January 2019

Report of the Auditor General to the Nova Scotia House of Assembly

Information Access and Privacy Information Technology Projects

Next

Back

Prior View

Independence • Integrity • Impact

Next

Back

Prior View

January 15, 2019

Honourable Kevin Murphy
Speaker
House of Assembly
Province of Nova Scotia

Dear Sir:

I have the honour to submit herewith my Report to the House of Assembly under Section 18(2) of the Auditor General Act, to be laid before the House in accordance with Section 18(4) of the Auditor General Act.

Respectfully,

MICHAEL A. PICKUP, FCPA, FCA
Auditor General of Nova Scotia

5161 George Street
Royal Centre, Suite 400
Halifax, NS B3J 1M7
Telephone: (902) 424-5907
Fax: (902) 424-4350
Website: http://www.oag-ns.ca
: @OAG_NS

Next
Back
Prior View

Next

Back

Prior View

Table of Contents

Next

Back

Prior View

Department of Internal Services: Information Access and Privacy Information Technology Projects

Overall Conclusion

- **Weak risk management and poor overall project management contributed to an environment where vulnerabilities were left in place. One vulnerability was exploited undetected and resulted in the unauthorized disclosure of personal information.**

Lack of Effective Information Technology Risk Management

The Department of Internal Services' IT risk management process was inadequate

- Limited risk assessment was completed; many relatively obvious risks were not identified
- Some identified risks did not have mitigation strategies
- Critical risks related to using cloud-based services were not fully considered. For example, data stored in the cloud is not protected by the Province's corporate network.
- Key project management documents for managing risks were either incomplete or not completed at all
- Neither threat risk assessments nor security assessments were performed or required prior to implementation

The Department assessed the implementation of the new projects as low risk despite the following:

- Nova Scotia was the first organization to implement Accesspro on AMANDA 7
- Nova Scotia was the first organization worldwide to implement the FOIA website
- The Department and the Information Access and Privacy Division were in a state of organizational change

An expert group within the Department was not adequately consulted on potential risks or mitigation strategies

- The Department's expert group approved a six-month pilot for Accesspro, but did not follow up
- The Accesspro and FOIA website projects were completed and implemented without further consultation from the experts
- Current responsibilities of the group do not include changes to existing systems; a gap in oversight still exists

Inadequate Project Management

Both projects were impacted by inadequate project management

- The Department did not address the risk that the project sponsor had limited IT experience or expertise
- There was no government project manager for the Accesspro project
- There was a project manager for the FOIA website project, but numerous key steps were incomplete
- An inappropriate level of reliance was placed on the vendor to ensure the security of the product
- Key contract components, including financial obligations related to the FOIA website project, were not documented

Next
Back
Prior View

Recommendations at a Glance

Recommendation 1
The Department of Internal Services should conduct comprehensive risk assessments for IT projects prior to implementation.

Recommendation 2
The Department of Internal Services should clearly define the scope of responsibilities of the Architecture Review Board and ensure stakeholders clearly understand what IT projects should be submitted. The scope should include new IT systems or changes to existing systems and should require a full scope of documentation and testing.

Recommendation 3
The Department of Internal Services should establish criteria to ensure adequate project management expertise is in place for all projects. The criteria should be documented, communicated, and put into practice in managing teams.

Recommendation 4
The Department of Internal Services should establish a process to ensure and document vendor compliance with contract terms at all stages of a contract.

Recommendation 5
The Department of Internal Services should ensure contracts with vendors include service expectations and financial obligations.

Next
Back
Prior View

Key Terms

AccessPro Project: the implementation of the new Freedom of Information Access (FOIA) Requests software to provide case management, redaction, and reporting functions for managing FOIPOP Information Access Requests.

FOIA Website Project: the implementation of a website used with Accesspro for the public to submit, track, pay for, and respond to Information Access Requests. It also provides government with the ability to share open data through a disclosure log.

AMANDA: the software suite adopted as the Province of Nova Scotia's enterprise standard for all permitting, licensing, land development/planning, compliance, inspection, and code enforcement applications.

