Office of the Auditor General: Audit of Information Technology (IT) Remote Access, Tabled at Audit Committee – November 30, 2017

Table of Contents

Acknowledgments

The team responsible for this audit, conducted by Orbis Risk Consulting, under the supervision of Sonia Brennan, Deputy Auditor General and the direction of Ken Hughes, Auditor General, would like to thank those individuals who contributed to this project, and particularly, those who provided insights and comments as part of this audit.

Original signed by:

Auditor General

Audit of IT Remote Access – at a Glance

What we examined

The audit examined the extent to which the City of Ottawa (the “City”) was effectively identifying and mitigating risks, including security risks, associated with providing remote access (RA) to the City’s Information Technology (IT) network. We also looked at how the City supports availability and performance of RA and provides timely and effective support to users.

Why we did this audit

The City is increasingly dependent on technologies that allow employees and other authorized users to access the City’s network from remote locations. While supporting efficiency and effectiveness in a number of business situations, remote connections also increase the risk of unauthorized access. Unauthorized access can lead to data loss or corruption, exposure of private or confidential information and service interruptions.

What we concluded

We concluded that weaknesses and gaps in security practices and controls designed to prevent incidents of unauthorized RA expose the City’s information systems to a range of potentially significant risks including data loss or corruption, exposure of private or confidential information and service interruptions. These issues include weaknesses in the technical security practices and controls that the City depends on to detect, respond and prevent incidents of unauthorized access. With the pace of technological change and the City’s increasing dependence on remote access, it is imperative that the City fully responds to the recommendations in this report, and complementary recommendations in previous IT audits, in a timely manner.

What we found

While the City has taken initiative to improve aspects of RA controls, risk management and governance, including the planned implementation of a new information security standard, we found weaknesses and gaps that require timely attention. The range of our findings extends from a lack of formal strategy for RA to concerns related to specific technical matters as described below:

Remote access technology strategy – The City does not have a strategy to direct and inform its RA related priorities, investments and decision making. Further, since management of the City's RA-related risks is not managed by a central authority, there is higher likelihood that these risks will not be optimally managed in a consistent manner.

Recommendation – 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.

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.

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.

Remote access architecture – We found that the City has not developed an inventory of its RA technologies and connections nor has it developed a comprehensive map showing the technologies, connections and nature of information moving between the City's network and the remote connection. Without such an inventory and map, it is very difficult to establish that RA technologies and connections are appropriate and authorized, and to confirm that appropriate security measures are in place.

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.

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.

Remote access security gaps – While the audit identified various security measures, we found weaknesses and gaps in certain technical aspects of RA security. [redacted]

[redacted]

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.

- [redacted]
- [redacted]

Monitoring and oversight – We found that the City had entered into a contract with a new “Managed Security Service Provider” (MSSP) in June 2016. [redacted] We also found that the City has not yet implemented plans to conduct routine monitoring and testing such as vulnerability assessments, penetration testing and reconciliation of RA accounts. Such monitoring and testing activities are critical to ensuring that RA risks, which change over time, are identified and assessed in a timely manner.

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

- [redacted]
- Continuing to improve operational practices including vendor and employee account management and reconciliation.

Executive Summary

Introduction

The Audit of IT Remote Access was included in the 2016 Audit Plan of the Office of the Auditor General (OAG), approved by City Council in November 2015.

Background and context

As with most organizations, the City of Ottawa (the “City”) has increasingly leveraged technology to support the achievement of a variety of operational and strategic objectives. One of the many ways that technology has evolved over the last several years is the ability of City employees and other authorized users to access the City’s Information Technology (IT) network from locations other than from workstations in City offices. This access has greatly improved the efficiency and effectiveness of workflow in a number of business scenarios and across a variety of users. Remote Access (RA) is no longer viewed as an option; rather, it is considered an essential business component in supporting the IT needs of mobile workers (such as paramedics and by-law officers), vendors (who use RA to conduct maintenance and to monitor applications and systems) and teleworkers, to name just a few.

As business needs and the related benefits of RA continue to trend upward, so has the associated risk. From the proliferation of certain technologies, such as smart phones, to the increase in RA options, the likelihood of unauthorized access is also trending upward. Any such unauthorized access could potentially lead to a number of damaging outcomes including: data loss or corruption, exposure of private or confidential information and service interruptions. In this environment, the City must be proactive in its approach to managing risks and opportunities associated with new technologies. This includes taking steps to ensure that its policies, requirements, guidelines and practices balance business benefits with the need to ensure that both new and existing RA technologies and tools are sufficiently secure.

The City has established a framework of policies and requirements with implications for RA including the *Responsible Computing Policy*, *Information Security Policy*, *Technology Devices Policy*, as well as the *Employee Code of Conduct* to name a few. Included in the suite of IT policies is the *Remote Access to City Network Policy* (RACN Policy) which was established in 2006 and applies to all City employees who require RA. The RACN Policy, last updated in 2012, establishes the user responsibilities, authorization processes and security safeguards that enable secure RA, by authorized staff, to the City network. It also identifies the various service offerings[1] provided by the City’s Information Technology Services department (ITS) in support of RA. At the time of this audit, ITS was in the process of completing a comprehensive review and update of the City’s IT policy framework, including the RACN Policy. This initiative led to the drafting of a number of new technology security standards including a new Information Security Standard - Remote Access Services (ISS-RAS). As described later in this report, the ISS-RAS addresses some important gaps in the existing policy framework and provides greater clarity regarding responsibilities and the authority of the Chief Information Officer (CIO). Clarification of CIO’s authority under the draft ISS-RAS is particularly important in light of the customized RA solutions that exist within certain areas such as OC Transpo, Water Services, Traffic Services and the Ottawa Public Library, etc. where Independent Technology Groups (ITGs) exist. This new standard had not yet been implemented as of the completion of our audit work.

