



Office of the Auditor General of Ontario

Value-for-Money Audit
Information
Technology (IT)
Systems and
Cybersecurity
at Metrolinx



December 2020

Information Technology (IT) Systems and Cybersecurity at Metrolinx

1.0 Summary

Information Technology (IT) systems play a vital role in managing day-to-day public transit operations at Metrolinx. In the 2019/20 fiscal year, Metrolinx provided a total of over 76 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 enables customers to purchase and load funds to PRESTO fare cards, and pay fares by tapping the cards on machines at train stations and on buses. Customers can also purchase individual tickets at stations from vending machines and from station attendants at customer service windows. PRESTO and other fare payment operations are also heavily dependent on IT systems.

IT systems and related technology components for critical transit operations have experienced frequent problems resulting in train delays and cancellations. Problems originating with Metrolinx IT systems and related technology components include network connectivity issues, system malfunctions, and software and hardware issues. In the last five years, nearly 4,500 GO train and UP Express delays and cancellations were the result of IT software and hardware issues. These issues have resulted in financial impacts from revenue loss of approximately \$450,000 for Metrolinx, as well as customer inconvenience.

Metrolinx has a Service Guarantee Program to refund trip fares to customers when their trains are delayed by 15 minutes or more, or boarded train trips cancelled after they departed due to factors within Metrolinx's control. We noted that Metrolinx does not automatically refund customers who qualify for the Program, although it has the technology and necessary data to do so. Instead, customers on eligible trips are encouraged to submit an online refund claim through the service guarantee portal at GOtransit.com. In the last five years, approximately \$2.2 million of eligible refunds directly related to train delays and cancellation from IT-related issues were not claimed by customers and were kept by Metrolinx.

We also noted Metrolinx's overreliance on IT contractors. The majority (63%) of Metrolinx's 435 IT staff were on contracts in 2019/20. Many of

these contractors held management positions and key decision-making roles, often overseeing other IT contractors hired to support day-to-day IT operations and services.

We also found that Metrolinx did not consistently test its critical IT systems and websites for security weaknesses. Many IT systems had not been tested for years and others had never been tested. Also, we found that software code had not been reviewed for all 12 critical IT systems we sampled for security weaknesses. These included systems for safety, dispatch, track allotment, scheduling and communications. Not performing regular penetration testing or reviewing software code that can identify system weaknesses resulted in two significant security breaches in the last five years. With weak security controls, Metrolinx customers' personal information, with the exception of PRESTO customer information, is not protected.

The following are some of our significant audit findings:

Train Operations

- **Frequent IT incidents caused train delays and cancellations, resulting in lost revenue.** Critical transit operations have experienced frequent IT-related incidents, such as network connectivity issues, system malfunctions, software and hardware issues resulting in train delays and cancellations. We noted that over the last five years, from January 2015 to January 2020, there were nearly 4,500 GO train and UP Express delays and cancellations resulting from IT software and hardware issues. Of all train delays and cancellations caused by IT incidents, 42% were at rail crossings where roads cross rail lines. Where rail crossing systems fail, rail crews must physically stop traffic and manually protect the crossing before the train proceeds—this causes significant delays. In the last five years, train delays and cancellations attributable to IT incidents have caused

customers to be inconvenienced and have resulted in approximately \$450,000 in lost revenue due to refunds through the Service Guarantee Program.

- **PRESTO customers are not refunded automatically with the Service Guarantee Program.** Eligible customers do not always receive a fare refund as entitled under the Service Guarantee Program when experiencing train delays of 15 minutes or more or cancellations that are within Metrolinx's control. We found that although Metrolinx has the technology and necessary data to automatically refund customers who qualify for the program, Metrolinx does not do this. Instead, only those customers who apply for the refund receive it. Of the 4,500 train delays and cancellations caused due to IT incidents, only 23% of the eligible customers applied for the Service Guarantee program for a total refund of approximately \$450,000, with another approximately \$2.2 million of eligible refunds kept by Metrolinx.

PRESTO Fare Payment System

- **IT incidents occur with PRESTO fare payment devices.** PRESTO ticket vending machines and green tap machines installed at GO and UP Express stations have experienced frequent IT incidents, such as faulty displays, an inability to dispense transit tickets, paper and coin jams and Internet connectivity outages that render the machines inoperable. We noted over 45,000 IT incidents with fare payment devices in the last five years, mostly in ticket vending machines and green tap machines. The vast majority of the 45,000 incidents did not have a significant impact on Metrolinx's customers, as stations are equipped with more than one fare device of similar type. Nevertheless, customers' experience was impacted, as they had to find a working fare device in order to pay for

their fare. We found that Metrolinx does not always record details, such as the root causes of these incidents and the steps taken to resolve them in order to help prevent these IT incidents from recurring.

- **PRESTO customers charged incorrect fares.** PRESTO's IT system charged customers twice, and charged regular adult fares instead of reduced fares to students and seniors. In addition, funds were not added to customers' PRESTO cards on time, resulting in PRESTO customers' cards being declined due to insufficient funds. We noted that there were over 6,700 fare-related IT incidents with PRESTO cards from January 2016 to April 2020. For example, one incident resulted in about 940 PRESTO customers being charged for monthly passes twice for the same month on the same day. This incident was due to an IT batch job that processed a sales order twice. In this particular case, all 940 customers were proactively reimbursed.

Overreliance on IT Contractors

- **Contractors are recruited without the required analysis of other options, and many hold key decision-making roles.**
 - Metrolinx neither assesses whether it already has the resources nor considers whether it should hire full-time employees prior to contracting resources at much higher rates. Metrolinx relies heavily on external contractors for IT operations and services, and has 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.
 - 80% of IT contractors we sampled had their contracts extended without

business justification or performance evaluations conducted.

- Contractors hold 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.

Cybersecurity

- **Metrolinx has not consistently tested its IT systems for cybersecurity risk.** With the exception of the PRESTO IT system, Metrolinx does not perform regular security scans, such as penetration tests, on selected critical IT systems and websites to identify security weaknesses. We noted that Metrolinx has been subject to cyberattacks resulting in breaches of its customers' personal information. For example, the Eglinton Crosstown website (thecrosstown.ca) was hacked three times between February 15, 2019 and March 27, 2019 resulting in customer data breaches.
- **Software code for transit IT systems is not reviewed for security weaknesses.** Software code, the instructions written by computer programmers, is not reviewed regularly to identify security weaknesses in critical transit IT systems. Metrolinx neither performs regular software code reviews, nor requires vendors that own the software code to perform these scans to identify security weaknesses. We found that software code for all 12 critical IT systems that we sampled had never been reviewed for security weaknesses. In December 2018, the lack of software code reviews resulted in a breach of the personal information—names, addresses and emails—of more than 100,000 Metrolinx customers.
- **The personal information of Metrolinx's customers is not consistently secured**

according to the *Freedom of Information and Protection of Privacy Act (FIPPA)*.

With the exception of the PRESTO IT system, Metrolinx does not consistently safeguard its customers' personal information by applying security controls such as encryption. We also found that 7 Metrolinx staff have access to customers' and employees' unencrypted personal information, which increases the risk of this information being accessed for inappropriate purposes.

