform targeted security policies that restrict or limit access to high-risk services or applications.

Carmen Fuellbrandt, CPA, CMA, CIA, CRMA
Manager, Internal Audit

A. BACKGROUND

Shadow IT

Shadow IT is the use of software or hardware without the knowledge of Technology Services. This includes cloud-based applications that do not require installation on City devices or software that could be acquired without costs.

Risks of shadow IT

Shadow IT may unintentionally introduce excessive cybersecurity, information privacy and compliance risks to the City. Shadow IT systems are not subjected to the same evaluation criteria as systems that go through Technology Services systems intake channels.

Users may be motivated to use shadow IT systems due to the innovative functionality that solutions provide and the ease of acquiring such applications. Some shadow IT applications may be well-known and widely used, resulting in users not understanding the potential risks when used in an enterprise setting. In addition, there may be increased costs from solutions that provide similar functionality used by different departments or missed opportunities to bundle user licence fees for savings.

City policies require approval of new technologies

The City's Technology Acceptable Use (ADMIN-035) and Technology Lifecycle (ADMIN-039) policies outline the requirements for approval by Technology Services to approve technology purchases or implementations. The policies state the following:

- **Technology Acceptable Use policy**: *"All applications must be authorized and installed by Technology Services and meet the City standards, which are published through the ServiceNow service catalog. Staff are not permitted to use cloud software and web applications (e.g. Dropbox, Trello, etc) that aren't yet approved by Technology Services."*
- **Technology Lifecycle policy**: "*Technology purchased or implemented without approval from Technology Services, inclusive of purchases or subscriptions on City credit cards (purchasing cards), introduces an unacceptable level of risk and may be removed or disabled by Technology Services at the expense of the business unit. Future integrations and ongoing support may not be provided*."

Channels are in place to intake and approve new technologies

The City has processes in place to evaluate technology purchases to ensure criteria are met for requirements such as security, information privacy, and vendor viability. New technologies are also evaluated for appropriate integration with the City's enterprise architecture and technology roadmap. Once approved, Technology Services reviews and designates technology solutions as a "City standard" to ensure they are supported, maintained and protected from vulnerabilities on an on-going basis.

Continuing growth of shadow IT

The full extent and instances of shadow IT solutions that exist across the City is not known because shadow IT detection tools are not in place. While risks could arise from usage of shadow IT systems, they could also introduce opportunities for process improvements. With the increasing availability of software and ease of acquisition of cloud-based solutions, processes are required to minimize the risks and manage the potential value introduced by shadow IT.

B. SCOPE

The objective of the audit was to assess the effectiveness of processes in place to manage shadow IT. The scope of the audit focused on policies and procedures under the City's Technology Services department. Our work included:

- Interviews with members of the Technology Services and other business unit departments;
- Review of policies such as the Technology Acceptable Use, Technology Lifecycle, and Cybersecurity policies;
- Review of processes to intake, evaluate and approve new technologies;
- Walk-throughs of monitoring tools and workflow dashboards; and
- Sample review of technologies acquired through various purchasing channels.

The audit was not designed to detect fraud. Accordingly, there should be no such reliance.

C. CONCLUSION

Opportunities exist to further develop processes and to implement tools that manage shadow IT. Users may be motivated to use shadow IT systems due to the innovative functionality that solutions provide. However, shadow IT may unintentionally create excessive cybersecurity, information privacy and compliance risks to the City. With the increasing availability of software and ease of acquisition of cloud-based solutions, additional processes are required to minimize risks and manage the potential value introduced by shadow IT.

Findings and recommendations have been discussed with management and their responses were incorporated in this report. We thank Technology Services for their assistance with this audit.

D. RISK ANALYSIS

The potential significant risks considered if controls were not in place included:

- Inability to adequately secure the IT environment due to an unknown cyberattack surface introduced by shadow IT;
- Financial losses and reputational harm from data loss or system breaches;
- Delayed execution of business continuity plans from lack of operational data backups and processes that rely on shadow IT;
- System inefficiencies and incompatibilities of shadow IT systems with existing infrastructure; and
- Increased technology costs due to duplication of systems that provide similar functionality.

E. POSITIVE OBSERVATIONS

Technology Services has been working to address the growing risk of shadow IT by:

- Exploring processes and solutions to better detect shadow IT technologies.
- Developing a communication plan to City staff on the channels for IT purchases. This was a recommendation identified from the Employee Expenses internal audit report dated September 2021.
- Developing a process to handle unapproved IT purchases. This was also a recommendation identified from the Employee Expenses internal audit report dated September 2021.

F. AUDIT ISSUES, RECOMMENDATIONS AND MANAGEMENT RESPONSES

F.1 Define the process for removal of high-risk shadow IT

Policy outlines removal of high-risk technologies

The Technology Lifecycle policy (ADMIN-039) outlines that technologies that introduce an unacceptable level of risk to the City may be removed or disabled. Unacceptable levels of risk may be introduced from shadow IT systems related to inadequate security, incompatibility with enterprise architecture, misalignment with technology roadmaps, or vendor viability risks.