As referenced above and described further in this report, concerns related to governance, including roles, responsibilities and authorities, have contributed to a number of the observations raised by this audit. The OAG has completed several IT audits over the last few years where observations highlighted governance issues as a contributing factor underpinning many of the audit findings and recommendations described in this report. Prior audits included the Audit of IT Governance (2014), Audit of IT Risk Management (2015) and the Audit of IT Security Incident Handling and Response (2015). Each of these audits identified risk factors that were linked to the existence of proprietary technology or systems that are managed by ITGs[2] rather than centrally by ITS. This condition makes it difficult for the City to support consistent enterprise-wide IT strategies and requirements, including those related to security. These audits also highlighted challenges associated with a systemic lack of continuity in the CIO position. While this audit of RA was not designed as a follow up to any prior IT audits, both of these conditions continue to exist in 2017. These ongoing conditions increase the risk associated with RA and have been identified as contributing to many of the audit findings and recommendations described in this report. During the course of this audit, the OAG engaged with ITS on the linkage between prior audit findings and

[1] The following service offerings are described in the RACN Policy: Web Mail, BlackBerry^{TM}, Virtual Private Network (VPN) i.e. access from a City owned Laptop, and Remote Desktop – i.e. access from an employee’s personal computer.

[2] As described later in this report, the existence of ITGs does not preclude ITS’s involvement in proprietary systems and technology only that such involvement was not governed by formal authority.

the results of this audit and has encouraged ITS to remain diligent in addressing prior IT audit recommendations. As per the City's audit protocol, the OAG continues to take steps in support of the active monitoring and follow up of ITS's response to prior audit findings.

Audit approach and methodology

The overall objective of this audit was to provide an independent assessment of the adequacy and effectiveness of key systems, practices, procedures and governance in place to identify and mitigate risks, including security risks, associated with providing remote access to the City's network. Priority areas were as follows:

- Use of remote access;
- Roles and responsibilities for granting remote access;
- Remote access architecture and technology; and
- Remote access operations and monitoring.

Audit criteria were established based on leading IT Remote Access guidance, such as that published by the National Institute of Standards and Technology (NIST) including relevant elements of the NIST Cybersecurity Framework[3].

Scope

The scope of this audit included remote access[4] offered to authorized users through the following means:

1. Virtual Private Networks including:
    a. Internet Protocol Security ("IPSec")
    b. Encrypted Links (Secure Socket Layer "SSL")
2. Remote control connections, including Citrix and Remote Desktop solutions;
3. Mobile connectivity (Blackberries^{TM}, other smartphones, tablets, etc.); and
4. Web-based remote access including Outlook Web Access (OWA).

[3] "Framework for Improving Critical Infrastructure Cybersecurity", 2014

https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[4] The audit did not include access or communication gateways that do not interface directly with the City network (e.g. radio or other communications systems).

Our examination included controls within ITS and across all City business lines and departments where RA capabilities exist, including those areas where ITGs exist.

For greater certainty, the scope of this audit did not involve an assessment of remote office VPNs nor access provided to Council members.

Summary of key findings

The findings in this audit report have been grouped according to the audit criteria. There are four resulting areas of findings:

- Strategy
- Inventory and Data Flows
- Security Gaps
- Monitoring and Oversight

Remote access technology strategy

In the OAG's 2014 Audit of IT Governance, it was noted that the City had developed a Technology Roadmap that provided insight to IT priorities, initiatives and objectives. However, that audit also raised concerns regarding the lack of clear alignment between IT investments and the City's strategic and business priorities. This audit found that the City had not yet addressed these concerns nor had it refreshed the Technology Roadmap since the 2013-16 version. It also confirmed that there are no plans to develop an RA Technology Strategy that would serve to support a consistent, city-wide, approach to RA priorities and decision making, and support clear ownership and management of RA-related risks. An RA Technology Strategy would also support the articulation of a clear vision for an efficient and enterprise-wide approach to remote access, including the need to balance business needs with security requirements and align planning/decision making around emerging areas such as mobile technologies.

The absence of a formal RA Technology Strategy with city-wide application was identified during this audit as a contributing factor related to findings associated with:

- Ownership and management of RA-related risks impacting the security of the overall network;
- Roles, responsibilities and accountabilities; and
- Governance/decision-making.

While the audit identified that roles, responsibilities and accountabilities at the operational level (e.g. RA account administration, approvals, risk assessments, etc.) are generally clear and often supported by formal procedures and checklists, concerns were identified at the higher level. Specifically, the audit identified that ownership of the City's RA-related risks, roles, responsibilities and accountabilities has not been clearly established across City departments and at the corporate level. This observation is consistent with the OAG's 2015 Audit of IT Risk Management which identified a similar concern regarding the CIO's authorities and responsibilities for city-wide IT risks.

The audit found that, within its traditional areas of responsibility, ITS plays an effective and appropriate role in the monitoring[5], oversight and mitigation of RA-related risks. However, as identified as a concern in various prior OAG audits, ITS's role does not formally extend to departmental RA deployments managed by ITGs. For these deployments, ITS's involvement may vary from no or limited involvement to significant involvement in all aspects of the initiative including the requisite decision making. This ongoing situation limits ITS's ability to have a holistic view of the City's RA technology in support of economical and effective strategic, and operational, planning and risk management. In the absence of a central authority with a holistic view of RA technologies, there is a significantly increased likelihood that RA-related risks will not be managed consistently across the organization, leaving the City's Network exposed to unintended security gaps or duplications.

Notwithstanding the concerns related to the lack of a city-wide RA Technology Strategy that effectively informs the City's vision for RA, the audit noted the existence of a number of initiatives that will help to address the concerns raised in this report. As noted in the Background and context section, ITS is in the process of completing a comprehensive review and update of the City's IT policy framework. This includes replacement of the existing Remote Access to City Network Policy which was identified as being both outdated and largely ineffective. The proposed new ISS-RAS Standard was found to provide good technical coverage for RA requirements related to monitoring, testing and patching, among others, and it provides clear expectations for end users regarding appropriate use. The draft standard also clearly indicates that it applies to all RA services that support remote connections to the "City's Enterprise Computing Environment" which includes those environments managed by ITGs and any third parties. It also clarifies that the CIO is required to sign off on any requested exclusions from the mandatory nature of the ISS-RAS. These are important elements

[5] Monitoring of compliance is a shared responsibility between each department (e.g. monitoring non-City employee accounts) and ITS (e.g. monitoring citywide dormant accounts).

that will help to address some of the concerns raised in this audit and in prior audits[6]. Approval and implementation of this new standard (which has been in draft form since 2016) will be a key step in addressing existing RA-related control weaknesses and inconsistencies across the City.