Disaster Recovery

- **Metrolinx has not established a disaster recovery strategy.** Metrolinx, with the exception of PRESTO, does not have a disaster recovery strategy, and has not tested its ability to recover its operations in an event of an actual disaster such as a major cybersecurity attack, software issues from unplanned changes or power outages. In addition, although Metrolinx has an alternate data centre, we found that it is not equipped with the necessary servers and software that would allow Metrolinx to switch its IT operations to the alternate data centre in case of a disruption at its primary data centre.

IT Strategy

- **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.

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

Overall Conclusion

Our audit concluded that Metrolinx does not always have systems and processes in place to manage its IT operations effectively, efficiently or with due regard for economy. Critical transit operations, including PRESTO, have been negatively impacted by IT system issues. Unresolved and recurring IT incidents have resulted in transit delays and cancellations, as well as fare payment and ticket purchase device malfunctions and outages. Further, although Metrolinx has the technology and necessary data to automatically refund fares to PRESTO customers who are eligible for the Service Guarantee Program, it does not do so. Customers may use the existing online submission form at GOtransit.com to submit a claim.

We also found that Metrolinx is overreliant on IT contractors for day-to-day operations of IT systems and services. Metrolinx spends more for IT contract staff than it would have for regular full-time staff, and does not always ensure that contract staff provide better value for money when making hiring decisions.

Metrolinx's cybersecurity functions are weak. We found that Metrolinx has not regularly performed security tests for selected IT systems and websites to identify potential vulnerabilities, and information stored on its servers is not consistently safeguarded

by encryption. As a result, the personal information of Metrolinx employees and customers, as well as sensitive corporate information, is not secure.

At the time of our audit, Metrolinx also lacked a disaster recovery strategy for the Guelph data centre and had not performed a comprehensive recovery testing to ensure service disruptions are minimized and restored quickly in the event of a disaster.

As well, Metrolinx lacks an overall IT strategy, resulting in redundant IT systems and websites. Poor IT project management practices contributed to cost overruns, as well as project delays and cancellations after millions had already been spent.

This report contains 14 recommendations, with 32 action items, to address our audit findings.

OVERALL METROLINX RESPONSE

Metrolinx thanks the Auditor General and her team for the Information Technology (IT) Systems and Cybersecurity audit. The findings will help support the transformation of the overall technology function at Metrolinx.

Metrolinx is committed to delivering safe and reliable services to our customers that are easy to use, engaging communities where neighbourhoods are being transformed by transit projects and ensuring strong corporate systems to underpin the growing complexity and scope of the Metrolinx business. On-time performance is important to our customers, and Metrolinx will implement the recommendations to further address technology delays and cancellations as part of ongoing continuous improvement efforts. Metrolinx will also complete a review of the Service Guarantee Program and assess the feasibility of implementing automated refunds. Asset management plans will be strengthened for PRESTO devices, and further root-cause analysis will be undertaken on IT incidents at all priority levels.

Metrolinx takes the recommendations to better protect personal and employee information very seriously. Metrolinx agrees with the

Auditor General that there are opportunities to improve the protection of some personal and employee information. This has been a priority for our organization, and Metrolinx has taken measures to ensure fare payment information is secure and compliant with industry standards. Further, Metrolinx will take additional measures to enhance protection of personal information in alignment with the Auditor General's recommendations.

Actions have been already taken to enhance governance and accountability for technology projects, strengthen project controls, and better define scope before initiating projects. The Board of Directors approved an updated capital approvals policy in February 2020 that strengthened approval and oversight processes for technology projects. Business units are now accountable for direct oversight of their technology projects and ensuring that projects meet intended outcomes, on time and on budget. Metrolinx has also strengthened its existing vendor management process to monitor vendors' performance and impose fines for non-compliance.

Metrolinx is bringing on an experienced technology leader to drive forward further transformation. As part of this important work, Metrolinx plans to continue to develop and roll out an overarching IT strategy, and plans to address the recommendations made in this audit.

2.0 Background

2.1 Overview of Metrolinx IT Operations

The IT department at Metrolinx is responsible for the operation and maintenance of Metrolinx's information systems and technology infrastructure, as well as managing the IT contractors and external vendors procured for IT projects and

day-to-day operations. The IT department provides technical support and cybersecurity services and maintenance. The department also provides Internet connectivity for GO and UP Express stations, ticket vending machines, PRESTO fare payment devices and wireless internet at GO and UP Express stations. See **Figure 1** for an overview of Metrolinx's Information Technology structure and staff allocation.

IT systems and data that support Metrolinx operations, transit safety, communications, and corporate IT systems are hosted at the following data centres:

1. **The Guelph Data Centre** is a primary data centre used for transit IT systems for scheduling and tracking UP Express, GO trains and buses, customer communications for service alerts, delays and changes, the Metrolinx/GO Transit website and corporate systems such as financial and email IT systems.
2. **The Kingston Data Centre** is an alternative data centre used by Metrolinx mainly for testing purposes where it tests changes made to existing IT systems to ensure changes meet business requirements and integrate well with other systems.

Key IT systems at Metrolinx support the following areas. See **Figure 2** for an overview of key IT systems that support transit services to customers.

1. **Transit operations** – Train signals and track allotment systems, train and bus planning, scheduling, tracking for arrivals and departures, timekeeping, digital signs at train stations and bus stops, and vehicle information such as position (GPS) and engine maintenance data.
2. **Transit safety** – Dispatch transit safety officers, co-ordination with appropriate police and emergency services, CCTV cameras for 24/7 monitoring of train stations, bus stops, corporate offices, revenue protection and parking enforcement activities.
3. **Communications** – Emergency mass notification, alerts via email, mobile

text messages and Twitter, as well as GO Transit and UP Express websites and customer complaints.

4. **Corporate systems** – IT incident tracking system, customer relations management system, email, mobile management, anti-virus software for virus and malware protection, and VPN for remote access.
5. **Ticket purchase** – GO Transit and UP Express websites, UP Express mobile application, PRESTO website, and PRESTO devices.
6. **Metrolinx websites and mobile application** – Primary customer communication channels for alert notifications, service disruptions, trip planning, changes to platforms or service, ticket purchase and fare calculation. Currently, Metrolinx has eight different websites and two mobile applications.

2.2 Metrolinx Rail and Bus Services Operations

Metrolinx operates GO trains across the Greater Toronto and Hamilton Area (GTHA) and beyond through its network of rail lines. (See **Figure 3** for Metrolinx's transit lines.) IT systems and related technology components, also known as Operational Infrastructure, such as rail signals, switches, rail crossings, scheduling systems, and others, are used to efficiently manage the movement and operation of GO trains across the system. Metrolinx's rail lines include:

1. **Lakeshore West:** Between Toronto Union Station and Aldershot station or Hamilton, consisting of 14 train stations covering communities such as Mississauga, Oakville, Burlington, Hamilton and Niagara Falls. Stops beyond West Harbour are shared with VIA Rail.
2. **Lakeshore East:** Between Union Station and Oshawa consisting of nine train stations covering communities such as Scarborough, Pickering, Ajax and Whitby.