Define the process for removal of high-risk shadow IT

While the policy outlines the removal of high-risk technologies, the process and steps for how technologies are removed is not formally defined. In the past, Technology Services has had challenges with removing shadow IT solutions. There have been instances where departments have continued to use certain software despite being notified by Technology Services to discontinue its use. A defined process with documented risk assessment criteria to inform senior City leadership for review and decision-making would assist Technology Services in implementing the policy.

Recommendation:

F.1.1 The Director, Enterprise Technology should define the process for removal of shadow IT systems that exceed an acceptable level of risk from a technology perspective. The process should outline the risk criteria used to evaluate shadow IT systems and the escalation process for informing the Risk Management Committee for review and decision-making. This should be completed by December 31, 2022.

Management Response:

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

Management Action Plan:

Technology Services agrees with both the findings and the recommendations. The Director, Enterprise Technology will work with Supply Chain Management, Access to Information and Privacy, Finance Accounts Payable and internal Technology Services teams to define a process identifying and reporting shadow IT to the Risk Management Committee.

F.2 Communicate requirements for maintaining shadow IT systems

Shadow IT systems may not be adequately maintained

Risks from shadow IT systems could arise from inadequate maintenance of software. Technology Services provides support and maintenance for approved software on an on-going basis such as user access management and data backups. These processes are foundational to ensuring cybersecurity and data protection. However, shadow IT systems obtained without the knowledge or approval of Technology Services may not be supported in the same manner.

Departments should be educated on processes to maintain shadow IT

To assist with reducing the potential risks of shadow IT, City departments should be educated on the processes for adequately maintaining software. In cases where usage of shadow IT has been identified, the software may remain unapproved by Technology Services and will not have an allocation of Technology Services resources to maintain and support it going forward. Therefore, departments are responsible to ensure that these processes are in place to protect systems from cybersecurity threats and vulnerabilities. Processes that should be considered include:

- Maintenance of system authentication controls;
- User access management to remove terminated users;
- Regular data backup procedures and data retention plans;
- Updates and patch management schedules;
- Monitoring of cybersecurity incidents affecting the vendor;
- Licence management according to vendor requirements;
- Periodic review of vendor independent assurance reports; and
- Documentation of critical shadow IT in departmental business continuity plans.

Recommendation:

F.2.1 The Director, Enterprise Technology should communicate to City departmental directors and managers the requirements to adequately maintain shadow IT systems that are not approved by Technology Services. This should be part of a communication package outlining the appropriate channels for software purchases, including purchases of cloud software. This should be completed by December 31, 2022.

Management Response:

☑ Agree with the findings

☑ Agree with the recommendations

☐ Disagree with the findings

☐ Disagree with the recommendations

Management Action Plan:

Technology Services agrees with both the findings and the recommendations. The Director, Enterprise Technology will work with Supply Chain Management, Access to Information and Privacy, Finance Accounts Payable and internal Technology Services teams to create communication content that will be shared out to City management and staff.

F.3 Implement a shadow IT detection tool

Tools to detect shadow IT

Various tools exist to aid in the detection and discovery of shadow IT systems. Detection of shadow IT enables appropriate risk management and mitigation efforts. While security and network monitoring tools are in place, a solution to detect shadow IT has not been implemented.

Risks of undetected shadow IT

With the number of users and endpoint devices managed by Technology Services, tools to detect shadow IT usage would enhance monitoring, identification, risk assessment and review. Enhanced information could then be used to inform targeted security policies that restrict or limit access to high-risk services or applications.

Recommendation:

F.3.1 The Director, Enterprise Technology should implement tools to enhance the detection and discovery of shadow IT systems. Shadow IT systems identified from the tool should be included in the shadow IT inventory listing. This should be completed by December 31, 2023.

Management Response:

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

Management Action Plan:

Technology Services agrees with both the findings and the recommendations. The Director, Enterprise Technology will put forward a budget request for operating budget to fund a tool. Insufficient funding will delay the completion of this recommendation.

F.4 Inventory known shadow IT systems

Known shadow IT systems not centrally inventoried

Shadow IT systems may be discovered through various Technology Services channels. However, a central inventory of known shadow IT systems discovered is not formally maintained.

Inventory of known shadow IT assists with managing risks

An inventory of known shadow IT systems that includes a risk classification system would assist with appropriate risk management. Such details could be useful in evaluating the extent of impact introduced by a security vulnerability. In addition, an inventory list could enable a periodic re-evaluation of the solution for changing risks or technology intake criteria. Opportunities to reduce vendor subscription costs and bundle user licence fees could also be negotiated if multiple departments are using the same solution.

Recommendation:

F.4.1 The Director, Enterprise Technology should develop an inventory of known shadow IT systems that categorizes items based on risk. The inventory should be kept updated with newly identified systems, as well as legacy shadow IT systems. This should be completed by December 31, 2023.

Management Response:

☑ Agree with the findings ☑ Agree with the recommendations

☐ Disagree with the findings ☐ Disagree with the recommendations

Management Action Plan:

Technology Services agrees with both the findings and the recommendations. The Director, Enterprise Technology will work with Supply Chain Management, Access to Information and Privacy, Finance Accounts Payable and internal Technology Services teams to develop an inventory of known or detected shadow IT. The creation of this inventory will signal the

completion of this recommendation. The ongoing updating will become part of Technology Services Software Asset Management practices.