Chapter 1
Section
1.05

Metrolinx

Follow-Up on 2020 Value-for-Money Audit:

Information Technology (IT) Systems and Cybersecurity at Metrolinx

RECOMMENDATION STATUS OVERVIEW

		Status of Actions Recommended				
	# of Actions Recommended	Fully Implemented	In the Process of Being Implemented	Little or No Progress	Will Not Be Implemented	No Longer Applicable
Recommendation 1	1	1				
Recommendation 2	2	1	1			
Recommendation 3	4	3	1			
Recommendation 4	2	1	1			
Recommendation 5	1	1				
Recommendation 6	3	2	1			
Recommendation 7	4	4				
Recommendation 8	1	1				
Recommendation 9	1		1			
Recommendation 10	4	1	1	2		
Recommendation 11	2		2			
Recommendation 12	2	1	1			
Recommendation 13	2	1	1			
Recommendation 14	3	3				
Total	**32**	**20**	**10**	**2**	**0**	**0**
%	**100**	**63**	**31**	**6**	**0**	**0**

Overall Conclusion

Metrolinx, as of August 31, 2022, has fully implemented 63% of actions we recommended in our *2020 Annual Report*. Metrolinx has made progress in implementing an additional 31% of our recommendations.

Metrolinx has fully implemented recommendations such as performing root cause analyses (RCAs) for IT incidents related to train delays by establishing a monthly dashboard to identify and resolve recurring IT incidents. Metrolinx has also implemented the recommendation to establish a device lifecycle plan to replace old and ineffective PRESTO devices and has also improved the change management process for IT systems to ensure changes are authorized, tested and implemented without errors. To effectively monitor vendor performance, Metrolinx has implemented the recommendation to receive detailed reports on

vendor incidents through monthly incident reports and meetings with vendors. To address cybersecurity weaknesses, Metrolinx has implemented our recommendation by establishing an annual plan to regularly perform security testing such as penetration tests and vulnerability scans through a newly acquired security scanning IT system. In addition, Metrolinx has implemented the recommendations related to overreliance on IT contractors, whereby, through a documented framework, it now assesses internal capability and performs cost/benefit analyses prior to hiring contractors instead of full-time staff. In addition, Metrolinx has also addressed the recommendation to implement audit logging capabilities. Metrolinx has also fully implemented the recommendation to develop an IT strategy to procure IT systems and services centrally. Additionally, to address the recommendation to review existing websites, Metrolinx has assessed the purpose of all websites and created a development plan to combine and decommission existing websites.

As noted, Metrolinx has made progress in implementing an additional 31% of the recommendations. These include the recommendation to enact a consistent service guarantee program across all Metrolinx services, which is in the process of being implemented for UP Express. In order to effectively monitor IT vendor performance, Metrolinx has made progress with respect to holding its vendors accountable by adding a contractual clause for missed service targets for new vendors that were onboarded after December 2021. Metrolinx is still in the process of making amendments to older contracts. It has also implemented an IT system to enforce password policies for single sign-on (SSO) IT systems, but has not yet implemented an IT system for the Oracle Database. It has also made progress in the recommendation to implement a Disaster Recovery (DR) strategy; at the time of the follow-up, Metrolinx was in the process of operationalizing the required infrastructure to perform DR test exercises. Additionally, Metrolinx has made progress on the recommendation surrounding the excess of existing websites and is in the process of combining and decommissioning the 20 current websites into three simplified ones by April 2023. IT has also made progress on the recommendation to set an IT strategy and centralized procurement function with a dedicated team and director. As part of its procurement process, Metrolinx performs analysis such as identifying a list of business requirements and evaluating existing systems to ensure an existing one does not satisfy the business need before procuring new technologies. Metrolinx has made progress regarding our cybersecurity recommendation to perform code scanning reviews by implementing an IT system. We noted that Metrolinx has onboarded four IT systems and is planning to onboard an additional 26 IT systems to perform code reviews.

However, Metrolinx has made little or no progress on 6% of the recommendations. There has been little progress on the recommendation to perform an assessment to classify existing data according to its data classification policy in order to encrypt applicable data. Metrolinx also has made little progress on the recommendation to restrict access to sensitive corporate information.

The status of actions taken on each of our recommendations is described in this report.

Background

Information Technology (IT) systems play a vital role in managing day-to-day public transit operations at Metrolinx. In the 2021/22 fiscal year, Metrolinx provided a total of over 70 million passenger trips on eight train lines through 68 GO train stations, on the Union-Pearson (UP) Express and its four stations, and on 44 GO bus routes. IT systems are used to operate critical transit functions such as rail signals, switches and fare payment devices as well as the customer information systems that provide schedule information, service alerts and disruption updates. Metrolinx has various IT systems and websites that are used by its employees for transit operations, and by its customers to plan their trips with information about fares and schedules, and for general inquiry.

Metrolinx also oversees the operation of PRESTO, a fare payment system that has been managed and

operated by Accenture under contract since 2006. PRESTO and other fare payment operations are also heavily dependent on IT systems.

During the course of our audit in 2020, we noted that Metrolinx had begun to act on some of our findings. It was in the process of improving contractor oversight processes, including contractors' performance reviews. Metrolinx had also begun to improve IT project management processes, such as documenting project approvals, monitoring timelines and tracking costs. In addition, Metrolinx was in the process of identifying key IT systems to assess impacts to business operations in an event of an outage from a disaster.