Figure 1: Metrolinx IT Organizational Chart, Responsibilities, Full-Time Equivalent (FTE) Staff and Contractor Complements, March 2020

Prepared by the Office of the Auditor General of Ontario

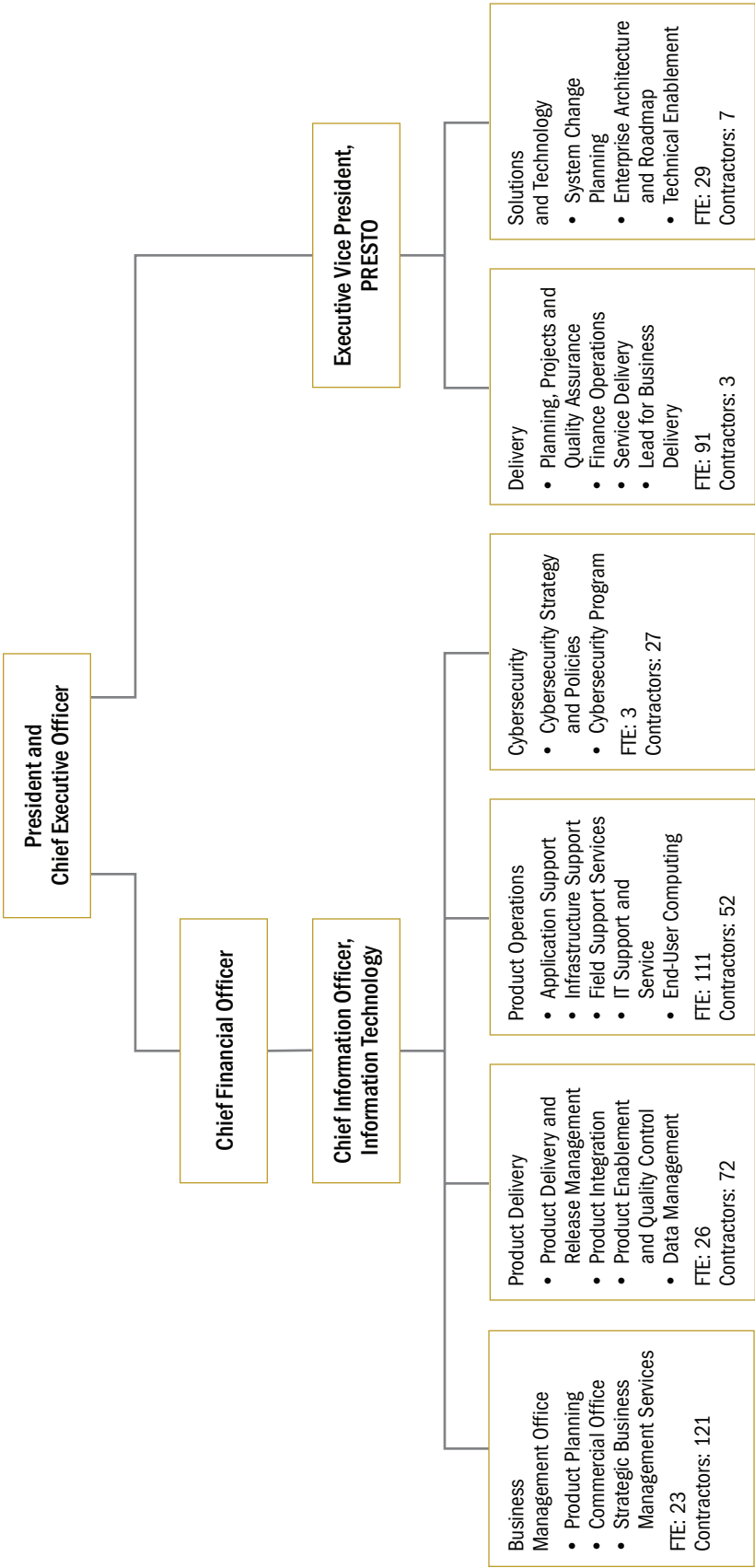


Figure 2: A Metrolinx Passenger Journey and IT Support Systems

Prepared by the Office of the Auditor General of Ontario







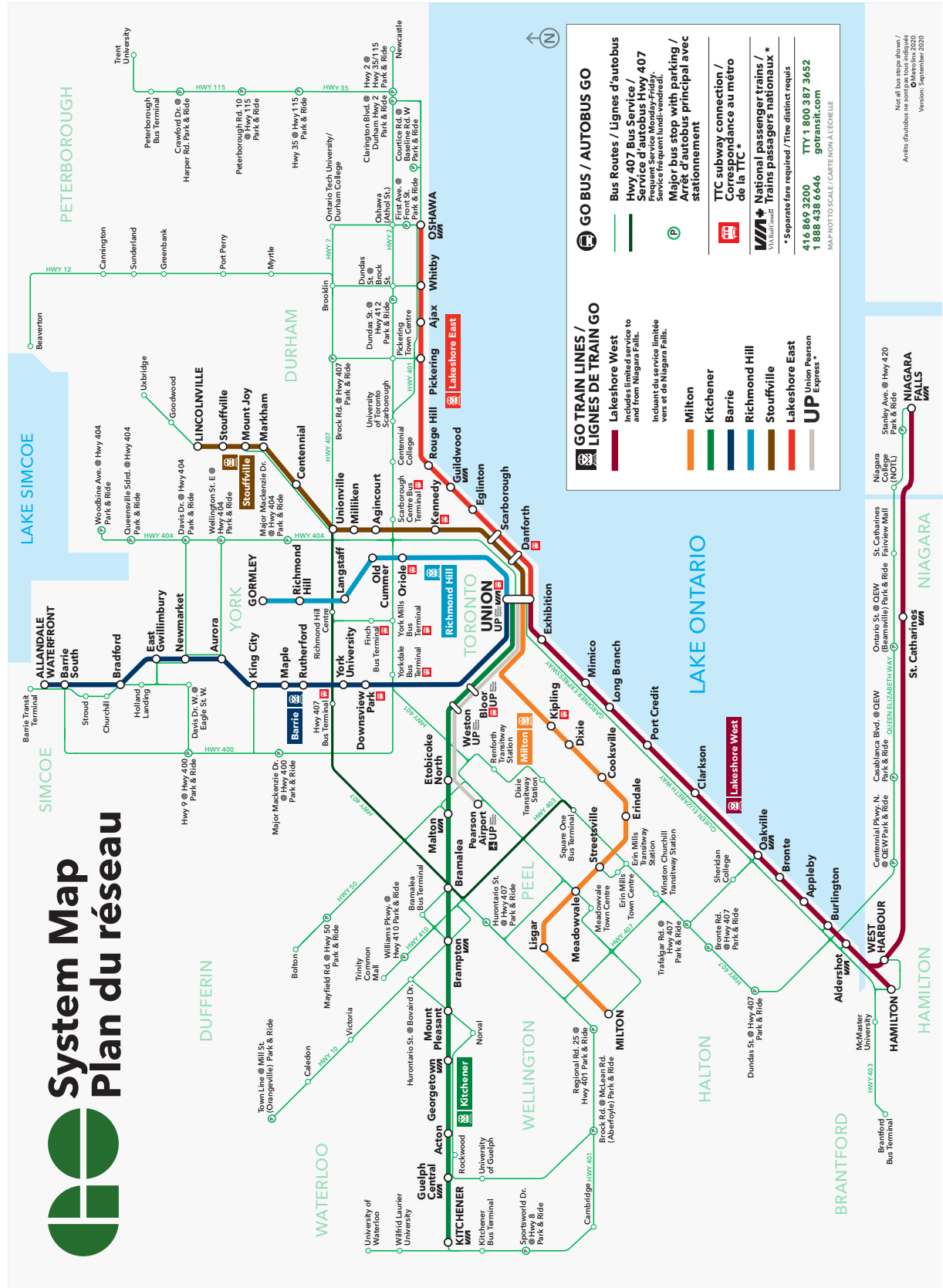
Description	IT Systems and/or Tasks
Information	
 <p>A Metrolinx customer can find information about train and bus schedules, as well as alerts to changes online, or via website, cell phone or other mobile device.</p>	<ul style="list-style-type: none"> • Customer Communication Management System (email, social media text alerts) • GO Transit Website • UP Express Website • Service Guarantee system (RTSI) • GO Tracker • Next bus arrival information • Interactive Voice Response (GO/UP Express/PRESTO)
Stations and Stops	
 <p>Stations have a number of safety and other systems in place. After travelling to a station, customers can check the platform number and schedules on digital signs.</p>	<ul style="list-style-type: none"> • Station Service Status • Station Service Status (digital signs) • CCTV cameras
Fare Payment	
 <p>Customers use PRESTO smart cards tap machines or purchase tickets using the ticket vending machines or from the ticket counter before or at the time of boarding.</p>	<ul style="list-style-type: none"> • Green tap machines • Ticket Vending Machines • Driver Control Unit (ticket printing on buses) • UPEXpress.com • GOTransit.com • PRESTOcard.ca • Card Query (balance check) device • Self-Serve Reload Machines (SSRM)
Transit Type	
 <p>IT Systems run in the background for various purposes like navigation, communication, tracking, live-traffic updates, safety and security monitoring.</p>  <p>Metrolinx shares railway tracks with CN and CP rail, and communicates for scheduling and track allotment.</p>	<ul style="list-style-type: none"> • Trains scheduled with Trip Manager • Trains tracked via Automatic Train Locating system/Trip Movement Manager (ATLS/TMM) • Buses scheduled using Giro-Hastus • Buses use Computer-Aided Dispatch and Automatic Vehicle Location (CAD/AVL) • Trackside “bungalows” (related technology components) • Bus CCTV Cameras • Signals, Switches, Crossings • Emergency Mass Notification System (EMNS) • TrainTrac • Revenue protection activities (GTECHNA)
Arrival at Destination	
 <p>At busy destinations such as Union Station, trains are allocated tracks and buses are allocated bays.</p> <p>Customers tap off using PRESTO if required.</p>	<ul style="list-style-type: none"> • Electronic Track Allotment (for managing high rail traffic, in Trip Manager) • Signals, Switches • Station Service Status (digital signs) • Green tap machines • CCTV on Union Station Platforms