AMANDA 6: the version of the software suite that is hosted in the Province's own data centre but supported by its vendor.

AMANDA 7: the newer version of the software suite that is used to run Accesspro. It is hosted by its vendor, outside of the Province's IT infrastructure.

Department of Internal Services: Information Access and Privacy Information Technology Projects

Breach caused by the Department's failure to properly identify and manage IT risks

1 On January 6, 2017, the Province of Nova Scotia unveiled a new public website, supported by new case management software Accesspro, to facilitate its access to information requests. Fifteen months later, in April 2018, a weakness in the design of the Freedom of Information Access (FOIA) website was exploited and resulted in the inappropriate download of over 7,000 documents. The inappropriate download included child custody documents, medical information, and proprietary business information.

2 We found the processes used to develop and implement the new software and public FOIA website were poorly managed and did not adequately consider risks. Risks had not been appropriately assessed at the start of the projects and even some risks that had been identified did not have plans in place to manage the risk. The result was that neither project, Accesspro or the FOIA website, had been designed or implemented with adequate consideration around protecting the sensitive information it held.

3 We identified a number of issues with each project and discuss each issue in more detail throughout this report.

- Extensive reliance on a vendor
- Lack of provincial IT experience in sponsoring and overseeing the projects
- Accesspro used on AMANDA 7 for the first time
- First organization in the world to use the new FOIA website
- Limited security testing

Risks associated with the use of the cloud and new FOIA website considered low

4 The poor approach to risk assessments can partially be linked to the fact the Department of Internal Services assessed the overall risk of procuring and implementing Accesspro and the FOIA website as low. The Department referenced its lengthy relationship with the vendor in providing similar solutions and services and the extensive adoption of Accesspro by industry as large factors in the assessment of risk. These two considerations do not accurately represent the environment in place at the time and we have

concerns with both. We also identified various other factors to suggest the risk of this project should have been assessed higher.

5 Accesspro and the FOIA website would be hosted in the cloud and serviced by a vendor. The Province of Nova Scotia would be the first organization to implement Accesspro on AMANDA 7 and also the first in the world to implement the FOIA website. Implementing something that has never been used before, as well as using it in the cloud, comes with a high degree of inherent risk.

6 Use of a cloud-based service means the data stored in it is not protected by the Province's corporate network. The Province has control of its own network security to protect its data and systems from unauthorized access through the internet. However, when data is stored outside the network and in the cloud, it is accessible publicly through the internet. Therefore, the additional risk of being potentially targeted by anyone on the internet should have been identified and mitigated.

7 We also noted that while the Department developed a cloud computing strategy in 2013 and it included questions to help understand and address the risks in procuring cloud-based services, the resources included in the strategy were not used on these projects. Using those resources would have been useful in identifying risk areas and understanding security expectations and responsibilities.

8 While the Department prepared privacy impact assessments as required for the projects, it assessed risks as either low or medium. This included the probability that the vendor's systems could be hacked and is another example of the Department of Internal Services understating the risks associated with the projects.

9 A threat risk assessment to assess the risk to all information in an IT system was not completed because project team members had been informed by the Department that one was not required. The Department of Internal Services was planning to upgrade from the AMANDA 6 platform to AMANDA 7 and was waiting to conduct the assessment as part of that upgrade project.

10 Waiting to complete a threat risk assessment at some future date, yet implementing a project without mitigating the risks of not having completed a threat risk assessment, leaves systems vulnerable. Risks around data integrity and unauthorized disclosure of personal information would be unknown.

Recommendation 1

The Department of Internal Services should conduct comprehensive risk assessments for IT projects prior to implementation.