Our significant findings included the following:

- Frequent IT incidents caused train delays and cancellations, resulting in lost revenue. Critical transit operations experienced frequent IT-related incidents, such as network connectivity issues, system malfunctions, and software and hardware issues that resulted in train delays and cancellations. From January 2015 to January 2020, there were nearly 4,500 GO train and UP Express delays and cancellations due to IT software and hardware issues. In that time period, train delays and cancellations attributable to IT incidents caused customers to be inconvenienced and resulted in approximately $450,000 in lost revenue due to refunds through the Service Guarantee Program.
- Metrolinx did not consistently test its IT systems for cybersecurity risk. With the exception of the PRESTO IT system, Metrolinx did not perform regular security scans, such as penetration tests, on selected critical IT systems and websites to identify security weaknesses. We noted that Metrolinx had been subject to cyberattacks resulting in breaches of its customers' personal information.
- Contractors were recruited without the required analysis of other options, and many held key decision-making roles. Metrolinx neither assessed whether it already had the resources nor considered whether it should hire full-time employees prior to contracting resources at much higher rates. Metrolinx relied heavily on external contractors for IT operations and services, and had paid approximately $157 million to contract staff in the last five years, almost 2.5 times the salaries and benefits paid for Metrolinx full-time staff. About one-third of these contractors have had their contracts repeatedly renewed for over two years, and some over five years in total.
- Contractors held key management and decision-making roles, such as overseeing project budgets, and hiring and supervising other contractors. From January 2015 to July 2020, about 40% (307 of 764) of IT contractors hired to support the day-to-day IT operations and services were overseen by other contractors.
- PRESTO fare payment devices have encountered software and hardware issues resulting in a number of problems that affect customers. These problems include transit tickets not dispensing and ticket paper jams, faulty displays and Internet connectivity outages that render the devices inoperable. From February 2016 to March 2020, the most current data available, PRESTO fare payment devices used for UP Express and GO trains and buses encountered over 45,000 such incidents. The two devices that have the highest number of IT incidents and significant impacts on customers are ticket vending machines and station fare transaction processors, the green tap machines found at stations.
- Lack of an enterprise IT strategy and governance result in the procurement of redundant IT systems and project cost overruns. Metrolinx does not take a centralized approach to procuring IT systems and websites. We found that different departments procured their own IT systems and websites, resulting in a number of redundant IT systems duplicating functions that already existed in other Metrolinx departments. In addition, systemic issues in IT project management resulted in cost overruns of approximately $152 million, for a total cost of

$288 million, more than double the initial estimate of $136 million from 2014/15 to 2018/19.

We made 14 recommendations, consisting of 32 action items, to address our audit findings. We received commitment from Metrolinx that it would take action to address our recommendations.

Status of Actions Taken on Recommendations

We conducted our assurance work between March 2022 and August 2022. We obtained written representation from Metrolinx that effective November 18, 2022, it has provided us with a complete update of the status of the recommendations we made in the original audit two years ago.

IT Issues Affecting Rail Operations Result in Revenue Loss

Recommendation 1

In order to use root cause analysis to improve customer experience and to reduce train delays and cancellations, we recommend that Metrolinx document and investigate the IT incidents that result in train delays and cancellations, determine their root causes and take corrective actions where necessary to avoid similar incidents from recurring.

Status: Fully implemented.

Details

In our 2020 audit, we found that IT systems and related technology components for critical transit operations had experienced frequent incidents, such as network connectivity issues, system malfunctions and software and hardware issues resulting in train delays and cancellations. While Metrolinx documents basic information about IT incidents that cause delays and cancellations, we found that key information, such as the root causes of the incidents and the steps taken to resolve them, were not recorded. These details were necessary for analysis and assessment to ensure that similar issues do not regularly occur.

In our follow-up, we noted that Metrolinx has enhanced its existing problem management process by performing root cause analyses for recurring IT incidents and develops monthly performance dashboards that identify frequently occurring incidents resulting from train delays or cancellations. This analysis includes customer and financial impact, and action items identified to implement permanent fixes to ensure similar IT incidents that impact GO Train service are identified and resolved.

We noted that from December 2020 to October 2022, 44 root cause analyses have been performed for IT incidents related to rail crossings, train signals, hardware issues, and track-side bungalows. In addition, we reviewed a sample of three incidents related to faulty rail crossing sensors, hardware malfunction and loss of power. We found that all three IT incidents were documented and action plans were created to implement permanent fixes.

Recommendation 2

In order to promote public transit ridership, and improve customer experience and satisfaction through fairness and transparency, we recommend that Metrolinx:

- *analyze the feasibility of implementing an automatic process to refund PRESTO customers for eligible service delays under the Service Guarantee Program, reducing the need for customers to manually apply for a refund;*

  Status: Fully implemented.

Details

In our 2020 audit, we noted that Metrolinx had a Service Guarantee Program to refund customers their fares when GO trains are delayed by 15 minutes or more. The program required customers to verify their eligibility and apply for refunds at GO Transit's website by entering the date of the trip, departure station, arrival station, scheduled train departure time and their PRESTO card number. Although Metrolinx had the technology and necessary data through PRESTO cards to automatically refund customers who qualify

for the Service Guarantee Program, Metrolinx customers are required to apply for a refund.

In our follow-up, we reviewed a detailed analysis performed by Metrolinx to determine the feasibility of implementing an automatic process to refund PRESTO and we noted that to automate the process, PRESTO tap machines would need to be installed on all trains and not just at the GO stations to accurately identify which train a customer boarded and process refunds. With the current set-up of PRESTO machines installed at GO stations, Metrolinx cannot determine which train a customer has boarded, as trains could be scheduled between short intervals during rush hours, or if a customer taps to board a train and does not tap off, Metrolinx cannot know whether the customer was on board during the portion of the trip that was delayed. We reviewed the feasibility analysis and noted that an investment of $73 million would be required to install PRESTO tap machines on GO Trains and automate the refunds. Due to this significant investment, Metrolinx has decided to maintain the previous self-serve process, and expand the eligible fares to include paper and e-tickets.

