Office of the Auditor General

Follow-up to the 2017 Audit of Information Technology (IT) Remote Access

Tabled at Audit Committee

April 27, 2021

Table of Contents

Executive summary

The Audit of IT Remote Access was conducted in 2017 and resulted in seven recommendations. Subsequently a follow-up audit was included in the 2020 Audit Plan of the Office of the Auditor General (OAG), to review the status of the seven recommendations.

The recommendations are summarized as follows:

Recommendation #1: The Chief Information Officer (CIO) should ensure that the City's IT strategy incorporates remote access across all departments and services. The strategy should consider how individual departments connect and secure remote access to critical services. The IT strategy should address, where applicable, work needed to respond to prior IT audits undertaken by the OAG.

Recommendation #2: The City should ensure their new standard for remote access is adopted across all City departments and supported as a corporate service managed by a central security authority. The standard should clearly define the scope and boundaries of the Enterprise Computing Environment.

Recommendation #3: The City should take steps to ensure that a review and update of its IT policies is completed at least every two (2) years.

Recommendation #4: The City should develop and maintain a document or diagram which effectively describes city-wide IT network architecture across all departments and services. Changes to the architecture should be subject to CIO approval.

Recommendation #5: As remote access connections are made across City networks, departments and services, the City should create a central register of all remote access solutions employed corporately and within City departments. The register should identify the nature of the remote access, how it is isolated (or connected) to other City services network and any security considerations or requirements. Proposed changes to the register should be subject to CIO approval.

Recommendation #6: The City should take steps to strengthen its mobile device management including the implementation of additional technical security requirements and controls for remote access including:

- Establishing mandatory strong two-factor authentication; and
- Restricting ability of users to install unauthorized remote access solutions on City issued devices.

Recommendation #7: The City should evaluate and implement enhancements to their remote access security management and monitoring, including:

- Finalizing the implementation of use cases specific to monitoring remote access security incidents with their Managed Security Service Provider (MSSP); and
- Continuing to improve operational practices including vendor and employee account management and reconciliation.

The follow-up to the 2017 Audit of IT Remote Access assessed the status of completion for each recommendation, results of which are summarized in Table 1 below, along with the status asserted by Management at the outset of the audit. Details on the assessment and detailed findings are included in the detailed report section.

Table 1: Summary of status of completion of recommendations

Recommendation	**Management status as at August 2020**	**OAG status as at November 2020**
#1	Complete	Complete
#2	Complete	Complete
#3	Complete	Complete
#4	Complete	Complete
#5	Complete	Complete
#6	Complete	Complete
#7	Complete	Complete
Total	**7 Complete (100%)**	**7 Complete (100%)**

Conclusion

The follow-up audit of IT Remote Access has identified that all seven of the previous recommendations from the 2017 audit have now been addressed and are assessed as complete.

As remote access has become even more critical during the COVID-19 pandemic, the City has taken steps to formalize the related process and must continue to monitor access and perform regular risk assessment reviews of any exemptions to the Remote Access Standard.

Acknowledgement

We wish to express our appreciation for the cooperation and assistance afforded to the audit team by management.

Detailed report – Assessment of implementation status

To complete the assessment, the auditors reviewed key City policy and process documents, in relation to IT Remote Access, including the Information Security Policy; Remote Access Standard; Architecture Review Committee Terms of Reference; Remote Access Monitoring procedure; and other related documentation.

The auditors also conducted interviews with various ITS information security team members including the City CIO, Manager of Technology Solutions, Chief Information Security/Digital Risk Officer.

The following information outlines management's assessment of the implementation status of each recommendation as of August 2020 and the Office of the Auditor General's (OAG) assessment as of November 2020.

Recommendation #1

Table 2: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

The CIO should ensure that the City's IT strategy incorporates remote access across all departments and services. The strategy should consider how individual departments connect and secure remote access to critical services. The IT strategy should address, where applicable, work needed to respond to prior IT audits undertaken by the OAG.

Original management response:

Management agrees with this recommendation.

The CIO will take steps to incorporate remote access across all departments and services into the IT strategy by Q2 2018.

Management update:

August 2020

The CIO has ensured that remote access objectives are incorporated into the Zero Trust and ITS strategic objectives as a part of the Objective and Key Results (OKR) framework. Examples of how this strategy has been operationalized to ensure corporate-wide compliance include: a Multi-Factor Authentication requirement as part of any new technology initiative assessment and, that Remote Access Standards were finalized and communicated to all corporate users in XXXX.

OAG assessment:

The actions as described in the management update were assessed as complete.

The XXXX slide pack was reviewed which details the approach to adopt XXXX in relation to access to City resources and systems, which is a strategic objective being applied to the City. The traditional concept of remote access would therefore be viewed differently in a XXXX environment which moves away from the use of Virtual Private Networks (VPNs) and a single point of access. Although it is noted that applying a XXXX environment is a large undertaking which is yet to be implemented.