Department of Internal Services Response: The Department of Internal Services accepts this recommendation. The level of project risk and complexity will vary by project; therefore, risk assessments and risk management will also vary based on the type of project. Project Risk management practices including Threat Risk Assessment (TRA) and Privacy Impact Assessment (PIA) processes have been and will continue to be enhanced and implemented. To support new initiatives and ongoing operations we have recently developed and communicated to staff an overview/guide describing the proper timing and execution of TRAs and PIAs. In addition, measures will be taken to increase awareness and invest in training and awareness of project team members, managers and client departments in general, to ensure adoption of risk management practices, including risk registers and risk mitigation strategies in alignment with industry best practices such as Project Management Book of Knowledge (PMBOK) and frameworks such as Control Objectives for Information Technology (COBIT) and National Institute of Standards and Technology (NIST) for Cybersecurity.

Expert group not adequately consulted

11 The Architecture Review Board (ARB) is comprised of Department of Internal Services staff who have experience in such areas as privacy, infrastructure, and cybersecurity. We identified gaps in the responsibilities of this expert group that meant only components of the projects that impacted the government network were sent to the ARB for assessment; components that did not impact the government network were not assessed.

12 One piece of the Accesspro project was submitted to the ARB for assessment. Following its assessment, the ARB gave this piece of the project a six-month pilot status requiring it to be resubmitted to the group for final approval. However, the entire project went ahead without final approval and the agreement with the vendor was signed without this project piece ever being resubmitted to the ARB. It is clear the Department should have followed the directions it was given, but this also identified the need for the ARB to have a process to ensure it follows up on projects like this.

13 We also noted that the ARB required only a limited amount of technical and risk information be submitted, basically only privacy impact assessments and architecture diagrams. We expected all information needed to assess the risk posed by new or changed technology would be required. In addition to what was submitted, this could include threat risk assessments or additional security assessments such as penetration tests.

14 Security assessments which include penetration testing might have identified security vulnerabilities that could have been addressed before the systems went live, but security assessments were not required or completed on either the Accesspro or the FOIA website project. Security vulnerabilities are weaknesses that could be exploited in a system and are critical to identify and

Next
Back
Prior View

manage. For these projects, the Department relied on their more than 20-year relationship with the vendor and the incorrect assumption that the software was secure; this was not an appropriate approach for government to take.

15 Following the breach in April 2018, the Department completed penetration testing which identified multiple critical security vulnerabilities still present, even after the exploited vulnerability had been addressed. Proper due diligence prior to using the new systems could have identified these issues and they could have been fixed before any personal information was exposed to the internet.

16 Currently, all new applications and systems must be submitted to the ARB for assessment. However, even though changes to business applications such as the addition of the FOIA website could have a significant impact on security over information, they would not be submitted to the ARB for review as they are categorized as a change, not a new application or system. This significant gap in the administration of the Province's IT systems results in considerable risk and should be addressed.

Recommendation 2

The Department of Internal Services should clearly define the scope of responsibilities of the Architecture Review Board and ensure stakeholders clearly understand what IT projects should be submitted. The scope should include new IT systems or changes to existing systems and should require a full scope of documentation and testing.

Department of Internal Services Response: The Department of Internal Services accepts this recommendation. A review of the current scope, mandate, and supportive processes is being performed, and where appropriate, improvements and enhancements will be implemented, communicated and enforced. Project assessment considerations will include scalability, timing, intake processes and documents, required output, and supportive governance structures, with a focus to ensure new IT systems and changes to existing systems are examined at the proper governance levels and at the right time.

Inadequate project management practices

17 We found the Department of Internal Services did not appropriately manage key parts of either the Accesspro or the FOIA website project. From the beginning, the Department did not mitigate the risks associated with the overall project sponsor, who, although experienced with freedom of information and privacy issues, had limited IT experience or knowledge. We do not expect all project sponsors to be familiar with IT projects, but it is important for the Department to identify this risk and take steps to ensure appropriate expertise is in place to provide support.

18 With a project sponsor inexperienced in IT, the Department should have taken steps to ensure there was IT project management expertise on the team that was focused on managing risks, including IT risks, to the Province. This expertise could have come from a Provincial employee or a contracted consultant. However, the Accesspro project had neither; project management services were provided by the vendor. This complete reliance on a private sector vendor was not sufficient and will be discussed in more detail later in this chapter.