Figure 3: GO Transit Service Map, as of November 2019

Source: Metrolinx



3. **Milton:** Between Union Station and Milton consisting of eight stations covering communities such as Mississauga and Milton.
4. **Kitchener:** Between Union Station and Kitchener consisting of 11 train stations covering communities such as Etobicoke, Brampton and Guelph and Acton.
5. **Barrie:** Between Union Station and Barrie consisting of 10 train stations covering communities such as King City, Newmarket and Bradford.
6. **Richmond Hill:** Between Union station and Gormley Station consisting of five stations covering communities such as Richmond Hill.
7. **Stouffville:** Between Union Station and Lincolnville Station consisting of nine train stations covering communities such as Scarborough, Markham and Stouffville.
8. **UP Express:** Between Union Station and Lester B. Pearson International Airport consisting of two stations in Toronto and the station at the airport, located in Mississauga.

The GO Bus network provides regional bus services across most of the Greater Golden Horseshoe Area (GGH), from early in the morning to late at night. Regional bus routes connect customers to destinations within the GO Transit service area that are not served by the GO Rail network, ranging from small communities to major destinations such as colleges, universities, business parks and shopping centres. GO buses may be offered during GO and UP rail service disruptions to minimize the impacts to customers and to bridge services during construction along the rail corridor. The GO Bus service area includes:

1. **Cities:** Barrie, Brantford, Guelph, Hamilton, Orillia, Peterborough and Toronto.
2. **Counties:** Brant, Dufferin, Peterborough, Simcoe and Wellington.
3. **Regional Municipalities:** Durham, Halton, Niagara, Peel, Waterloo and York.

2.2.1 Service Guarantee Program

Through Metrolinx's Service Guarantee Program, established in 2012, customers are eligible for a refund if their GO trains are delayed by 15 minutes or more due to factors within Metrolinx's control, such as signal failures, operational and mechanical issues, equipment failures and train traffic. For eligible trips, customers are refunded the fare through their PRESTO cards by applying through the GO Transit website or in person at one of GO stations. Customers who travel using papers ticket can request refunds or fare voucher at any GO station. Over the past five years this has resulted in about 900,000 customers receiving refunds worth a total of \$6.5 million, of which approximately \$450,000 attributed to IT incidents.

2.3 PRESTO

Customers can buy PRESTO cards online using the PRESTO website (prestocard.ca), in person at customer service windows at GO or local transit stations, ticket vending machines at GO stations and at retail locations such as Shoppers Drug Marts. While cards purchased in person are activated and ready to use, cards purchased using the PRESTO website must be activated via phone or the PRESTO website.

Customers can use PRESTO cards to pay for transit services by using the green tap machines at transit stations or on buses. They also have the option to load funds or check balances using PRESTO machines at stations, or online via the PRESTO website and mobile application. Customers can set PRESTO cards to load funds automatically once the card balance reaches a set threshold. Funds are added to PRESTO cards immediately if a customer chooses to load a card manually at a PRESTO payment machine at a station. In addition, funds can be loaded at transit agency customer service outlets as well as at third-party retailers. However, funds may take up to 24 hours to load

if a customer chooses to purchase PRESTO funds through the website.

PRESTO's website, prestocard.ca, enables customers to manage their PRESTO cards. It allows customers to purchase a card, as well as activate, register, check balance, view transaction history, load funds and report a problem with a card if it is lost or damaged. Customers can also set up and manage the autoload function, choose to receive alerts when they have a low balance, and receive email receipts for fare purchases. In addition to the website, PRESTO also has a mobile application for smartphones. The PRESTO mobile application has additional features, such as enabling customers to load funds using a credit card for payment. The PRESTO mobile application also allows customers to load funds instantly with tap functionality-enabled phones.

2.3.1 PRESTO Devices

PRESTO has seven different devices installed or in use by staff at train and bus stations to perform various tasks. Refer to **Appendix 1** for detailed breakdown of device descriptions, number of devices, costs and vendors responsible to provide support.