Remote access architecture – Inventory and data flows

Given the increasing reliance on RA to support business operations including critical functions, the audit expected there would be a formally documented Enterprise Remote Access Architecture that would provide a comprehensive view of all RA connections across the City. Such a document would provide information on (1) how RA devices across all City departments interface; (2) the remote technologies in place, including those relevant to SCADA or proprietary applications with remote connectivity; and (3) the related data flows (i.e. the nature, such as volume or sensitivity, of information moving between the City's network and the remotely connected device).

The audit found that the City has not documented its Enterprise Remote Access Architecture, nor has it developed a comprehensive inventory of its RA technologies, connections and data flows at a city-wide level, including departmental implementations where ITS was not involved. While there is no enterprise-wide architecture, there was evidence of documented architecture pertaining to specific corporate RA services (including the City's VPN Infrastructure, Blackberry^{TM} infrastructure, Remote Desktop connectivity) and an inventory of City owned laptops and Smartphones. We also understand that ITS has recently developed plans and assigned responsibility to build a central repository of RA risks and technologies. At the time of the audit, however, there were a number of potentially significant implications associated with not having a comprehensive enterprise inventory including an inability to develop and leverage effective strategic planning.

In the absence of effective strategic planning, there is an increased likelihood that investments in RA technologies, services and procedures will not be coordinated and result in unnecessary or ineffective investments and ineffective security measures. At the operational level, this gap increases the likelihood of a variety of negative outcomes including: security or regulatory (e.g. privacy) breaches resulting from non-conforming remote connections, delays in identification of such breaches and the use of unauthorized RA platforms. Finally, the new ISS-RAS states that it applies to information technologies that support connections to the City's "Enterprise Computing

[6] As noted earlier, this audit was not designed as a follow-up to any prior IT audits conducted by the OAG.

Environment”. However, that “environment” needs to be clearly defined to avoid the likelihood of inconsistent interpretation by different groups across the City.

IT remote access security gaps

While providing reliable and highly available RA is a business imperative in the current environment, there are information technology security risks which are inherent in RA. These include potential breaches of confidentiality, integrity or availability. Mitigation and management of these risks requires that the City’s technical security practices and controls can detect, respond and prevent incidents of unauthorized access to information via RA services (i.e. VPN, Remote Desktop, smartphones). These practices and controls should reflect a consideration of both the City’s business requirements and the need for adequate security measures. In reviewing these security measures, the auditors considered the following contexts:

- Endpoint devices (i.e. the laptop or smartphone, used to access the City’s network) – devices need to be configured and secured against unauthorized and other potentially risky activities. A secure endpoint device will be encrypted, require strong passwords, incorporate malware prevention and is centrally managed with a locked-down configuration.
- Network architecture – The City must prevent unauthorized remote connections to the corporate network. The network design and architecture must ensure that departments with critical infrastructure have isolated it from RA through the corporate network.
- Support services – the support provided to RA users should promote a high degree of availability (including after-hours service) while reflecting appropriate security measures (e.g. validation of the user’s identity prior to providing service) and compliance with standards.
- Operational monitoring and incident detection – monitoring of RA traffic and activities should identify and escalate, as applicable, security anomalies, alerts and potential security incidents. The controls examined by the auditors include those outsourced by the City to a Managed Security Service Provider (MSSP).

The audit addressed the security measures referenced above through a series of technical tests which included the use of a City issued laptop and Blackberry™ smartphone which were used to connect to the City network via RA. The testing also involved the use of non-City issued devices that were used to identify exposures to unauthorized network access and functionality.

Testing conducted on City issued devices revealed a number of effective security measures while also evidencing resilient RA systems capable of supporting high levels of availability. The auditors noted that default architecture ensures that critical infrastructure remains isolated from the corporate network. In terms of specific security measures, the City issued laptop was found to be considerably more secure than the smartphone. The laptop provided effective controls to prevent bypass of restrictions (e.g. passwords) or elevate the user's access to beyond what was authorized. Among other effective features, the laptop was configured with updated security software, featured full disk encryption, and did not allow the unauthorized export of VPN software to a non-City laptop.

Among the other positive results of the testing in this area, the audit team's testing of City RA systems revealed that the RA network architecture did not exhibit significant vulnerabilities to unauthorized access. Authorized users were also found to be restricted in terms of access and functionality when connecting non-City owned devices via RA. In addition, audit testing concluded that the City has established RA management operating procedures suitable for end user support and effective account administration.

However, the audit testing also yielded concerns related to weaknesses and gaps in the RA security environment. The existence of these weaknesses or gaps could compromise the City's ability to prevent, detect and respond to incidents, including unauthorized access. Specifically, the audit identified the following concerns related to the technical aspects of RA security:

- City issued mobile devices are not sufficiently secured;
- [redacted]
- [redacted]
- Security monitoring has not been optimized to detect and respond to RA security breach scenarios.

These are further described below.

Audit testing conducted using the City issued smartphone[7] revealed that the mobile device was configured with the latest Blackberry™ operating system and various security measures, including Blackberry's "balance" feature to separate work and personal spaces. Further, the City's device management system generated an email alert to the user when anomalous activity[8] was detected. However, the device was not considered to be sufficiently secure in light of the weaknesses and gaps identified.

- [redacted]
- [redacted]
- [redacted]
- [redacted]

As with the City issued smartphone, testing of the City issued laptop confirmed that core security safeguards were implemented, including encryption, restricting administrative access, current antivirus software and current operating system patches.

[redacted]

[7] The City is in the process of replacing its Blackberry™ devices, including the one used for audit testing. However, the findings identified in this audit will not be impacted by these changes and remain relevant following the change.