We observed that MFA is now a requirement listed on the Scoping Template Feb 2020, for all new requests for Active Directory access.

OAG requested additional evidence of MFA adoption within the City. A summary report by Management was provided which shows XXXX

It was also noted via information provided by Management that the Adoption rate will rise as the City has recently added XXXX.

An export of the XXXX MFA remote access was provided in an Excel spreadsheet which also showed approximately XXXX with MFA access in different forms such as XXXX.

The following Mitigation Measures were provided by Management for cases where MFA may not be in use:

- Actively work with vendor to setup MFA.
- Upgrade XXXX to latest version to prepare for MFA implementation.
- Advise client to connect to XXXX first then using XXXX.
- Identify MFA requirement on new initiatives during business intake process.

Recommendation #2

Table 3: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

The City should ensure their new standard for remote access is adopted across all City departments and supported as a corporate service managed by a central security authority. The standard should clearly define the scope and boundaries of the Enterprise Computing Environment.

Original management response:

Management agrees with this recommendation.

The Technology Risk Security Management authority will ensure that the 'Technology Security Standard - Remote Access Service' is adopted across all City departments and supported as a corporate service managed by a central security authority by Q2 2018.

Management update:

August 2020

The Remote Access Standard and related practices and controls were communicated to all technology partners and staff in February and March 2020.

OAG assessment:

The Technical Security Standard for Remote Access Services was reviewed. The standard defines the scope as "all technologies used in the implementation, operation and management of Remote Access Services that support remote connections to the City of Ottawa's enterprise computing environment. The City's enterprise computing environment includes those environments managed and operated by Federated Partners and any third parties that store or transmit City data."

The Standard is Approved by the CIO and the content is controlled by the Manager, Technology Security Branch. Any exceptions need to be approved by both the CIO and the GM/Director of the business unit seeking the exemption.

A presentation on RAS Governance was presented to Technology Partners including from XXXX in February and March 2020.

Recommendation #3

Table 4: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

The City should take steps to ensure that a review and update of its IT policies is completed at least every two (2) years.

Original management response:

Management agrees with this recommendation. The CIO will take steps to ensure that by Q4 2018, all policies will be refreshed, whereby a further two-year update cycle will be implemented.

Management update:

August 2020

The CIO took steps to ensure that all policies were refreshed and updated and, a two-year update cycle has been implemented. The Objectives and Key Results (OKR) for the Technology Security Branch include a review of the policies and standards on a two-year cycle.

At the time of this response, two IT policy documents are being reviewed and updated per the two-year review cycle (Responsible Computing Policy and Corporate ITS Security Standards). The remaining policies owned by IT Services were updated in 2019 and are scheduled for review in 2021.

OAG assessment:

A spreadsheet XXXX was reviewed and noted that of the 8 policies and standards listed, 5 were last reviewed in 2019 and are scheduled for review in 2021. However, the Responsible Computing Policy was last reviewed 30th Jan 2018 and an update has been drafted as part of the 2020 ITS work plan.

It was noted that the Technical Security Standard for Remote Access Services has not been updated since August 1st, 2017 when it was issued, however the original finding relates to policies rather than standards, hence this recommendation is marked as complete.

Recommendation #4

Table 5: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

The City should develop and maintain a document or diagram which effectively describes city-wide IT network architecture across all departments and services. Changes to the architecture should be subject to CIO approval.

Original management response:

Management agrees with this recommendation.

The CIO will take steps to ensure that city-wide IT network architecture across all departments and services will be documented and the documentation maintained by Q3 2018. Changes to the architecture will be processed through a review structure for approval.

Management update:

August 2020

The CIO has implemented a range of functions and initiatives to support the regular maintenance of architecture diagrams and mature the overall practice, including:

1. Ensuring that an up-to-date reference architecture is completed, which includes infrastructure and network standards within it;
2. Establishing an Architecture Review Committee to evaluate technology risk and major architectural changes across the city-wide infrastructure; and
3. Establishing full change control over all infrastructure, network and appliance assets by way of the IT Change Management Policy and supporting Change Advisory Board.

Remote Access architecture diagrams for ITS and Technology Partners are documented and maintained per these processes (completed September 2019).

OAG assessment:

The XXXX document was reviewed which details the technical architecture and systems in use at the City of Ottawa. It was noted that this document does not contain any document control, however it does have the date 2020 on the cover, but also states "Request for Proposal". If this document is considered a formal reference architecture document, then appropriate document control should be applied so that updates and modifications are tracked and recorded.

The Architecture Review Committee Terms of Reference document (dated November 20th, 2019) was reviewed. It was noted that the ARC meets bi-weekly and on an 'ad hoc' basis. The ARC is sponsored by the CIO and chaired by the Lead for Enterprise Architecture. Delegates with appropriate decision-making authority are listed as:

Assigned delegates with appropriate decision-making authority are listed as the following:

- Business Architect, Data/ Information Architect, Application/ Integration Architect, Technology/ Infrastructure Architect, Security Architect
- XXXX Architects
- XXXX Architects
- XXXX Architects
- XXXX Architects
- Product Owners

Additionally, the ARC ToR details the voting procedure for making the Architectural related decisions or approvals.