1. Station Fare Transaction Processors (SFTP), the green tap machines, are used to collect fares from customers. For fare payments, customers tap their PRESTO cards on a green tap machine before boarding a train.
2. Card Query Devices (CQD), the yellow tap machines, are used to check card balances and activate new PRESTO cards.
3. Driver Control Units (DCU) are tap machines installed on GO buses to collect fares from customers.
4. Ticket Vending Machines (TVM) at GO stations are used to purchase tickets and PRESTO fare cards, as well as to re-load fare cards and check balances.
5. Self-Serve Reload Machines (SSRM) at GO stations are used to re-load or add money to PRESTO cards.

6. Inspection Devices (Hand-held Card Readers) are used by fare ticket inspectors on GO and UP Express trains.
7. Station Point of Sale Machines (SPOS) are used by GO Station attendants to issue tickets.

2.3.2 Key PRESTO Vendors

Two PRESTO devices used mainly by GO Transit and UP Express customers on a regular basis are the green tap machines and ticket vending machines. These two devices are used to pay transit fares, buy transit tickets, purchase PRESTO cards and load funds to PRESTO cards.

PRESTO's IT systems have been managed and operated by third party vendor Accenture since 2006. Accenture also manages and operates PRESTO's website (prestocard.ca), mobile application, and contact centre. Accenture's responsibilities also include the development and maintenance of PRESTO's IT systems, website, and mobile application. PRESTO's ticket vending machines were procured by Metrolinx through another vendor, Flowbird. Flowbird is responsible for the development and maintenance of the ticket vending machines' IT system, providing hardware replacement parts, and providing technical support to resolve IT incidents.

Metrolinx's IT department is responsible for performing quality assurance testing for any new PRESTO devices before they are installed at GO and UP Express stations. They also perform IT security testing, such as penetration testing, and provide Internet connectivity. In addition, the Metrolinx IT department is identified in the contracts with Accenture and Flowbird as the first level of support for PRESTO device-related IT incidents, such as Internet connectivity and power failures, as well as mechanical issues such as paper and coin jams. IT incidents that require second-level support, such as software issues causing system-wide failures or outages, or hardware requiring replacement are escalated to the respective vendors, Accenture or Flowbird.

2.4 IT Contractors

Metrolinx has a contractor management process for fulfilling its IT staffing requirements for day-to-day operations and services, and IT projects. The Resource Coordination team is responsible for IT staffing. When additional resources are required, a request is made to the team, and the team identifies a new IT contractor who is put forward to the requesting manager for approval.

Metrolinx has a Request to Qualify and Quote (RQQ) process that is used to purchase IT consulting services, including IT contractors. A minimum of three vendors from a list of approved vendors are approached for assignments with a value of up to \$99,999. For assignments with a value of \$100,000 or more, a publicly advertised tender is required. When a tender is used, an evaluation committee is established to assess, evaluate and score vendor submissions against evaluation criteria. The approved vendors must present appropriate candidates to Metrolinx, set up interviews, conduct background checks, as well as provide information such as hourly billing rate, and contract start and end dates.

2.5 Cybersecurity

Metrolinx relies on IT systems to deliver critical transit operations such as rail signals, track switching, scheduling, safety (platform and track safety) and customer communications, as well as collecting and storing customer information. Cybersecurity is a critical function required to protect organizations from cyberattacks, privacy breaches, reputational damage, and the destruction of critical information and infrastructure. There has been an increase in the number of transportation industry cyberattacks globally, such as the December 2015 cyberattack against British Columbia's transit agency that resulted in the shutdown of its trip planning and call centre IT systems for two days. The San Francisco and Sacramento and transit agencies were also attacked in November 2016 and November 2017, respectively. San Francisco's fare payment

systems malfunctioned for two days and Sacramento's bus scheduling systems were disrupted.

3.0 Audit Objective and Scope

Our audit objective was to assess whether Metrolinx has effective IT systems and processes in place so that:

- IT systems for critical transit operations such as rail signals and switches, scheduling and dispatch, and safety and communications are managed efficiently, operating effectively, and are secure, reliable and protected against cybersecurity threats;
- resources are deployed efficiently and effectively to carry out IT activities necessary for operations, including the appropriate usage and oversight of IT contractors; and
- all IT assets, software, and licences are acquired in an efficient and economical manner, and corrective action is taken to remedy IT-related service disruptions on a timely basis.

In planning for our work, we identified the audit criteria we would use to address our audit objective (see **Appendix 2**). These criteria were established based on a review of applicable legislation, policies and procedures, internal and external studies, and best practices. Senior management at Metrolinx reviewed and agreed with the suitability of our audit objective and related criteria.

We conducted our audit between January 2020 and September 2020. We obtained written representation from management that, effective November 16, 2020, they had provided us with all the information they were aware of that could significantly affect the findings or the conclusion of this report.

We conducted audit work primarily at Metrolinx's Toronto office which is responsible for the operation and maintenance of Metrolinx information systems and technology infrastructure, and for managing technology vendors.

We also interviewed staff at the Network Operations Centre (NOC) that operates and manage IT systems related to train tracks, rail signals, switches and engine data, and also monitors all customer communications and incidents.

As well, we also interviewed senior and front-line staff and reviewed documents. We visited the Metrolinx locomotive rail yard site in Etobicoke to inspect IT systems and safety controls on trains. As part of the visit, we were provided with a demonstration of safety equipment such as the emergency passenger alarm assist, smoke/heat detectors, the activity-based event recorder that records and stores data from various devices on board, and intruder alarm controls.

In addition, we interviewed Field Service Technicians about IT-related incidents with Metrolinx IT systems at GO stations, such as ticket vending machines and PRESTO fare payment devices, to review root causes behind IT-related incidents and resolution processes.

We also visited the PRESTO test lab facility in Toronto used by Metrolinx's quality assurance staff to test PRESTO fare payment devices such as green tap machines, ticket vending machines, point-of-sale and fare inspection devices. The lab facility lets Metrolinx test the devices in a safe and secure environment before they are deployed on GO Transit's fleet and at stations.

We assessed IT systems that deliver critical transit operations, such as rail signals, track switching, scheduling, and transit safety and cybersecurity operations at Metrolinx. We also assessed whether access to IT systems responsible for operating transit services (such as rail signals, switches, scheduling and customer communications) is restricted based on staff job function, and whether IT systems have strong disaster recovery plans to make them available in an event of an outage or disaster.

We reviewed Metrolinx's governance and oversight processes for IT vendors and contractors. We also assessed procurement practices for staffing vendors, and the contractors that account for more than half of Metrolinx's IT staff. In addition, we

reviewed the contractor procurement process (such as interviews, reporting structure, timesheets, billing hours charged and performance reviews).

We also examined key IT projects implemented over the last five years for project management requirements, the use of standard and consistent project management frameworks, potential delays and under/over estimation of project costs.

We conducted our work and reported on the results of our examination in accordance with the applicable Canadian Standards on Assurance Engagements—Direct Engagements issued by the Auditing and Assurance Standards Board of the Chartered Professional Accountants of Canada. This included obtaining a reasonable level of assurance.

The Office of the Auditor General of Ontario applies the Canadian Standard on Quality Control and, as a result, maintains a comprehensive quality-control system that includes documented policies and procedures with respect to compliance with rules of professional conduct, professional standards and applicable legal and regulatory requirements.