[8] In this case, the alert indicated that the device was no longer enabled with services that support policies and security settings intended protect the City's information and network and that their cell service may be suspended if the situation was not rectified.

[redacted]

[redacted]

The audit also examined authentication controls that are intended to assure that users are who they claim to be. Authentication can be validated by a combination of factors; the more factors required, the stronger the control. For example, the requirement for a password would be a one-factor authentication. Two-factor could be a password in combination with digital certificate, while three-factor would also include a biometric (e.g. a fingerprint or retinal scan). [redacted]

Passwords are susceptible to theft and misuse. [redacted]

The City's efforts [redacted] no longer reflects the industry standard and increases the risk of unauthorized users gaining access to the network.

As part of the technical testing, the audit team also created security incidents using malware, containing a non-functional virus, to determine if the City's security technologies would detect and block the attempted security breach. While one of the tests was successfully detected, reported and blocked, similar other tests were not detected, reported or blocked. Had this been a malicious attack, the City's Network would have been susceptible to the hacker's objective.

Monitoring and oversight

Preventing security incidents, while providing reliable and available RA, is an important objective. Notwithstanding, it is a near certainty that security incidents will occur. Whether malicious in intent or otherwise, we expected that the City would have formal and effective capabilities that would support timely detection and response and escalation in the event of actual or potential security events or other circumstances that

[redacted]

threaten the availability of RA services. Further, we expected to see an effective regime of oversight whereby: RA solutions that are being considered for implementation are subject to risk assessments and are tested for vulnerabilities; practices, roles and responsibilities for managing RA accounts are effective and appropriate; and where effective and timely incident reporting is used in support of continuous improvement.

Consistent with the observations in the OAG's 2015 Audit of IT Security Incident Handling and Response, this audit revealed that the City has incident monitoring, detection and escalation capabilities which include RA applications. While these capabilities continue to lack maturity, as highlighted in the 2015 audit, there were also signs of improvement over the last two years. For example, in 2016 the City entered into a contract with a new Managed Security Service Provider (MSSP) with the objective of improving service delivery and value add compared to its previous arrangement. We also identified ITS's comprehensive review and update of the City's IT policy framework; particularly, the development of a proposed new ISS-RAS as representing a potentially significant improvement in the oversight and control of RA solutions through the enforcement of mandated risk assessments. Also of note, was the audit's findings that effective and formal practices were in place regarding the granting of RA and that practices in support of the effective RA account administration; for example, the periodic reconciliation of users had been improved.

Notwithstanding the improvements referenced above, the audit revealed some gaps and weaknesses in the City's ability to detect and respond to security threats and vulnerabilities related to RA. Specifically, the audit identified the following concerns related to monitoring and oversight:

- [redacted]
- There has not been focused third party penetration testing of remote points to identify possible issues[11].

These issues are further described below.

In June 2016, the City entered into a contract with a new MSSP provider. During the audit, it was identified that the City and the new MSSP are still in the process of implementing the new service arrangement. [redacted]

[11] This observation is mirrored in the 2015 Audit of Security Incident Handling and Response whereby it was recommended that the CIO conduct penetration testing on all critical infrastructure.

[redacted] Industry standards suggest this process would normally take less than three (3) months which is considerably less time than the City's experience.

Use cases describe specific scenarios and vulnerabilities that the MSSP would be expected to identify through monitoring. They would also provide the basis for the nature and scope of RA activity logs that should be collected and the types of RA activity (or "traffic") the MSSP is responsible to monitor. The MSSP has implemented standard use cases under their contract with the City. [redacted]

As part of the technical testing, the audit conducted vulnerability scans of the City's RA servers. While these scans did not identify any significant vulnerabilities, they were not designed to provide the level of assurance that would be provided by a focused vulnerability assessment or penetration test conducted by a third party. Consistent with findings from the 2015 Audit of IT Security Incident Handling and Response, it was noted that vulnerability assessments and penetration testing was not routinely conducted[12] on all corporate and departmental RA solutions. Interviews with ITS personnel further indicated that ITS has historically performed risk assessments on RA solutions on a case-by-case basis based on the perceived level of risk. This existing weakness is addressed by the proposed new ISS-RAS which requires that vulnerability assessments on RA technologies are conducted two times a year, and threat/risk assessments be conducted at least once every three years. As referenced in Recommendation 2, staff are encouraged to implement this new standard as soon as possible.

Audit interviews and document review results indicated that reconciliation of RA accounts[13] (those provisioned to non-City employees) had not been completed in a

[12] The audit team noted that the new CITRIX VPN solution, scheduled for implementation in 2017, had undergone a vulnerability assessment.

[13] These are accounts held by Non-City Employees (NCE), including contractors and vendors that require RA as part of their responsibilities.

timely manner. However, during the course of the audit, ITS commenced an initiative to reconcile its database of third parties with RA to ensure the access was still required and that relevant information was current and accurate (e.g. contract end dates, contact names within the relevant City business line, etc.). The audit team understands that this improvement to RA account administration will be sustained with periodic reconciliation to ensure account access is limited to appropriate and authorized users.

Recommendations and responses

Recommendation #1

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

[redacted]

Management response:

Management agrees with this recommendation. The CIO will implement the appropriate controls [redacted] for RAS connections. [redacted] This will be completed by Q4 2019.

Recommendation #7

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

- [redacted]
- Continuing to improve operational practices including vendor and employee account management and reconciliation.

Management response:

Management agrees with this recommendation. [redacted] Operational steps will be implemented to improve vendor account management and ensure reconciliation of accounts is maintained by Q4 2019.

Conclusion

Ottawa is a modern and connected city with growing dependencies on information and communication technologies. Protecting the City's network and critical technology infrastructure from unauthorized remote access is a crucial component of an effective cyber security strategy. As detailed in this report, the audit revealed a number of weaknesses and gaps which expose the City to a range of potentially significant risks to IT security, reliability and service delivery. [redacted] With the pace of technological change and the City's increasing dependence on remote access, it is imperative that the City fully responds to the recommendations in this report, and complementary recommendations in previous IT audits, in a timely manner.