- *assess the feasibility of establishing a consistent Service Guarantee Program for GO Transit and UP Express customers.*
  Status: In the process of being implemented by March 2023.

Details

Our 2020 audit found that Metrolinx's Service Guarantee Program was delivered inconsistently for customers on GO trains and UP Express, offering refunds based on different criteria. We noted that GO Transit's program offered a full refund of fares if GO trains are delayed by 15 minutes or more. UP Express customers are eligible to receive a fare refund if trains are delayed for more than 45 minutes.

In our follow-up, we noted that Metrolinx had performed a review of the feasibility of implementing a consistent and standard service guarantee program across GO Transit trains, buses and UP Express. While a service guarantee program had existed at the time of our 2020 audit for GO trains, Metrolinx is proceeding to implement the same service guarantee to UP Express that it offers for GO trains. The UP Express service guarantee will function identically to the GO train system with the same 15-minute guarantee. We reviewed the results of the feasibility analysis and noted that Metrolinx had considered the impact on revenue of offering a UP Express service guarantee and it was estimated to have an impact of approximately $57,000 annually. The UP Express service guarantee program is targeted to be implemented by March 2023.

In addition, to determine if a service guarantee is feasible for GO buses, Metrolinx performed a case study that considered a list of 35 regional bus transit agencies worldwide and found that a service guarantee for buses was only offered by one agency and was not automated. Based on the case study, Metrolinx decided it was not reasonable to implement a service guarantee program for buses, due to the unpredictability of external factors such as traffic and detour routes. It was also noted that the bus transit agency with the service guarantee saw a significant increase in fraudulent claims for refunds. Due to these factors, Metrolinx decided to not extend the guarantee program to buses, but only to UP Express.

Recommendation 3

In order to promote transit ridership and improve customer experience and satisfaction, we recommend that Metrolinx improve the reliability of PRESTO devices and cards by:

- *reviewing and analyzing the root causes of incidents to identify software and connectivity issues and take corrective actions to prevent these incidents from re-occurring;*
  Status: Fully implemented.

Details

In our 2020 audit, we found a significant number of IT incidents affecting PRESTO cards and devices, ticket vending machines, and station fare processors. PRESTO fare payment devices encountered software and hardware issues resulting in a number of problems that affected customers. From February 2016 to March 2020, PRESTO fare payment devices used for UP

Express, GO trains, and buses encountered over 45,000 such incidents.

In our follow-up, we noted that Metrolinx has enhanced its existing incident management system that is used to record and resolve IT incidents for PRESTO devices to also include a problem management module. A problem record allows for the ability to group similar, recurring incidents together and add a root cause classification to assist in performing an RCA. In our 2020 audit, we noted that Metrolinx performed root cause analyses (RCAs) only for Priority 1 and Priority 2 type of IT incidents that may have a significant impact on PRESTO devices, but not for Priority 3 or 4.

During our follow-up, we noted that RCAs are performed for all priorities of incidents, including Priority 3 and 4 incidents that affect PRESTO devices.

We reviewed a list of all problem records from November 2021 to November 2022 and noted that 112 problem records have been created to identify and resolve recurring Priority 3 and 4 IT incidents. We reviewed a sample of five problem records, and noted root cause analysis was performed for all problem records which included a reference to similar incidents and impact to customers and operations.

- *establishing a device lifecycle plan to ensure replacement of old and ineffective devices in a timely manner;*
  Status: Fully implemented.

Details

In our 2020 audit, we noted that ticket vending machines at GO Transit and UP Express stations are used to purchase paper tickets, and purchase and load PRESTO cards using cash, debit and credit cards. We noted that there were over 40,000 IT incidents over the last five years that rendered these machines partially or completely inoperable. These incidents included software issues caused by unplanned changes, interface issues between IT systems, and hardware issues where machines were unable to dispense tickets due to mechanical issues as a result of aging devices. Other IT incidents included, for example, display screen malfunctions in older devices and poorly written software code that caused machines to malfunction, rendering them inoperable.

In our follow-up, we noted a detailed PRESTO asset management plan was developed by Metrolinx in October 2021, which included a review of all PRESTO assets, along with documenting the age of devices, and lifecycles of assets for all PRESTO devices, including the ticket vending machines. Assets that have reached their end of lifetime are assessed for replacement on a continuous basis. We noted that as of September 1, 2022, Metrolinx has replaced about 2,700 devices as part of the asset replacement plan.

- *improving the existing Change Management process to detect exceptions such as unplanned changes, duplicate and delayed transactions;*
  Status: Fully implemented.

Details

In our 2020 audit, we noted that many IT incidents included, for example, display screen malfunctions in older devices and poorly written software code that caused machines to malfunction, rendering them inoperable. We analyzed these incidents and noted that over half related either to connection time-outs, software issues or hardware issues. Many of these software issues were caused by unplanned changes.

In our follow-up, we noted that, in July 2021, Metrolinx enhanced the Change Management process by expanding the scope of their Change Advisory Board (CAB) whereby they now review planned and unplanned changes to IT systems. The CAB meets twice a week to review all changes to ensure that changes are tested, approved by the right stakeholders (for example, IT, Cybersecurity and Business) and the process includes other necessary components, such as an implementation plan, fallback plan, and change impact. As per the new process, all changes are approved by the CAB before final implementation. We reviewed a sample of five change tickets and identified that the changes were tested, required plans were attached, approved by required individuals and implemented without errors.