We have complied with the independence and other ethical requirements of the Code of Professional Conduct of the Chartered Professional Accountants of Ontario, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

4.0 Detailed Audit Observations

4.1 IT Issues Affecting Rail Operations Result in Revenue Loss

Information technology (IT) is critical to Metrolinx's operations. Information systems such as the rail traffic control system, and train signal and track allotment systems that manage signals and rail crossings rely heavily upon IT and related technology components such as signals and switches to

efficiently manage and operate transit services. IT incidents with these systems and technologies can result in significant delays and cancellations which can in turn result in the refund of fares for delayed and cancelled trains and inconvenience customers.

4.1.1 Frequent IT Issues Result in Delays and Cancellations

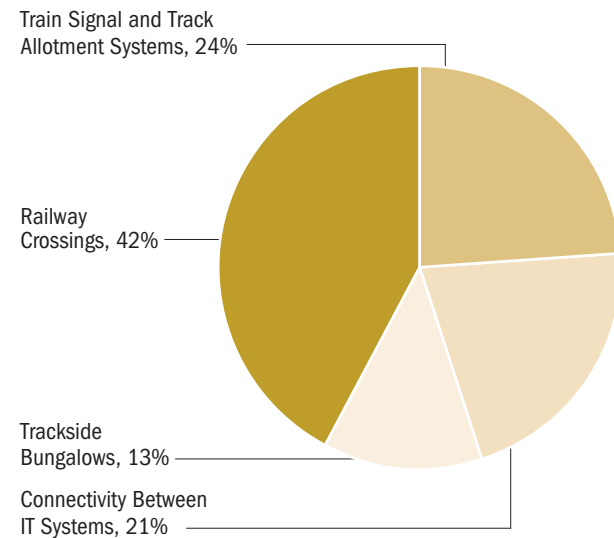
Trains can be delayed or cancelled for reasons rooted in Metrolinx's IT systems, such as signal or rail crossing control failure. We found that IT systems and related technology components (see **Section 2.2**) for critical transit operations have experienced frequent incidents, such as network connectivity issues, system malfunctions and software and hardware issues resulting in train delays and cancellations.

We noted that from January 2015 to January 2020, there were nearly 4,500 GO train and UP Express delays and cancellations resulting from IT software and hardware issues, which account for over 10% of all delays and cancellations. Twenty per cent of these 4,500 IT-related train delays and cancellations were eligible for Metrolinx's Service Guarantee Program. These significantly delayed and cancelled trips impacted over 300,000 customers and resulted in approximately \$450,000 in fare refunds, a revenue loss. See **Section 4.1.2** for the impact of these 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 resolve them, are not recorded. These details are necessary for analysis and assessment to ensure that similar issues do not regularly occur. Refer to **Section 4.2** of our 2020 audit of Metrolinx Operations and Governance for further information regarding all incidents causing train delays and cancellations.

We reviewed these IT incidents to determine the root causes that resulted in train delays and cancellations and categorized these incidents into four broad categories—rail crossings, train signal

Figure 4: Trains Affected by IT Incidents by Category,* January 2015–January 2020

Source of data: Metrolinx



* OAGO has grouped IT incidents in categories for analysis.

and track allotment systems, connectivity between IT systems and trackside “bungalows.” See **Figure 4** for a breakdown of four broad categories of the 4,500 train delays and cancellations from January 2015 to January 2020.

Specifically, we noted the following for each category of incidents:

1. **Rail Crossings (42% of all IT-related train delays and cancellations)** – Where roads cross rail lines, rail crossing barriers are activated to allow trains to pass safely. We noted that IT incidents were caused by both IT software and hardware issues such as sensor issue within the railway crossing or defective hardware that failed since it reached its life expectancy. In addition, IT software issues such as application errors caused due to incorrect settings within the software had to be correct and reinstalled have caused rail crossing equipment to fail. When rail crossings fail, rail crews must physically stop traffic and protect the crossing to ensure that there are no vehicles or pedestrians on the tracks before the train can proceed to

the next stop, ultimately causing significant delays. For example, on November 12, 2019, we noted that 48 trains were affected by three defective rail crossing systems affecting 38 Lakeshore East GO train line and 10 resultant delays on other corridors. In these cases, sensor issues in the rail crossings' control equipment required inspections for faulty or loose cables.

2. **Train Signal and Track Allotment Systems (24% of all IT-related train delays and cancellations)** – Signal and track allotment systems ensure safe movement of trains by monitoring train tracks, and by coordinating rail traffic and signals. IT incidents such as system hardware failure due to performance issues, and software failure due to outdated system patches with these IT systems resulted in delays and cancellations of trains. For example, in May 2017, a system outage was caused when a connection between systems timed out, as system software was no longer able to communicate necessary data about train movements to other IT systems. This issue resulted in 19 train delays and cancellations on four GO train lines.
3. **Connectivity between IT Systems (21% of all IT-related train delays and cancellations)** – Connectivity issues or malfunctions in systems that allow systems to communicate with one another impacted train operations and caused delays. We noted that IT incidents such as communication failures due to faulty cables or network communication cards requiring replacement resulted in delays and cancellations. For example, a major connectivity issue between the Network Operations Centre and train signals hardware occurred when there was a hardware change that affected compatibility between two pieces of hardware. This issue resulted in the delay or cancellation of all UP Express trains for six hours on February 14, 2020.

4. **Trackside “Bungalows” (13% of all IT-related train delays and cancellations)** – A bungalow is a building structure usually located beside train tracks. The bungalow contains IT equipment, both hardware and software, used to send information along the train lines to rail traffic and tracking systems, as well as signal and rail crossing systems. We noted IT software and hardware issues resulted in train delays and cancellations when train signal and track allotment systems were unable to communicate with the rail crossings and signals. For example, in October 2019, nine trains were delayed or cancelled due to a hardware failure in a bungalow. A defective communication card used for the connection between the rail crossing and signals failed and was subsequently replaced with a new unit and then configured and calibrated for service.

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.

RESPONSE FROM METROLINX

Metrolinx accepts the Auditor General's recommendation. Metrolinx is in the process of establishing a business case for a root-cause analytical tool, which will help Metrolinx to record and perform a root-cause analysis. In order to achieve this, Metrolinx-Operations has recently established a centralized and dedicated performance team and hired a performance director in November 2020. The business case will be presented to the Board within the next six months. Subject to business case approval, the

root-cause analytical tool will be implemented to perform root-cause analysis.

4.1.2 Delays and Cancellations Result in Revenue Losses from Service Guarantee Program

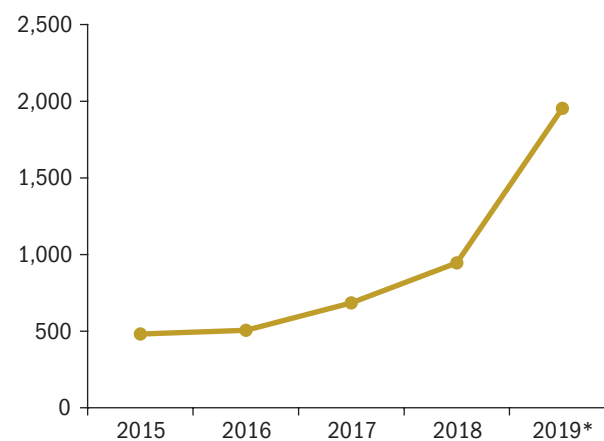
Metrolinx has a Service Guarantee Program to refund customers their fares when GO trains are delayed by 15 minutes or more or boarded train trips cancelled after they departed due to factors within Metrolinx's control (such as signal or other equipment failures, and train traffic). However, customers are not eligible if GO trains are delayed or cancelled due to factors outside of Metrolinx's control (such as weather, trespassers on train tracks, onboard emergencies and fatality investigations). Customers can verify their eligibility and apply for refunds at GO Transit's website (GOtransit.com) by entering the date of the trip, departure station, arrival station, scheduled train departure time and their PRESTO card number. If the trip is eligible for a refund, fares for the trip are refunded back to customers through their PRESTO cards. Customers who travel using tickets can request refunds at any GO station and will receive GO fare vouchers. Refer to **Section 4.4** of our 2020 audit of Metrolinx Operations and Governance for further information regarding the Service Guarantee Program.