19 Poor project management led to many issues throughout the Accesspro project. We found several key documents, including the initial Accesspro project charter, were left unsigned, or were incomplete. We also noted many instances of missing supporting documentation, including meeting minutes, key milestone approvals, evidence of user acceptance testing, a project plan, and a close-out report.

20 The project charter for the Accesspro project was never signed and it lacked key components, particularly around risk assessment. A strong project charter is intended to lay out the basics of a project and serve as a guide for what the project should entail, what it is intended to accomplish, what the possible challenges or risks to success are, and how management will deal with those risks. Failing to complete a strong project charter meant the Accesspro project began without a clear plan and it significantly increased the chances the project would fail.

21 The Accesspro charter included some project risks, such as the Information Access and Privacy Division's lack of established policies and procedures, impact of summer holidays, and availability of staff throughout the project. However, the charter did not include mitigation strategies for those risks.

22 Several other types of risks, including reputational risks (public confidence in government), financial risks (costs of project overruns), and regulatory risks (breach of privacy related legislation), had not been considered. In addition, the impact of the significant organization changes happening in the Department were not included. See background information in Appendix II.

23 The second project, the FOIA website project, had a dedicated project manager from the Province's Project Management Office and used a project framework. There was a signed project charter that expanded further on risks and included the impacts of the risks and mitigation strategies. However, we found a number of important steps had not been followed. For instance, the User Acceptance Testing approvals were not obtained, there was no contract for ongoing support of the FOIA website, documents sent from the project manager for approvals were left unsigned, and approvals to move the website into production were not documented.

Next
Back
Prior View

24 It is reasonable to expect projects to have a thorough review of all risks and appropriate steps to address the risks identified. Key actions such as completing threat risk assessments, security assessments, and appropriate reviews and approvals by the Province's Architecture Review Board should be taken. Taking such steps might help prevent the implementation of a system that has security vulnerabilities which exposes personal information to unauthorized access, changes, or destruction.

Recommendation 3

The Department of Internal Services should establish criteria to ensure adequate project management expertise is in place for all projects. The criteria should be documented, communicated, and put into practice in managing teams.

Department of Internal Services Response: The Department of Internal Services accepts this recommendation. A Resource Fulfillment Process for assigning project team members, including project managers, will be developed and implemented, and will include identification of key engagement criteria; it will be used for matching project team members with the appropriate skills and experience to IT projects as well as to support project managers in gaining experience and skills to progress through their careers.

Extensive reliance on outside parties

25 The Office's November 2016 chapter on AMANDA Case Management and Compliance System focused on the AMANDA 6 environment. At that time, we reported our concerns regarding the Province's belief that less oversight was needed due to the long-standing relationship with the vendor. We noted we found no evidence the Province was ensuring vendor staff had read and accepted the Province's IT standards as required by the contract. The problems around the Accesspro and FOIA website projects in the AMANDA 7 environment are consistent with our finding in 2016 – *"Without proper oversight, the Department cannot ensure contract terms are fulfilled to the level required."*

26 The change request for Accesspro required the vendor to protect the Province's information. It included a listing of Provincial policies and standards the vendor was required to follow, but we noted the list included some outdated policies, non-applicable policies, and excluded others. The Wide Area Network Security Policy was last updated in 2013 and did not reflect the IT environment at the time of signing the contract and the Department of Finance and Treasury Board's SAP Security Policy was noted, but has not been relevant since those services were outsourced.

27 The Open Web Application Security Project (known as OWASP) is used as the Province's standard for secure coding and provides guidance on the top 10 most critical web application security risks. It includes specific reference to

Next
Back
Prior View

the exact weakness that allowed personal information to be inappropriately downloaded from the FOIA website. It is reasonable to conclude that basic security assessments would have identified the vulnerability.