- *implementing a process to calculate loss of revenue due to IT incidents that result from PRESTO devices being inoperable and factor this into future contracts with the IT device vendors.*
  Status: In the process of being implemented by November 2023.

Details

In our 2020 audit, we noted that from February 2016 to March 2020 there were over 3,500 IT incidents with green tap machines. Any problems with these devices at a high-traffic GO station (such as Union Station) may result in a number of inconvenienced customers. For example, for approximately two hours on February 25, 2019, the devices at Union Station were inoperable and unavailable for fare payment while the system updated. This impacted about 35,000 customers who were unable to pay their fares, resulting in an estimated loss of $315,000 in fare revenue. We had also noted that Metrolinx did not analyze and assess the loss of revenue due to tap machine outages.

In our follow-up, we noted that Metrolinx has updated its existing contracts with its vendors to include a clause to hold them accountable in case of missed service targets and will use the clause to calculate loss of revenue.

Loss of revenue has been addressed by commercial agreements created with Service Level Agreements (SLAs) for availability and restoration time. We reviewed the contract for the vendor responsible for managing and addressing IT issues with ticket vending machines and noted that a point system calculates reductions in service and availability and that Metrolinx is compensated according to standard clauses included in vendor contracts that reduce Metrolinx's invoices based on any failures by the vendor to restore service. This loss of revenue calculation has been defined. However, Metrolinx is in the process of updating the vendor contracts to include loss of revenue calculations, where applicable. At the time of our follow-up, there has been no breach of the defined SLAs by vendors and therefore no need to enact any of these clauses.

Recommendation 4

In order to effectively monitor IT vendor performance, we recommend that for all vendors, Metrolinx:

- *receive detailed reports for incidents at all priority levels broken down by priority level and review the reports to assess if resolution performance targets are being met within the required time frame, and take corrective action where necessary;*
  Status: Fully implemented.

Details

In our 2020 audit, we found that third-party contracts did not adequately allow Metrolinx to monitor vendor performance and escalate vendor incidents appropriately. We noted that performance targets are reported collectively, with performance information for all four priority levels (Priority 1, Priority 2, Priority 3, and Priority 4) consolidated, rather than by individual priority level as identified in the agreement. Reporting on each priority level separately is important because each priority level requires a different resolution time.

In our follow-up, we noted that Metrolinx has implemented monthly touch points with vendors to obtain service level reports, track performance and review any incidents with four existing PRESTO vendors: Telus, Accenture, Sheidt & Bachmann, and BAI Communications. Metrolinx now receives reports on incidents on a monthly basis from vendors that provide an overview of incidents and availability of services and SLA performance. We reviewed a sample of meeting minutes for the four PRESTO vendors, as well as for Flowbird, the Metrolinx vendor that was identified in the 2020 audit. We noted that monthly meetings are occurring with these vendors to assess if resolution performance targets are being met within the required time frame. We confirmed that Metrolinx and PRESTO had representatives attending the meetings and that they noted incidents for discussion. Additionally, Metrolinx has the ability to request the raw data used to generate the reports provided by the vendors, should it decide to perform its own validation of reported results.

- *incorporate clauses in contracts to hold vendors accountable and incentivize them to meet targets, and allow for penalties where targets are not met.*
  Status: In the process of being implemented by November 2023.

Details

In our 2020 audit, we noted that Metrolinx does not systematically analyze the information that is reported by Accenture to assess if targets are being met by individual priority level, and that Accenture miscategorized Priority 1 incidents as Priority 2 in 15 instances. We also noted that the contract between Metrolinx and Flowbird does not require monthly service level agreement reports or penalties that allow Metrolinx to hold Flowbird accountable for missed resolution-time targets for incidents at each priority level.

In our follow-up, we noted that all new contracts from December 2021 onwards include a standardized set of clauses that mandate vendor performance reports and meetings. We reviewed an extract of these clauses from contracts initiated after December 2021 and noted that they consistently include deductions from vendor invoices based on availability of the service or time to restore service from an incident. While this has been completed for Flowbird, we noted that for legacy and evergreen contracts, such as the one with Accenture that was established before December 2021, a third-party legal firm has been selected to develop enhanced clauses in new contracts that will go to market as part of the procurement process. This process was ongoing at the time of our follow-up.

Overuse and Overreliance on IT Contractors

Recommendation 5

To effectively manage its contract staff, we recommend that Metrolinx align with the Ontario Public Service Procurement Directive, and require that key roles and responsibilities be performed by qualified, full-time Metrolinx IT management staff.

Status: Fully implemented.

Details

In our 2020 audit, we found that contractors had key management roles in Metrolinx. Of the 307 IT contractors, about 80% (246) of these IT contract staff reported to three contractors holding management positions. Contrary to the Ontario Public Service (OPS) Directive, these three contractors were making decisions about project budgeting and recruiting contractors from staffing vendors.

In our follow-up, we noted that Metrolinx had reduced its total number of IT contractors from 243 in March 2021 to only 57 in March 2022, while increasing its full-time staff count from 148 to 262. We reviewed the position title for these 57 IT contractors and noted none of them had key management roles in Metrolinx.

Recommendation 6

To effectively and economically resource IT projects and align with the Ontario Public Service Procurement Directive, we recommend that Metrolinx:

- *assess the internal capability of IT resources before making the decision to hire contractors;*
  Status: Fully implemented.