We noted an upward trend in the number of train delays and cancellations due to IT related software and hardware issues in the past five years. Since 2015, the number of train delays and cancellations due to IT incidents have increased by more than three times. See **Figure 5** for the trend of IT-related train delays and cancellations in the past five years.

Of the 4,500 delays and cancellations resulting from IT incidents, we noted approximately 80% were delayed by less than 15 minutes, 20% of trains were delayed by 15 minutes or more, and boarded train trips that were cancelled after they departed the station. We noted that over 300,000 customers were eligible for a refund through Metrolinx's

Figure 5: Trains Delayed and Cancelled due to IT Incidents, January 2015–January 2020

Prepared by the Office of the Auditor General of Ontario



* 2019 includes numbers for January 2020 (244 train delays and cancellation in the month of January 2020).

Service Guarantee Program as their train was either cancelled or delayed by 15 minutes or more. The refunds issued through this program for the 4,500 delays and cancellations resulted in approximately \$450,000 in refunds—a revenue loss.

We noted that on November 12, 2019, 18 GO trains on the Lakeshore East line were delayed by 15 minutes or more, and another six trains were cancelled due to a rail crossing hardware failure that affected all rail lines excluding Kitchener and Barrie rail lines. This incident impacted over 13,000 customers and resulted in a refund of approximately \$19,000 to 2,500 customers who applied to the Service Guarantee Program. If all customers who were eligible had applied to the program, Metrolinx would have had to pay out approximately \$80,000 in additional refunds.

Customers Are Not Refunded Automatically with the Service Guarantee Program, Even Though the Capability Exists in PRESTO

Although Metrolinx has 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. We noted that in the last five years only 23% (72,000) of about 300,000 eligible customers applied for the Service Guarantee Program for trips impacted by IT incidents, resulting in approximately \$450,000 in refunds. If all eligible customers were refunded automatically, the total cost of the refund would have been approximately up to a maximum of \$2.2 million, using an average fare of \$9, based on maximum ridership on affected trips and fare revenue for 2018/19.

Although customers have made inquiries about automatic refunds, Metrolinx has not implemented an automatic refund process. When customers asked Metrolinx why automatic refunds had not been implemented, they indicated that many customers made last-minute decisions to take alternate routes. However, based on our research, for most GO train services there are no alternate routes provided by GO Transit. Customers may be accommodated on bus replacement services, or during major incidents Metrolinx may enact the TTC Protocol whereby customers may ride the TTC using their GO fare. Some customers must may choose to pay for alternative local transit services or other means of transportation to get to their destinations when trains are cancelled; when trains are delayed, customers who do not find alternative transportation simply wait for their trains to proceed.

Fare Refund Program Is Inconsistent between GO Train and UP Express

Metrolinx's Service Guarantee Program is delivered inconsistently for customers on GO trains and UP Express. We noted that GO Transit's program offers 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. UP Express customers may also be eligible for additional compensation such as airline rebooking fees or complimentary future trip vouchers. We found that before the Service Guarantee Program eligibility threshold for refunds on GO trains was set to 45 minutes or

more, the threshold was changed to 15 minutes or more in November 2012 when the Service Guarantee Program launched. When UP Express was launched in June 2015, it followed the original refund practice of compensating customers for eligible trips when trains were cancelled or delayed by 45 minutes or more.

We also found that UP Express customers are able to apply for a refund within 30 days of their trip, but eligible customers of GO Transit have to apply for a refund within seven days. The UP Express was built with the latest technology for signalling systems. In addition, it has dedicated tracks, and therefore does not contend with competing rail traffic from Canadian National (CN), Canadian Pacific (CP) and VIA Rail, like some GO train services, which would reduce any additional chance of delays or cancellations.

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; and
- assess the feasibility of establishing a consistent Service Guarantee Program for GO Transit and UP Express customers.

RESPONSE FROM METROLINX

Metrolinx appreciates the Auditor General's recommendations. Metrolinx is currently performing a comprehensive review of the Service Guarantee Program and its application to GO Transit and UP Express. The policy review will evaluate the business objectives and intent of the program and provide recommendations for enhancing the Service Guarantee

Program to improve customer experience and business outcomes.

The review will assess the cost and benefits of harmonizing the Service Guarantee Program for GO and UP Express, considering the unique customer value proposition that both services provide.

Once the program review is complete, Metrolinx will complete a business case to assess the feasibility of automating refunds to PRESTO customers for eligible service delays and cancellations under the Service Guarantee Program. The review will consider Metrolinx's expanding payment channels, including e-ticketing and open payment. The evaluation will consider customer experience, cost, benefit, risk and technical feasibility, and will culminate in a recommendation that is well supported by data. Metrolinx would not be able to issue automatic refunds for paper tickets.

4.2 Metrolinx Management of PRESTO Operations Requires Improvement

Metrolinx's PRESTO fare payment system has required software and hardware support from vendors to develop and maintain its service. Under contract to Metrolinx since 2006, Accenture developed the PRESTO fare payment system, installed its fare payment software to devices, and supported the its customer website, mobile application and contact centre. Ticket vending machines are key devices with integrated PRESTO software. These devices were developed and have been maintained since 2010 by Flowbird, an external vendor. Refer to **Section 2.3.2** for vendor roles and responsibilities for PRESTO operations.

According to the contracts between Metrolinx and both Accenture and Flowbird, IT incidents with PRESTO devices that are operating within GO Transit and UP Express are initially reviewed by Metrolinx's field service technicians from the IT department for troubleshooting and resolution.

IT incidents, such as software issues and hardware replacement, that require additional support are escalated to either Accenture for green tap machines or Flowbird for Ticket Vending Machines for resolution.

4.2.1 IT Incidents Affect PRESTO Devices and Cards

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 vast majority of the 45,000 incidents did not have a significant impact on Metrolinx's customers, as stations are equipped with more than one fare device of similar type. Nevertheless, customers' experience was impacted, as they had to find a working fare device in order to pay for their fare. See **Figure 6** for the 45,000 PRESTO software and hardware issues by device type.