28 Department management indicated the OWASP standard only applies to custom designed software; the FOIA website is an off-the-shelf product. Our Office has concerns with this assessment as it does not consider the risks associated with being the first in the world to buy this particular off-the-shelf product. Given the untested nature of the FOIA website, the Department of Internal Services should have ensured the risks identified in OWASP had been considered. Failure to ensure a new system is designed to mitigate against cyber exploitation is simply unacceptable in today's cybersecurity environment.

29 Regardless of how familiar government is with an individual vendor, we believe it is unreasonable to ever put full responsibility for project management, risk assessment, and overall due diligence on a private sector partner. The private sector is largely driven by their own goals and government must maintain responsibility for the public interest in any dealings with them.

Recommendation 4

The Department of Internal Services should establish a process to ensure and document vendor compliance with contract terms at all stages of a contract.

Department of Internal Services Response: The Department of Internal services accepts this recommendation. With the creation of Shared Services more robust processes are being put in place to manage and administer IT vendor compliance starting with major contracts and vendor relationships. Contracting terms and processes associated with compliance are stronger in newer contracts. An analysis of Vendor Relations and Contract Governance capacity has been completed. Work will continue to ensure processes are put in place to monitor compliance with contract terms.

Contractual obligations inadequately documented

30 Accesspro and the FOIA website were procured appropriately through an alternative procurement process. Provincial procurement policies allowed the Department's preference to find a solution to its business needs in existing software used by the Province or from existing vendors. As a result, the Department was not required to go through a competitive process to look for potential solutions. However, we found the contractual agreement and detailed obligations of the Province and the vendor were inadequately documented. The only contractual documentation supporting either of these projects was a change order adding services and costs to the existing agreement for the addition of Accesspro. When the FOIA website was implemented, there was no amendment, change order, or new contract created.

31 We believe it is important for the Province to have contracts with vendors for the procurement and continued delivery of all services, regardless of the Province's previous relationships with the vendor. The estimated annual costs of $63,000 for the software, hosting, and support of the website is over and above the $10,500 monthly cost of Accesspro noted in the change order. The website annual costs are not supported by a contract, change order, or other amendment and Department staff indicated they never actually paid anything to the vendor for hosting and support because they could not agree with the vendor on the details.

32 Without contractual agreements in place between parties, responsibilities and roles are not clearly defined and agreed upon. Systems could be left vulnerable if responsibilities for security are not defined; there could be delays when responding to incidents reducing the availability of critical systems; and unforeseen costs could be made the responsibility of the Province.

Recommendation 5

The Department of Internal Services should ensure contracts with vendors include service expectations and financial obligations.

Department of Internal Services Response: The Department of Internal Services accepts this recommendation. New contract templates have already been established that include many standard terms and conditions including explicit service level expectations and failure consequences and new security and privacy terms and conditions. Contract Terms and Conditions will continue to evolve as the IT industry evolves and will be developed to ensure the proper requirements are made for the various types of IT systems.

Next
Back
Prior View

Additional Comments from Department of Internal Services

Both access to information and privacy protection are important to the Province. Since 2015, staff from across government have been integrated with additional resources hired via open competition, resulting in the current team of more than 20 Information, Access and Privacy professionals.

We have:

- *Brought together and provided training for all staff in the unit;*
- *Created management positions in both Access and Privacy;*
- *Adopted case management technology that has improved efficiency, tracking, and reporting capabilities;*
- *Developed a Privacy Policy and Breach Response protocol;*
- *Developed and delivered privacy training to more than 4500 government staff.*

The intent of the Requestor and Disclosure Portal was to make non-sensitive information that had previously been disclosed more widely available through public access, which would also improve and simplify the associated administrative processes.

What was learned in April 2018 is that despite the best of intentions, this site was the source of the unauthorized disclosure of information belonging to hundreds of Nova Scotians. This was not due to a single decision or oversight failure by the government, but rather a series of decisions, governance issues, and design shortfalls within a complex IT environment.

Government takes seriously its role in the protection of Nova Scotian's privacy, and greatly regrets the impact these disclosures have had on citizens. We are committed to improving in the performance of our duties and have accepted the recommendations of the Auditor General.