Details

In our 2020 audit, we found that according to the OPS Procurement Directive, the decision to procure external consulting services must include prior consideration of using internal resources. Metrolinx has paid approximately $157 million to IT contractors, almost 2.5 times the salaries and benefits paid for Metrolinx staff, while the total costs for full-time IT employees were approximately $65 million. Based on our review of a sample of 25 contractor recruitment files, we found that for all 25, Metrolinx had not documented any review of internal capability, contrary to Metrolinx's own policy and the OPS directive that clearly requires a review of internal capability and a cost/benefit analysis for hiring a full-time employee before hiring a contractor.

In our follow-up, we noted that Metrolinx has implemented a documented process to consider full-time staff before a contractor can be hired. After a resource request is placed, an assessment is performed to check for staff internally. If staff are identified and

available, the request is filled. If there is no internal staff available, there is another assessment to determine if a contractor is needed, or if a full-time staff can be hired. This process requires approval from a Vice President (VP) before a contactor can be hired and is included as part of the overall framework created by Metrolinx to overhaul the resource management process for both contractors and full-time staff. From a total of 57 existing IT contractors we selected a sample of five and reviewed the internal capability assessment. We noted for all five IT contractor positions, Metrolinx performed an assessment of internal capability prior to hiring the contractor and the request to hire contractors was approved by the Vice President.

- *perform cost/benefit analyses to assess the economy and appropriateness of retaining contractors rather than hiring full-time employees, especially when resources are likely to be required long-term;*
  Status: Fully implemented.

Details

In our 2020 audit, based on our review of a sample of 25 contractor recruitment files, we found that for all 25, Metrolinx had not performed cost/benefit analyses for hiring contractors instead of full-time employees. This is contrary to Metrolinx's own policy and the OPS directive that clearly requires a cost/benefit analysis for hiring a full-time employee before hiring a contractor.

In our follow-up, we noted that the cost/benefit analysis was included as part of the updated framework that considers full-time staff over contractors. After it is determined that an existing internal full-time staffer cannot be used to fulfill a resource request, there is then an assessment to determine if a contractor is needed, or if the request is long-term and a full-time staffer can be hired. From a total of 57 existing IT contractors we selected a sample of five and reviewed their recruitment files to assess if Metrolinx had performed a cost/benefit analysis. We noted that an assessment was performed for all five contractors to ensure economy and appropriateness of retaining contractors rather than hiring full-time employees.

- *perform and document interviews, and retain interview notes including the required approvals prior to hiring contractors.*
  Status: In the process of being implemented.

Details

In our 2020 audit, we found that there were no documented records showing justification for new resources, or that approvals for procuring contractors were properly obtained by hiring managers. For 23 of the 25 contractor recruitment files we reviewed, Metrolinx did not have any documents for candidates interviewed for contractor roles, interview notes, or names of the employees that participated on the interview panel.

In our follow-up, we noted that Metrolinx has established a centralized process identical to the one implemented for full-time staff, in which a calculated score is assigned to all candidates for a role based on documented interview answers. We selected nine recruitment files for IT contractors hired after our 2020 audit to assess whether interview notes were documented along with the names of the employees that participated on the interview panel. We noted that for five IT contractors Metrolinx did not document and retain interview notes. We also noted that two of these five IT contractors were hired directly, bypassing the interview process without any formal justification. Upon our review, Metrolinx is committed to fully implement this recommendation by documenting and retaining interview notes in all future hiring of contractors.

Recommendation 7

So that Metrolinx manages its IT resources efficiently and effectively, we recommend that Metrolinx:

- *align with the Ontario Public Service Procurement Directive and document the rationale and justification for contract renewals or extensions;*
  Status: Fully implemented.

Details

In our 2020 audit, we observed that Metrolinx was not providing appropriate justification or performing evaluations of vendor performance before renewing or extending contractors' contracts. Based on our sample of 25 IT contractors, 20 (or 80%) had their contracts extended by their managers.

In our follow-up, we noted that every contractor renewal is now mandated to have a documented rationale and VP approval, which is stored in an IT system. We reviewed a sample of five contract renewal documents, and noted that all five contractors had received adequate justification and documented rationale, approved by a VP prior to their contract extension.

- *confirm through performance evaluations that the contractor is performing satisfactorily and obtain the appropriate approvals prior to the renewal or extension of a contract;*

  Status: Fully implemented.

Details

In our 2020 audit, we noted that none of the 20 contract extensions we sampled had business justifications for the extensions provided or had performance evaluations conducted by their managers to ensure the adequacy of their work.

In our follow-up, we noted that as of March 2021, Information & Information Technology (I&IT) conducts a performance survey prior to every contract renewal and contractor departure. We reviewed five sample performance reviews and noted that the survey rates the contractor's technical requirements, professionalism, and whether the manager wants to re-hire and extend the contract. We also noted that all five contract extensions had been appropriately approved by a VP via email prior to extension of the contract.

- *assess the rationale for increases in contractors' hourly rates so that the revised rates are economical;*

  Status: Fully implemented.

Details

In our 2020 audit, we found that contractors were also consistently receiving rate increases without documentation or rationale to justify the increases. Based on the sample of 25 contractors whose recruitment files we reviewed over the previous five years (at the time of the audit), we found that Metrolinx paid increased hourly rates to 12 (or 48%) of the 25 contractors. There were no reasons identified for these increases, such as promotions to more senior roles or being assigned more responsibilities. These hourly rate increases ranged from 4% to 12%.