Notwithstanding the identified issues and related risks referenced above, we acknowledge that the City has demonstrated a high level of remote access availability and has taken initiative to improve aspects of remote access controls, risk management and governance. This includes the development of a new information security standard that will help address ongoing concerns linked to the lack of central authority and responsibility for the management of remote access related risks.

The detailed section of this report is currently available in English only. The French version will be available shortly. For more information, please contact Ines Santoro at 613-580-2424, extension 26052.

La partie détaillée de ce rapport n’existe qu’en anglais. Elle sera disponible en français sous peu. Pour tout renseignement, veuillez communiquer avec Ines Santoro, 613-580-2424, poste 26052.

Detailed audit report

Audit of IT Remote Access

Introduction

The Audit of IT Remote Access was included in the 2016 Audit Plan of the Office of the Auditor General (OAG), approved by City Council in November 2015.

Background and context

As with most organizations, the City of Ottawa (the “City”) has increasingly leveraged technology to support the achievement of a variety of operational and strategic objectives. One of the many ways that technology has evolved over the last several years is the ability of City employees and other authorized users to access the City’s Information Technology (IT) network from locations other than from workstations in City offices. This access has greatly improved the efficiency and effectiveness of workflow in a number of business scenarios and across a variety of users. Remote Access (RA) is no longer viewed as an option; rather, it is considered an essential business component in supporting the IT needs of mobile workers (such as paramedics and by-law officers), vendors (who use RA to conduct maintenance and to monitor applications and systems) and teleworkers, to name just a few.

As business needs and the related benefits of RA continue to trend upward, so has the associated risk. From the proliferation of certain technologies, such as smart phones, to the increase in RA options, the likelihood of unauthorized access is also trending upward. Any such unauthorized access could potentially lead to a number of damaging outcomes including: data loss or corruption, exposure of private or confidential information and service interruptions. In this environment, the City must be proactive in its approach to managing risks and opportunities associated with new technologies. This includes taking steps to ensure that its policies, requirements, guidelines and practices balance business benefits with the need to ensure that both new and existing RA technologies and tools are sufficiently secure.

The City has established a framework of policies and requirements with implications for RA including the *Responsible Computing Policy*, *Information Security Policy*, *Technology Devices Policy*, as well as the *Employee Code of Conduct* to name a few. Included in the suite of IT policies is the *Remote Access to City Network Policy* (RACN Policy) which was established in 2006 and applies to all City employees who require RA. The RACN Policy, last updated in 2012, establishes the user responsibilities, authorization processes and security safeguards that enable secure RA, by authorized staff, to the City network. It also identifies the various service offerings[14] provided by the City's Information Technology Services department (ITS) in support of RA. At the time of this audit, ITS was in the process of completing a comprehensive review and update of the City's IT policy framework, including the RACN Policy. This initiative led to the drafting of a number of new technology security standards including a new *Information Security Standard - Remote Access Services* (ISS-RAS). As described later in this report, the ISS-RAS addresses some important gaps in the existing policy framework and provides greater clarity regarding responsibilities and the authority of the Chief Information Officer (CIO). Clarification of CIO's authority under the draft ISS-RAS is particularly important in light of the customized RA solutions that exist within certain areas such as OC Transpo, Water Services, Traffic Services and the Ottawa Public Library, etc. where Independent Technology Groups (ITGs) exist. This new standard had not yet been implemented as of the reporting phase of this audit.

As referenced above and described further in this report, concerns related to governance, including roles, responsibilities and authorities, have contributed to a number of the observations raised by this audit. The OAG has completed several IT audits over the last few years where observations highlighted governance issues as a contributing factor underpinning many of the audit findings and recommendations described in this report. Prior audits included the Audit of IT Governance (2014), Audit of IT Risk Management (2015) and the Audit of IT Security Incident Handling and Response (2015). Each of these audits identified risk factors that were linked to the

[14] The following service offerings are described in the RACN Policy: Web Mail, BlackBerry^{TM}, Virtual Private Network (VPN) i.e. access from a City owned Laptop, and Remote Desktop – i.e. access from an employee's personal computer.

existence of proprietary technology or systems that are managed by ITGs[15] rather than centrally by ITS. This condition makes it difficult for the City to support consistent enterprise-wide IT strategies and requirements, including those related to security. These audits also highlighted challenges associated with a systemic lack of continuity in the CIO position. While this audit of RA was not designed as a follow up to any prior IT audits, both of these conditions continue to exist in 2017. These ongoing conditions increase the risk associated with RA and have been identified as contributing to many of the audit findings and recommendations described in this report. During the course of this audit, the OAG engaged with ITS on the linkage between prior audit findings and the results of this audit and has encouraged ITS to remain diligent in addressing prior IT audit recommendations. As per the City's audit protocol, the OAG continues to take steps in support of the active monitoring and follow up of ITS's response to prior audit findings.

Audit approach and methodology

The overall objective of this audit was to provide an independent assessment of the adequacy and effectiveness of key systems, practices, procedures and governance in place to identify and mitigate risks, including security risks, associated with providing remote access to the City's network. Priority areas were as follows:

- Use of remote access;
- Roles and responsibilities for granting remote access;
- Remote access architecture and technology; and
- Remote access operations and monitoring.

Audit criteria (refer to Appendix A – Audit objectives and criteria) were established based on leading IT Remote Access guidance, such as that published by the National Institute of Standards and Technology (NIST). Specifically, NIST Special Publication (SP) 800 463[16] , NIST SP 800-534[17], and relevant elements of the NIST Cybersecurity

[15] As described later in this report, the existence of ITGs does not preclude ITS's involvement in proprietary systems and technology only that such involvement was not governed by formal authority.

[16] "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security", 2016 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

[17] "Security and Privacy Controls for Federal Information Systems and Organizations", 2013 (updated 2015) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Framework[18] were leveraged as valuable sources of audit criteria.

Scope

The scope of this audit included remote access[19] offered to authorized users through the following means:

1. Virtual Private Networks including:
    a. Internet Protocol Security ("IPSec")
    b. Encrypted Links (Secure Socket Layer "SSL")
2. Remote control connections, including Citrix and Remote Desktop solutions;
3. Mobile connectivity (Blackberries™, other smartphones, tablets, etc.); and
4. Web-based remote access including Outlook Web Access (OWA).