The ITS Change Management and Configuration Management Process and Procedures was reviewed (v2.1) which was last updated in October 2019. The document details the Change Management procedure including the four types of Requests for Change (RFCs) which include: XXXX change. The Change Advisory Board (CAB) meet weekly on XXXX Scheduled, approved and completed RFCs are visible on the Forward Schedule of Change, for members of the CAB to review.

Recommendation #5

Table 6: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

As remote access connections are made across City networks, departments and services, the City should create a central register of all remote access solutions employed corporately and within City departments. The register should identify the nature of the remote access, how it is isolated (or connected) to other City services network and any security considerations or requirements. Proposed changes to the register should be subject to CIO approval.

Original management response:

Management agrees with this recommendation.

The CIO will create the capability to register remote access solutions including their attributes and relationships across all City departments. A mechanism will be developed to track, monitor and approve changes to the solutions registered, by Q1 2019.

Management update:

August 2020

The Configuration Management Database (CMDB) has been updated to identify all Remote Access Solutions (RAS). Each RAS has a Configuration Item (CI) created in CMDB, and the CI is linked to a remote access diagram. A change management process is in place and training was completed in December 2019 by all technology partners.

OAG assessment:

The RAS CI spreadsheet containing contents from the CMDB was reviewed which lists XXXX diagram listed. Upon enquiry, an additional request was made in relation to documenting the nature of the remote access, how it XXXX. Additional evidence was provided in the spreadsheet entitled XXXX where appropriate, for the related remote access systems. It was noted that not all systems have a related Parent or Child CI. A further enhancement would be to include where it is 'not applicable' to have a Parent or Child CI, so it is clearer to ascertain if this has been completed or missed.

Recommendation #6

Table 7: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

The City should take steps to strengthen its mobile device management including the implementation of additional technical security requirements and controls for remote access including:

- Establishing mandatory strong two-factor authentication; and
- Restricting ability of users to install unauthorized remote access solutions on City issued devices.

Original management response:

Management agrees with this recommendation.

The CIO will implement the appropriate controls to detect, respond and prevent incidents of unauthorized access, including strong two-factor authentication for RAS connections and monitoring/restricting the use of unauthorized remote access solutions. This will be completed by Q4 2019.

Management update:

August 2020

Mobile device management is in place. Multi-Factor Authentication (MFA) deployment has been completed XXXX. This is being addressed through the addition of an existing product licence expansion. XXXX is defined, and restriction is handled through security technology operations.

OAG assessment:

Multi Factor Authentication has been implemented as part of the Conditional Access policy for MFA for Remote Access from XXXX. A screenshot of this access was observed.

A spreadsheet of the XXXX was also provided which contains the related Risks and the mitigations for exemptions to the RAS Standard. XXXX. Each Mitigation has a Risk Owner allocated.

It was noted that while there is an allocated Risk ID, there are no dates included in the spreadsheet for review or re-assessment of the risk and related mitigation.

Recommendation #7

Table 8: Status

Management update	OAG assessment
Complete	Complete

Audit recommendation:

The City should evaluate and implement enhancements to their remote access security management and monitoring, including:

- Finalizing the implementation of use cases specific to monitoring remote access security incidents with their MSSP; and
- Continuing to improve operational practices including vendor and employee account management and reconciliation.

Original management response:

Management agrees with this recommendation.

The CIO will ensure use cases specific to monitoring remote access security incidents with the ITS MSSP are implemented by Q4 2019. Operational steps will be implemented to improve vendor account management and ensure reconciliation of accounts is maintained.

Management update:

August 2020

Security monitoring within the ITS MSSP is in place for use cases specific to remote access. Account management and reconciliation of internal staff and contractors is managed by the City's Enterprise Directory System (EDS), which has had major updates to automatically provision and disable accounts based on SAP data changes. This XXXX systems to keep them in sync. MFA has also been implemented corporate-wide.

OAG assessment:

Management have stated that security monitoring is in place at the XXXX.

On review of Page 2 of the Information Security Administrative Procedures it was noted that the XXXX.

In relation to the recommendation for improving operational practices, there are weekly meetings for Security Operations XXXX and weekly ITS meetings XXXX. Minutes for the Weekly Operations meeting on August 24th were observed, which included a discussion on Remote Access.

XXXX. A screenshot was provided by management to show the daily reports being produced. Additionally, a Marval case relating to a review of XXXX was also provided.

XXXX.

Table 9: Status legend

Status	Definition
Not started	No significant progress has been made. Generating informal plans is regarded as insignificant progress.
Partially complete	The City has begun implementation; however, it is not yet complete.
Complete	Action is complete, and/or structures and processes are operating as intended and implemented fully in all intended areas of the City.
Unable to assess	Action is not currently taking place; however, remains applicable.