In our follow-up, we noted that Metrolinx has implemented a new vendor management process to ensure any contractor that requests a rate increase has their request reviewed for justification and approved by the applicable Vice President. As part of the vendor management process, Metrolinx reviews the tenure of the contractor and when the last rate increase was given and conducts a comparison against other contractors in the same role on the same contract. There is a defined maximum rate for each role that cannot be exceeded by the rate increase. The rate increase must also be approved by the applicable Vice President and Chief Information Officer before the contract can be amended. We reviewed all three contractors who had their rate increased and noted that all three increases were appropriately approved by an applicable Vice President and the Chief Information Officer with appropriate rationale provided. We also reviewed three rate increase requests that were rejected, and noted that one request to increase a contractor's hourly rate above the maximum for that role was denied with justification being documented as the rate being beyond the maximum. We also noted two other instances where contractors that had requested to switch to a role with a higher rate were also denied, as the requestors could not provide detailed justification to switch to that role to get higher pay.

- *conduct a comprehensive qualitative and quantitative analysis of its outsourcing strategy and obtain both board and ministry approvals prior to any major strategic change such as IT department outsourcing.*

  Status: Fully implemented.

Details

In our 2020 audit, we noted that Metrolinx had a strategy in April 2020 to hire more full-time staff instead of contractors to reduce the existing overreliance on contractors, reduce costs and help retain knowledge within the organization. The ratio of contractors to full-time employees had increased from 40% to 63% from 2015/16 to 2019/20. The strategy was presented to the Metrolinx's Board of Directors and the Chief Executive Officer and senior leadership team and the department was approved to hire about 60 full-time IT staff. However, in August 2020, we found that Metrolinx had considered engaging a research firm to develop options for outsourcing certain activities within the IT department in order to transfer the technology risks to an outsourced vendor.

In our follow-up, we noted that Metrolinx has not outsourced any of its Information Technology functions such as Project Management Office, IT Infrastructure, IT Development and Delivery, and IT Architecture and Information Security. Instead, Metrolinx has hired a new Chief Information Officer and four Vice Presidents to manage the four technology divisions noted above. In addition, if there were any large decisions such as outsourcing the entire Information Technology division, Metrolinx indicated that it would involve the Ministry of Transportation and its Board for approvals.

Security Weaknesses in Metrolinx's IT Systems

Recommendation 8

To minimize Metrolinx's vulnerability to cyberattack and accidental release of information, we recommend that Metrolinx reduce its risks and more effectively protect across its IT systems by performing security tests, such as penetration testing, on its critical IT systems and websites regularly, according to industry standards.

Status: Fully implemented.

Details

In our 2020 audit, we found that Metrolinx lacked regular security testing of IT systems to identify weaknesses and prevent breaches from occurring. With the exception of the PRESTO IT system, we noted that Metrolinx had not performed regular penetration tests on critical IT systems and websites for years. As a result, we noted IT systems were vulnerable to attack and resulted in two significant security breaches.

In our follow-up, we noted that Metrolinx has implemented a new IT system, to perform regular testing including vulnerability scans for new product releases and major changes. In addition, Metrolinx has developed a schedule for vulnerability scans and penetration testing. We reviewed the security testing schedule for the last two years and all penetration tests that have been performed since our 2020 audit. We noted that Metrolinx has performed regular penetration testing for its IT network and individual IT systems. In addition, we also noted that penetration testing for the IT network was re-performed to ensure previously identified weakness were remediated. All IT systems identified in the audit were included in these penetration tests and risks were identified and remediated.

Recommendation 9

To effectively protect its IT systems from the risk of cyberattack due to security weaknesses, we recommend that Metrolinx regularly review essential and critical transit system software codes according to industry best practices.

Status: In the process of being implemented by March 2023.

Details

In our 2020 audit, we found that Metrolinx did not perform reviews of software code to identify security weaknesses. We found that the software code had not been reviewed for any of the 12 sampled IT systems for security weaknesses. According to industry best practices, organizations should perform software code reviews whenever changes are made to critical IT systems to determine security weaknesses.

In our follow-up, we noted that Metrolinx has implemented a new IT system, which it uses to perform software code reviews for Metrolinx IT systems. All new projects go through the code review process to identify errors and all identified errors must be

resolved or go through a formal process to gain an exception prior to going live. We reviewed a sample code review and confirmed that findings and errors were identified to be remediated. At the time of the follow-up, we noted that four IT systems had been onboarded into the code review IT system and code reviews have been performed. Metrolinx is currently in the process of onboarding an additional 26 IT systems into the code review IT system. Metrolinx indicated that all new IT systems implemented will be onboarded into the code review IT system.

Recommendation 10

To effectively protect information and comply with the Freedom of Information and Protection of Privacy Act *requirements, we recommend that Metrolinx:*

- *safeguard all personal information by classifying the data and masking or encrypting it using industry best practices;*
  Status: Little or no progress.

Details

In our 2020 audit, it was observed that not all Metrolinx customer personal information was adequately protected. With the exception of PRESTO, we found in our review that Metrolinx does not consistently identify, classify and protect customer and employee personal information. Since this information is covered by the province's *Freedom of Information and Protection of Privacy Act* (FIPPA), Metrolinx is required to store and transfer any personal information in a secure manner, as well as create an annually updated inventory of its customers' personal information.

In our follow-up, we noted that Metrolinx has not performed an assessment as per its data classification policy to identify highly sensitive data and apply adequate protection such as encryption. Metrolinx has implemented an IT system used to scan and identify Personal Identifiable Information (PII). We noted that Metrolinx is currently in the process of identifying IT systems that contain highly sensitive information, as per Metrolinx's Information Security Policy. The assessment is expected to be completed by May 1, 2023.

- *restrict access to sensitive corporate information according to industry standards and best practices;*
  Status: Little or no progress.