Next
Back
Prior View

Appendix I

Reasonable Assurance Engagement Description and Conclusions

In fall 2018, we completed an independent assurance report at the Department of Internal Services. The purpose of this performance audit was to assess the implementation of the Province's system supporting Freedom of Information requests.

The information contained in the responses to FOIPOP requests can contain personal information and needs to be managed in accordance with the Freedom of Information and Protection of Privacy Act. Therefore, proper governance over the information technology containing the responses to these requests is critical to the Province in order to adhere to the FOIPOP Act and protect Nova Scotian's personal information.

It is our role to independently express a conclusion about whether the Department of Internal Services comply in all significant respects with the applicable criteria. Management at the Department of Internal Services acknowledged their responsibility for IT governance over Accesspro and the FOIA website.

This audit was performed to a reasonable level of assurance in accordance with the Canadian Standard for Assurance Engagements (CSAE) 3001—Direct Engagements set out by the Chartered Professional Accountants of Canada; and Sections 18 and 21 of the Auditor General Act.

We apply the Canadian Standard on Quality Control 1 and, accordingly, maintain a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

In conducting the audit work, we complied with the independence and other ethical requirements of the Code of Professional Conduct of Chartered Professional Accountants of Nova Scotia, as well as those outlined in Nova Scotia's Code of Conduct for public servants.

The objectives and criteria used in the audit are below:

Objective:

1. To determine whether the Department of Internal Services followed an adequate process when it selected AMANDA 7.

Criteria:

1. Sourcing of the new system for the Information Access and Privacy Division should have been in accordance with Provincial procurement policies.
2. The project requirements should have been clearly defined in the project planning and procurement documents.
3. Appropriate steps should have been taken to maximize the exposure and competitiveness of the procurement process.

Next
Back
Prior View

Objective:

2. To determine whether the Department of Internal Services followed its project management processes to implement AMANDA 7.

Criteria:

1. AMANDA 7 should have been implemented using ICTS's project management framework.
2. Management should have provided adequate governance over the AMANDA 7 project to ensure that the project was adequately defined and approved.
3. The AMANDA 7 project team should have had the required expertise and authority levels with clearly defined roles and responsibilities.

Objective:

3. To assess whether the Department of Internal Services ensured the system had sufficient controls in place to protect the confidentiality and integrity of the sensitive information held by the Province.

Criteria:

1. Internal control requirements for all parts of the AMANDA 7 system should have been established as part of the high-level system design, risk assessment, and requirements definition.
2. AMANDA 7 should have been tested using the guidance provided in the Province's own Cloud Adoption Strategy and the Government of Canada's Security Control Profile for Cloud-based GC Services and issues identified should have been rectified before it went live.
3. The Department should have ensured security monitoring including periodic testing and implementing corrective actions for identified security weaknesses or incidents was completed.
4. All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment should have been approved, tested, and implemented in accordance with Provincial policies and procedures for a cloud environment.

Next
Back
Prior View

Many of the criteria for the audit are derived from the IT Governance Institute's framework, COBIT 4.1, which is generally accepted as an international authoritative source of best practices for the governance, control, management, and audit of IT operations. Additional criteria were developed by our Office based on work completed on similar types of audits previously completed by our Office. The criteria were accepted as appropriate by senior management at the Department of Internal Services.

Our audit approach consisted of interviewing management and other key personnel and reviewing documentation to determine whether management and those charged with oversight responsibilities effectively procured a cloud-based software solution, managed the projects to implement the software, and took appropriate steps to procure the software. Our audit covered the period April 1, 2014 to March 31, 2018. We examined documentation outside of that period as necessary.

We obtained sufficient and appropriate audit evidence on which to base our conclusion on January 7, 2019, in Halifax, Nova Scotia.