Our examination included controls within ITS and across all City business lines and departments where RA capabilities exist, including those areas where ITGs exist.

For greater certainty, the scope of this audit did not involve an assessment of remote office VPNs nor access provided to Council members.

Audit approach and methodology

The audit was designed and conducted in accordance with the requirements of the City's Audit Standards to ensure that sufficient and appropriate audit procedures were conducted and evidence gathered to provide reasonable assurance of the accuracy of audit findings and conclusions, as they existed at the time of the audit.

The approach encompassed a city-wide review of IT Remote Access. The audit team assessed IT Remote Access policies, procedures and practices for design adequacy and effective implementation both within ITS and across the City.

Document reviews, interviews and testing were performed during the audit conduct phase (January - May 2016). The audit work included technical testing whereby ITS provided the audit team with a City standard Windows laptop and Blackberry™ phone.

[18] "Framework for Improving Critical Infrastructure Cybersecurity", 2014

https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[19] The audit did not include access or communication gateways that do not interface directly with the Cityn network (e.g. radio or other communications systems).

The auditors tested these devices and employed them to connect to the City's remote access services. Technical testing involved the examination and assessment of:

- Endpoint Security Controls (such as malware prevention and detection);
- Departmental Remote Access Isolation Security (to ensure critical systems are effectively isolated from the corporate network);
- Support and Availability (including routine operational practices and updates); and
- Operational Monitoring and Incident Detection (such as alerts on a potential security event).

Audit observations and recommendations

This section provides details on the key observations resulting from the audit. Where applicable, recommendations are also provided.

Remote access technology strategy

In the OAG's 2014 Audit of IT Governance, it was noted that the City had developed a Technology Roadmap that provided insight to IT priorities, initiatives and objectives. However, that audit also raised concerns regarding the lack of clear alignment between IT investments and the City's strategic and business priorities. This audit found that the City had not yet addressed these concerns nor had it refreshed the Technology Roadmap since the 2013-16 version. It also confirmed that there is no formal strategy that would serve to guide the City's RA-related priorities and decision making and support clear ownership and management of RA-related risks.

ITS indicated that they are in process of drafting a new IT strategy, however there were no existing plans to include or develop an RA Technology Strategy that would serve to guide the city-wide RA priorities and technology in alignment with a clear vision[20]. In addition to increasing the likelihood of gaps or variances in RA practices and technologies across the City, the absence of a formal RA Technology Strategy with city-wide application was identified as a contributing factor regarding identified concerns related to:

[20] Such a vision would serve to articulate and support an efficient and enterprise-wide approach to remote access, including balancing business needs with security requirements and support aligned planning/decision making around emerging areas such as mobile technologies and Bring your Own Device.

- Ownership and management of RA-related risks impacting the security of the overall network;
- Roles, responsibilities and accountabilities; and
- Governance/decision-making.

While the audit identified that roles, responsibilities and accountabilities at the operational level (e.g. RA account administration, approvals, risk assessments, etc.) are generally clear and often supported by formal procedures and checklists, concerns were identified at the higher level. Specifically, it identified that ownership of the City's RA-related risks, roles, responsibilities and accountabilities has not been clearly established across City departments and at the corporate level. This observation is consistent with the OAG's 2015 Audit of IT Risk Management which identified a similar concern regarding the CIO's authorities and responsibilities for city-wide IT risks. For this audit, the OAG found that ITS plays an effective and appropriate role in the monitoring[21,] oversight and mitigation of RA-related risks. This role includes having ITS develop tools and practices that help ensure the City's standards, protocols and other requirements are reflected in: selection and deployment of RA technologies, granting of RA connections to employees or vendors, account administration, et al. However, as identified as a concern in various prior OAG audits, their role does not formally extend to departmental RA deployments managed by ITGs. For these deployments, ITS's involvement may vary from no or limited involvement to significant involvement in all aspects of the initiative including the requisite decision making. This ongoing situation limits ITS's ability to have a holistic view of the City's RA technology in support of economical and effective strategic, and operational, planning and risk management.

Notwithstanding the concerns related to the lack of a city-wide RA Technology Strategy that effectively informs the City's vision for RA, the audit noted the existence of a number of initiatives that will help to address the concerns raised in this report. As noted in the Background and context section, ITS is in the process of completing a comprehensive review and update of the City's IT policy framework. This includes replacement of the existing *Remote Access to City Network Policy* which was identified as being both outdated and largely ineffective. The proposed new ISS-RAS Standard was found to provide good technical coverage for RA requirements related to monitoring, testing and patching, et. al., and it provides clear expectations for end users regarding appropriate use. The draft standard also clearly indicates that it applies to all

[21] Monitoring of compliance is a shared responsibility between each department (e.g. monitoring non-City employee accounts) and ITS (e.g. monitoring citywide dormant accounts).

RA services that support remote connections to the “City’s Enterprise Computing Environment” which includes those environments managed by ITGs and any third parties. It also clarifies that the CIO is required to sign off on any requested exclusions from the mandatory nature of the ISS-RAS. These are important elements that will help to address some of the concerns raised in this audit and in prior audits[22]. Approval and implementation of this new standard (which has been in draft form since 2016) will be a key step in addressing existing RA-related control weaknesses and inconsistencies across the City.

Recommendation #1

> 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.

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.

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.

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.

[22] As noted earlier, this audit was not designed as a follow-up to any prior IT audits conducted by the OAG.

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.

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.

Remote access architecture – Inventory and data flows

Given the increasing reliance on RA to support business operations including critical functions, the audit expected there would be a formally documented Enterprise Remote Access Architecture that would provide a comprehensive view of all RA connections across the City. Such a document would provide information on (1) how RA devices across all City departments and ITS connect; (2) the remote technologies in place, including those relevant to SCADA or proprietary applications with remote connectivity; and (3) the related data flows.