Details

In our 2020 audit, we noted that Metrolinx has seven IT database administrators with full access to read and modify confidential Metrolinx customer and employee personal information stored in two databases. Further, three of the seven IT database administrators were contractors, not full-time Metrolinx employees. We also noted that four administrators of the Oracle database were sharing administrator user IDs and passwords, making it less likely that Metrolinx would be able to establish accountability in the event of an error or breach.

In our follow-up, we noted that Metrolinx has not limited or removed the excessive access to its databases that store confidential information. In addition, we noted that passwords were still being shared among the four administrators identified in our audit. However, Metrolinx has initiated a Privileged Access Management (PAM) project to implement an IT system to securely store and share administrator IDs. We reviewed the project scope and noted that the project roadmap will be created by November 2022. Additionally, we reviewed four sample meeting minutes from biweekly meetings that Metrolinx has established, and noted that it reviews any changes or additions to all administrator user groups.

- *review password settings for all critical IT systems and enforce its password policy to reduce the risk of unauthorized access;*
  Status: In the process of being implemented by March 2023.

Details

In our 2020 audit, we noted that four administrators of the Oracle database were sharing administrator user IDs and passwords, making it less likely that Metrolinx would be able to establish accountability in the event of an error or breach.

In our follow-up, we noted that Metrolinx is in the process of implementing a new IT system, which will enforce password policies to reduce the risk of unauthorized access. At the time of our follow up, password policies had been enforced for all IT systems that rely on Microsoft Windows authentication. However, Metrolinx is still in the process of implementing the IT system to enforce password policies for IT systems that have their own authentication process. As of September 1, 2022, there were 22 IT systems that Metrolinx had onboarded into the password IT system. Metrolinx is also in the process of migrating its Oracle IT System to the password IT system, which will enable multi-factor authentication for Oracle.

- *implement audit logging capabilities and alerts for events that are necessary for ensuring accountability and protecting information.*
  Status: Fully implemented.

Details

In our 2020 audit, we noted that Metrolinx does not log necessary activities in the event a database table is either modified or deleted. Detailed database logs and tracking activities performed by database administrators allow organizations to establish accountability, identify unauthorized data modification and detect fraud-related activities.

In our follow-up, we noted that Metrolinx has installed an IT system that is used to monitor IT security threats on its network. We reviewed a sample report for January 2022 for threat events, such as phishing and computer viruses, that occurred, including severity of the threat event and resolution status. In addition, we noted that audit logging capabilities were implemented for the Oracle database in August 2021.

Lack of Disaster Recovery Strategy

Recommendation 11

To better manage risks to information technology systems that are critical to transit services, we recommend that Metrolinx:

- *establish a disaster recovery strategy, and plan and perform disaster recovery exercises on a regular basis in order to minimize disruptions due to IT incidents;*
  Status: In the process of being implemented by March 2023.

Details

In the 2020 audit, we found that Metrolinx lacked any disaster recovery (DR) strategy or regular testing. We noted that Metrolinx had not established an organizational disaster recovery strategy to ensure continuity of business operations.

At the time of our follow-up, we noted that Metrolinx was developing a DR strategy and was in the process of setting up the infrastructure required for the strategy to be operational. DR exercises were not yet being performed; however, Metrolinx has performed an assessment of its IT systems to identify the 54 most critical systems, and has established a plan to develop a DR test exercise for all 54 critical IT systems. We reviewed a schedule for the DR project and noted that DR is set to be fully operational for the most critical 20 out of 54 critical IT systems identified by Metrolinx by October 2022, with the remaining IT systems to follow.

- *perform a cost/benefit analysis for establishing a functional disaster recovery location for continuity of transit operations.*
  Status: In the process of being implemented by March 2023.

Details

In our audit, we found that the Kingston Data Centre was Metrolinx's DR site. The Kingston centre, however, is not equipped with the necessary servers, software and data to function as an alternative location in case of a disaster. Because any disaster affecting the Guelph Data Centre could result in significant delays to transit operations, back-ups and redundancies should be established so that service outages can be minimized.

In our follow-up, we found that Metrolinx has performed a cost/benefit analysis and selected a private data centre in Barrie, Ontario, to be the DR site for all applicable systems. We reviewed the contract between

Metrolinx and the vendor that owns the Barrie Data Centre and noted that it was signed October 1, 2021. At the time of the follow-up, the infrastructure required for the site was being installed in order for the site to be operational. We also noted that a comprehensive DR exercise has not yet been performed.

Lack of IT Strategy Results in Duplicate Costs, Resources and Avoidable Cost Overruns in IT Projects

Recommendation 12

In order to reduce duplicate costs and efforts, and improve the oversight of IT operations, we recommend that Metrolinx:

- *set an overall IT strategy with a centralized procurement process for IT systems and services;*
  Status: Fully implemented.

Details

In the 2020 audit, it was observed that IT projects lacked a centralized procurement process to avoid duplicate costs and avoidable cost overruns. Metrolinx has a decentralized approach for procuring IT systems with no overall IT strategy or effective oversight. According to the Ontario Public Service Procurement Directive, organizations should validate if the same goods and services already exist within the organization before a new procurement process is initiated.

In our follow-up, we noted that in August 2021, a new director for Corporate I&IT Procurement was hired to lead a dedicated team for procurement. A strategy was established that stipulates that all procurement is facilitated by the dedicated I&IT procurement team. There is a process to first go through existing Metrolinx Vendors of Record and then justify and gain approval from the procurement team to seek another external vendor. For all new IT systems that Metrolinx wants to implement, prior to requesting funding, the project must undergo a full architectural review to ensure existing technology is used where possible. We reviewed a recently procured IT system, Microsoft Customer Insights, that provides analytics-related data from Metrolinx's existing IT system. We noted that the procurement documents included business requirements and was compared against two others existing Metrolinx IT systems across all businesses to verify that the existing systems do not satisfy requirements adequately or cost-effectively. For the sampled IT systems reviewed in the 2020 audit, we noted that Metrolinx has performed an assessment and is in the process of replacing duplicate IT systems.