Based on the reasonable assurance procedures performed and evidence obtained, we have formed the following conclusions:

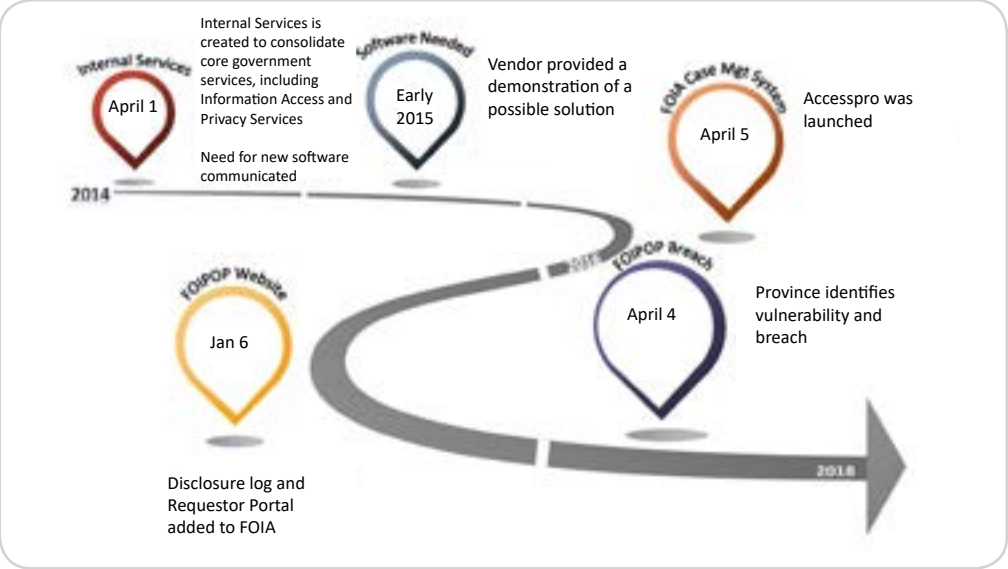
- Accesspro and the FOIA website were procured appropriately through an alternative procurement process.
- Information technology risk management practices at the Department of Internal Services were not adequate to securely implement Accesspro and the FOIA website as a cloud-based system.
- Project management was inadequate.
- Risks that were identified were not mitigated against, the assessment of overall risk was unsupported, and the list of risks was not comprehensive.
- Lack of risk management and effective processes allowed an unknown vulnerability to be exploited undetected causing the unauthorized disclosure of personal information.

Next
Back
Prior View

Appendix II

Background Information

Software Needed to Meet the Needs of a New IAP Division



The Department of Internal Services was created on April 1, 2014, to centralize some of government's core services. Among those services were all network and infrastructure support, the help desk, corporate solutions and communications, and procurement.

Soon after, the Department created an Information Access and Privacy Division (IAP) to centralize the delivery of those services under a Chief Information Access and Privacy Officer. To better support this new centralized model, the new Privacy Officer indicated the need for new case management software and communicated the need to the Department.

The Department was informed by the vendor already providing the Province's business licensing, permitting, and registration case management software, that it could also provide case management software for IAP. The software being proposed, Accesspro, was used by over 100 organizations throughout North America at that time. The vendor provided a demonstration of the software.

The existing contract with the vendor was amended to support the additional services and software licensing fees. IAP moved forward with implementing Accesspro on April 5, 2016. Following the implementation of Accesspro, IAP immediately started a second project with the vendor to implement a FOIA website.

The FOIA website project consisted of two parts – a disclosure log and a requestor portal. Anyone visiting the site could use the disclosure log to search for public information held by government. The portal allowed individuals to submit, purchase, and receive freedom of information requests and correspondence. Those requests could contain personal information that should only be accessible to the owner of the information and would not be available through the disclosure log. It went live on January 6, 2017.

April 4, 2018 the Department became aware of a vulnerability and took the system offline April 5, 2018.

Next
Back
Prior View

• • • Office of the Auditor General • • •
5161 George Street, Royal Centre, Suite 400
Halifax, Nova Scotia
B3J 1M7
http://www.oag-ns.ca
@OAG_NS
Facebook:
https://www.facebook.com/Office-of-the-Auditor-General-of-Nova-Scotia-434965506899059/