The audit found that the City has not documented its Enterprise Remote Access Architecture, nor has it developed a comprehensive inventory of its RA technologies, connections and data flows at a city-wide level, including departmental implementations. While there is no enterprise-wide architecture, there was evidence of documented architecture pertaining to specific corporate RA services (including the City's VPN Infrastructure, Blackberry^{TM} infrastructure, Remote Desktop connectivity) and an inventory of City owned laptops and Smartphones. We also understand that ITS has recently developed plans and assigned responsibility to build a central repository of RA risks and technologies. At the time of the audit, however, there were a number of potentially significant implications associated with not having a comprehensive enterprise inventory including an inability to develop and leverage effective strategic planning. In the absence of effective strategic planning, there is an increased likelihood that investments in RA technologies, services and procedures will not be coordinated to optimize value for money and security. At the operational level, this gap increases the likelihood of a variety of negative outcomes including: security or regulatory (e.g. privacy) breaches resulting from non-conforming remote connections, delays in identification of such breaches and the use of unauthorized RA platforms. Finally, the effective implementation of the new ISS-RAS also requires a clear definition and demarcation of the City’s Enterprise Computing Environment as described in that standard (see Recommendation #2).

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.

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.

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.

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.

IT remote access security gaps

While providing reliable and highly available RA is a business imperative in the current environment, there are information technology security risks which are inherent in RA. This includes a potential breach of confidentiality, integrity or availability. Mitigation and management of these risks requires that the City’s technical security practices and controls can detect, respond and prevent incidents of unauthorized access to information via RA services (i.e. VPN, Remote Desktop, smartphones). These practices and controls should reflect a consideration of both the City’s business requirements and the need for adequate security measures. In reviewing these security measures, the auditor considered the following contexts:

- Endpoint devices (i.e. the laptop or smartphone, used to access the City's network) – devices need to be configured and secured against unauthorized and other potentially risky activities. A secure endpoint device will be encrypted, require strong passwords, incorporate malware prevention and is centrally managed with a locked-down configuration.
- Network architecture – The City must prevent unauthorized remote connections to the corporate network. The network design and architecture must ensure that departments with critical infrastructure have isolated it from RA through the corporate network.
- Support services – the support provided to RA users should promote a high degree of availability (including after-hours service) while reflecting appropriate security measures (e.g. validation of the user's identity prior to providing service) and compliance with standards.
- Operational monitoring and incident detection – monitoring of RA traffic and activities should identify and escalate, as applicable, security anomalies, alerts and potential security incidents. The controls examined by the auditors include those outsourced by the City to a Managed Security Service Provider (MSSP).

The audit addressed the security measures referenced above through a series of technical tests which included the use of a City issued laptop and Blackberry™ smartphone which were used to connect to the City network via RA. The testing also involved the use of non-City issued devices that were used to identify exposures to unauthorized network access and functionality.

Testing conducted on City issued devices revealed a number of effective security measures while also evidencing a resilient RA systems capable of supporting high levels of availability. The auditors noted that default architecture ensures that critical infrastructure remains isolated from the corporate network. In terms of specific security measures, the City issued laptop was found to be considerably more secure than the smartphone. The laptop provided effective controls to prevent bypass of restrictions (e.g. passwords) or elevate the user's access to beyond what was authorized. Among other effective features, the laptop was configured with updated security software, featured full disk encryption and did not allow the unauthorized export of VPN software to a non-City laptop.

Among the other positive results of the testing in this area, the audit team's testing of City RA systems revealed that the RA network architecture did not exhibit significant vulnerabilities to unauthorized access. Authorized users were also found to be restricted in terms of access and functionality when connecting non-City owned devices via RA. In addition, audit testing concluded that the City has established RA management operating procedures suitable for end user support and effective account administration.

However, the audit testing also yielded concerns related to weaknesses and gaps in the RA security environment. The existence of these weaknesses or gaps could compromise the City's ability to prevent, detect and respond to incidents, including unauthorized access. Specifically, the audit identified the following concerns related to the technical aspects of RA security:

- City issued mobile devices are not sufficiently secured;
- [redacted]
- [redacted]
- Security monitoring has not been optimized to detect and respond to RA security breach scenarios.

These are further described below.

Audit testing conducted using the City issued smartphone revealed that the mobile device was configured with the latest Blackberry™ operating system and various security measures, including Blackberry's "balance" feature to separate work and personal spaces. Further, the City's device management system generated an email alert to the user when anomalous activity[23] was detected. However, the device was not considered to be sufficiently secure in light of the weaknesses and gaps identified. [redacted]

- [redacted]
- [redacted]

[23] In this case, the alert indicated that the device was no longer enabled with services that support policies and security settings intended protect the City's information and network and that their cell service may be suspended if the situation was not rectified.

[redacted]

- [redacted]

[redacted]

As with the City issued smartphone, testing of the City issued laptop confirmed that core security safeguards were implemented, including encryption, restricting administrative access, current antivirus software and current operating system patches.

[redacted]

The audit also examined authentication controls that are intended to assure that users are who they claim to be. Authentication can be validated by a combination of factors; the more factors required, the stronger the control. For example, the requirement for a password would be a one-factor authentication. Two-factor could be a password in combination with digital certificate, while three-factor would also include a biometric (e.g. a fingerprint or retinal scan). [redacted]

Passwords are susceptible to theft and misuse. [redacted]

[redacted]

The City’s efforts [redacted] no longer reflects the industry standard and increases the risk of unauthorized users gaining access to the network.

As part of the technical testing, the audit team also created security incidents using malware, containing a non-functional virus, to determine if the City’s security technologies would detect and block the attempted security breach. While one of the tests was successfully detected, reported and blocked, similar other tests were not detected, reported or blocked.

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.
>
> - [redacted]
> - [redacted]

Management response:

> Management agrees with this recommendation. The CIO will implement the appropriate controls [redacted] for RAS connections. [redacted] This will be completed by Q4 2019.