- *monitor and assess the need for existing IT systems or devices installed across the organization, and establish a process to determine if there is an existing system within Metrolinx prior to procuring any new IT systems.*
  Status: In the process of being implemented by October 2023.

Details

In our audit, we found that some departments had procured additional IT systems and services when other departments already possessed the same systems or functions that were needed. Metrolinx's decentralized approach to IT governance has resulted in a lack of centralized knowledge about IT systems that are being used in different departments across the organization.

In our follow-up, we noted that, in February 2022, Metrolinx Procurement, I&IT, and the Commercial Office jointly introduced a monthly relationship management forum that supports the strategy, planning, prioritization and oversight of IT-related procurement transactions. A weekly strategy standup is also held with attendees including the Chief Information Officer, the Vice President of IT, Director Procurement, Vice President Commercial, and Director Commercial. We reviewed an assessment completed by Metrolinx to identify duplicate IT systems and noted that 32 systems were identified and a strategy is in place to leverage existing technology where applicable.

Recommendation 13

To save costs and realize potential efficiencies, we recommend that Metrolinx:

- *review and consider existing websites;*
  Status: Fully implemented.

Details

In our 2020 audit, we found that Metrolinx had a total of 20 different websites with overlapping functionality, similar information and unnecessary development costs. Metrolinx has a total of eight customer websites with various features such as ticket purchasing, trip planning, schedules and service updates. In total, Metrolinx has paid approximately $44 million in capital costs for the development of these websites, and pays approximately $14 million annually for maintenance and operating costs to various vendors.

In our follow-up, we noted that Metrolinx has created a development plan to consolidate all the 20 identified duplicate websites into three unique websites. Website development had commenced at the time of our follow-up and evidence of an implementation schedule was provided, with the first consolidated website going live in September 2022 and all remaining duplicate websites will be consolidated and launched as part of the remaining websites by March 2023.

- *assess the information and functionality requirements, and perform cost/benefit analyses to identify if a new website is required in the future, or if an existing website should be enhanced.*
  Status: In the process of being implemented by March 2023.

Details

In our 2020 audit, we found that three of the eight websites provided similar information with overlap, such as corporate information and construction updates.

In our follow-up, we reviewed evidence of investment panel approval of the project to merge the websites, approved on April 13, 2021. We noted that a vendor was selected to perform the development work to merge the existing websites, with a contract award memo having been approved on March 4, 2022. We reviewed a development schedule, as at August 2022, and noted that the vendor had completed several stages of the project and was on track according to its schedule, to release the first merged website on September 27, 2022.

Recommendation 14

To improve the oversight of IT projects and improve project management practices so that IT projects are completed on time and within estimated budgets, we recommend that Metrolinx:

- *clearly define and provide necessary details in project scope;*
  Status: Fully implemented.

Details

In our 2020 audit, we observed poor project management and oversight practices at Metrolinx, resulting in project cost overruns, delays, and cancellations. Based on our review, we found that Metrolinx's project management process does not ensure that IT projects are delivered within approved budgets and timelines.

In our follow-up, we found that all action plans for this recommendation were addressed through a new agile development method implemented by Metrolinx that uses a 90% "on time" delivery target. This development method includes a clear project scope, and a monthly project review has been implemented to review projects that are in "red" status to ensure concerns are identified. We reviewed two sample projects, the Customer Digital Transformation Strategy (CDTS), and Identity and Access Management projects. We noted that Metrolinx retained and reviewed a detailed project scope in steering committee meetings that explains project milestones, risks, and project dependencies for both projects.

- *properly document and monitor project timelines, budgets and costs;*
  Status: Fully implemented.

Details

In our 2020 audit, we found that Metrolinx's project management process does not ensure that IT projects are delivered within approved budgets and timelines. About 72% of all completed IT projects experienced combined cost overruns of approximately $152 million for a total IT projects cost of $288 million, more than double the initial estimate of $136 million.

In our follow-up, in addition to the monthly project review noted in the previous recommendation, monthly exception reports are presented by Metrolinx to the investment panel on all red or yellow status projects. We reviewed submissions made by Metrolinx to the investment panel for the two sampled projects, and noted that Metrolinx includes detailed budgets and cost projections broken down by specific requirement, and whether the work is being performed by a vendor or Metrolinx. The submission also lists out key milestone dates to be approved, as well as lists all previous milestone dates from previous investment panel submissions for the same project.

- *ensure proper oversight over project changes with well-documented justification and appropriate approvals.*

  Status: Fully implemented.

Details

In our 2020 audit, we identified systemic issues in IT project management and operations, including a lack of oversight over project changes.

In our follow-up, we noted that Metrolinx's top 10 projects were identified for an exercise to test the newly implemented agile development method and it has now been extended to all projects. Additionally, a steering committee has been established to review changes occurring in key projects. We reviewed the presentation decks for the steering committee for two months for each of our two selected projects, Revenue Accounting Management System (RAMS), and Identity and Access Management. We noted that the presentations included detailed breakdowns of outstanding issues and status, and a roadmap of the current status of what has been done and what needs to be completed, with key dates attached to each step. The key purpose and requirements of the project are listed as well, with the budget allocations used to date to ensure that the project requirements are being met in a timely fashion, cost-effectively, and to the specifications noted in the original project scope.