Monitoring and oversight

Preventing security incidents, while providing reliable and available RA, is an important objective. Notwithstanding, it is a near certainty that security incidents will occur. Whether malicious in intent or otherwise, we expected that the City would have formal and effective capabilities that would support timely detection and response and escalation in the event of actual or potential security events or other circumstances that threaten the availability of RA services. Further, we expected to see an effective regime of oversight whereby: RA solutions are subject to risk assessments and are tested for vulnerabilities; practices, roles and responsibilities for managing RA accounts are effective and appropriate; and where effective and timely incident reporting is leveraged in support of continuous improvement.

Consistent with the observations in the OAG's 2015 Audit of IT Security Incident Handling and Response, this audit revealed that the City has incident monitoring, detection and escalation capabilities which include RA applications. While these capabilities continue to lack maturity, as highlighted in the 2015 audit, there were also signs of improvement over the last two years. For example, in 2016 the City entered into a contract with a new Managed Security Service Provider (MSSP) with the objective of improving service delivery and value add compared to its previous arrangement. We also identified ITS's comprehensive review and update of the City's IT policy framework; particularly, the development of a new ISS-RAS as representing a significant improvement in the oversight and control of RA solutions through the enforcement of mandated risk assessments. Also of note, was the audit's findings that effective and formal practices were in place regarding the granting of RA and that practices in support of the effective RA account administration; for example, the periodic reconciliation of users had been improved.

Notwithstanding the improvements referenced above, the audit revealed some gaps and weaknesses in the City's ability to detect and respond to security threats and vulnerabilities related to RA. Specifically, the audit identified the following concerns related to monitoring and oversight:

- [redacted]
- There has not been focused third party penetration testing of remote points to identify possible issues[26].

These issues are further described below.

In June 2016, the City entered into a contract with a new MSSP provider. During the audit, it was identified that the City and the new MSSP are still in the process of implementing the new service arrangement. [redacted] Industry standards suggest this process would normally take less than three (3) months which is considerably less time than the City's experience.

[26] This observation is mirrored in the 2015 Audit of Security Incident Handling and Response whereby it was recommended that the CIO conduct penetration testing on all critical infrastructure.

Use cases describe specific scenarios and vulnerabilities that the MSSP would be expected to identify through monitoring. They would also provide the basis for the nature and scope of RA activity logs that should be collected and the types of RA activity (or “traffic”) the MSSP is responsible to monitor. The MSSP has implemented standard use cases under their contract with the City. [redacted]

As part of the technical testing, the audit conducted vulnerability scans of the City’s RA servers. While these scans did not identify any significant vulnerabilities, they were not designed to provide the level of assurance that would be provided by a focused vulnerability assessment or penetration test conducted by a third party. Consistent findings from the 2015 Audit of IT Security Incident Handling and Response, it was noted that vulnerability assessments and penetration testing was not routinely conducted[27] on all corporate and departmental RA solutions. Interviews with ITS personnel further indicated that ITS has historically performed risk assessments on RA solutions on a case-by-case basis based on the perceived level of risk. Notwithstanding this identified weakness, the draft ISS-RAS requires that vulnerability assessments on RA technologies are conducted two times a year, and threat/risk assessments be conducted at least once every three years. As referenced in Recommendation 2, staff are encouraged to implement this new standard as soon as possible.

Audit interviews and document review results indicated that reconciliation of RA accounts[28] (those provisioned to non-City employees) had not been completed in a timely manner. However, during the course of the audit, ITS commenced an initiative to reconcile its database of third parties with RA to ensure the access was still required and that relevant information was current and accurate (e.g. contract end dates, contact names within the relevant City business line, etc.). The audit team understands that this

[27] The audit team noted that the new CITRIX VPN solution, scheduled for implementation in 2017, had undergone a vulnerability assessment.

[28] These are accounts held by Non-City Employees (NCE), including contractors and vendors that require RA as part of their responsibilities.

improvement to RA account administration will be sustained with periodic reconciliation to ensure account access is limited to appropriate and authorized users.

Recommendation #7

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

- [redacted]
- Continuing to improve operational practices including vendor and employee account management and reconciliation.

Management response:

Management agrees with this recommendation. [redacted] Operational steps will be implemented to improve vendor account management and ensure reconciliation of accounts is maintained by Q4 2019.

Appendix A – Audit objectives and criteria

Overview of the audit objectives and criteria

Use of remote access (policies, procedures and standards)	
1.1	Formal policies and procedures have been established to: • Require that users agree to maintain expected security controls on connecting devices; • Require that users follow City policies, standards and directives; • Require the conduct of risk assessments as part of selecting appropriate remote access methods; and • Formalize the secure management, administration and operation of remote access solutions.
1.2	Standards for remote access are formally defined, including authentication, encryption, authorization, device types permitted and network access permitted.
Roles and responsibilities for granting remote access	
2.1	Roles, responsibilities and accountabilities of all parties involved in the IT remote access process are clearly defined, communicated and understood.
2.2	Users or organizations provided with remote access capabilities have received formal authorization and approval prior to being granted access privileges.
2.3	Dormant accounts are identified and purged.
Remote access architecture and technology	
3.1	An Enterprise Remote Access Architecture is developed, with a scope including IT Systems, SCADA systems and proprietary technology.
3.2	City departments with specific business needs have implemented remote access in accordance with policies, standards and the ITS architecture.
3.3	Connectivity between remote access systems and the corporate network is documented and assessed by ITS for security implications.

Remote access operations and monitoring	
4.1	Departmental and corporate remote access systems are available and properly function to support operational and business requirements as determined by a business continuity plan or impact assessment.
4.2	Timely and effective support is available for all remote access staff. User support services (e.g. IT help desk) are available to staff and meet the required service standards.
4.3	Maintenance patching and updates are applied in a timely fashion in accordance with best practices and compliance with City standards for patch and vulnerability management.
4.4	A risk assessment has been performed on corporate and departmental remote access solutions.
4.5	Anomalies and security incidents are detected within the remote access infrastructure using appropriate and effective technologies.
4.6	Incident handling and escalation practices for remote access are formally defined and followed for all implementations of remote access.
4.7	ITS conducts performance and availability monitoring for remote access services and notifies stakeholders when service level or performance requirements are not met.