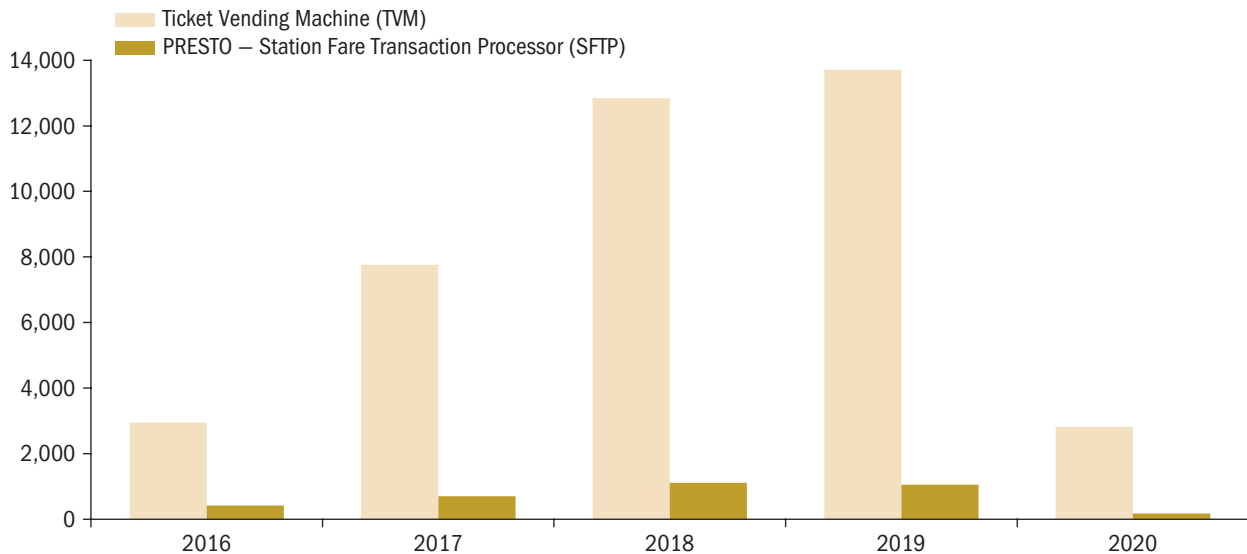
The two devices that have the highest number of IT incidents and significant impacts on customers are Ticket Vending Machines and Station Fare Transaction Processors, the green tap machines found at stations.

Ticket Vending Machines

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

Figure 6: PRESTO IT Incidents by PRESTO Device Types, February 2016–March 2020

Source of data: Metrolinx



hardware issues where machines were unable to dispense tickets due to mechanical issues as a result of aging devices. See **Appendix 1**. Other IT incidents included, for example, display screen malfunctions in older devices and poorly written software code causing 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. Specifically:

- About 12,000 IT incidents were caused by connection time-outs that left machines able to perform only limited functions, or unable to take credit and debit cards to pay for tickets; in these cases, customers were left with cash as the only option to buy from a functioning nearby machine or from a station attendant, resulting in inconvenience.
- An additional 9,000 IT hardware incidents were resulted in ticket printing issues, such as tickets not dispensing after a customer has paid the fare, blank tickets being dispensed, insufficient paper due to printer sensor failures, low printer ink cartridges and paper jam issues; these incidents required customers

to contact customer service, causing them inconvenience.

Some examples that impacted customers as a result of IT incidents involving Ticket Vending Machines include the following:

- From May 31, 2018, to November 8, 2019, Ticket Vending Machines at GO and UP Express stations were occasionally out of service when some customers tried to use them for purchasing tickets or loading PRESTO cards. We noted that this occurred due to poorly written software code used to operate the machines. The incident was resolved when the vendor upgraded the software to a newer version.
- Ticket Vending Machines at GO stations were unavailable for two hours and 15 minutes on Friday, December 29, 2017, due to an IT system change that was implemented a day earlier than planned. As a result, the machines were unable to retrieve updated data files with purchase information such as dates and times tickets were purchased. This resulted in about 200 machines being unavailable for ticket purchases, and PRESTO card purchase and load functions.

- All Ticket Vending Machines at GO and UP Express stations experienced software issues that affected the interface between Ticket Vending Machines and PRESTO IT systems from April 25, 2018, to July 10, 2018. Ticket Vending Machines shut down and restarted on occasion when some customers tried to perform any operations related to PRESTO, resulting in customers' inability to load funds to PRESTO cards at that specific device.

Station Fare Transaction Processors (Green Tap Machines)

PRESTO Station Fare Transaction Processors (green tap machines) enable fare payment. Any problems with these devices at a high-traffic GO station (such as Union Station) may result in a number of inconvenienced customers. In the last four years, from February 2016 to March 2020 (the most current data available), we noted over 3,500 IT incidents with the green tap machines. We also noted that Metrolinx does not currently analyze and assess the loss of revenue due to tap machine outages.

We analyzed these incidents and noted that over half related to connection time-out issues, hardware issues and software issues. Specifically:

- About 800 IT incidents related to connection time-out issues between the green tap machines and the fare payment back-end IT system that processes transit fares and loads funds, resulting in customer inconvenience when they are required to find a working green tap machine for payment.
- About 700 IT incidents occurred due to hardware failures such as faulty displays, card readers, wiring and replacement parts which had reached the end of their useful lives required replacement.
- About 400 IT incidents related to software issues in green tap machines that rendered them unavailable. These incidents were caused by incorrect updates sent to the

machines at the end of the day. As a result, Metrolinx IT staff were required to restart the devices to ensure the correct files were downloaded, and the machines could be returned to service.

Some customer impacts from IT incidents with green tap machines include the following:

- All PRESTO fare payment devices at Union Station were unavailable for approximately two hours on February 25, 2019. The devices were inoperable and unavailable for fare payment while the system updated. This impacted about 35,000 customers who were unable to pay their fares. By obtaining average ridership data for the period of the incident, and multiplying it by an average fare of \$9, we calculated that approximately \$315,000 in fare revenue could have been lost due to this outage.
- About 29,000 PRESTO customers were unable to pay their fares on all green tap machines on November 16, 2017, due to a website configuration error that caused a number of PRESTO cards to be wrongly blocked. By obtaining average ridership data for the period of the incident, and multiplying it by an average fare of \$9, we calculated that approximately \$260,000 in fare revenue could have been lost due to this outage.

PRESTO Cards

Customers use PRESTO cards to pay their fares by tapping on fare payment devices located at GO train and UP Express stations, and on GO buses and local transit services. Based on our review, we noted software issues with the PRESTO IT system that resulted in customers being double-charged when they chose to auto-load their PRESTO cards, and a small number of customers being charged adult fares instead of the appropriate reduced fares for seniors and students.

We noted that Metrolinx became aware about these incidents when customers contacted Metrolinx

regarding overcharges. Metrolinx then verified the overcharges and refunded the differences to customers who contacted Metrolinx. In addition, we noted that PRESTO cards sometimes required up to 24 hours to reflect the correct balance, resulting in fare payment devices reading insufficient funds when customers tapped their cards, even though they had recently loaded funds to their cards.

We noted there were over 6,700 PRESTO card-related IT incidents from January 2016 to March 2020 (the most current data available). See **Figure 7** for a breakdown of incidents and related issues that impacted customers. The following are two examples of incidents that occurred:

- About 940 PRESTO customers were charged twice for their monthly passes on November 25, 2016 due to an automated sales order that was processed twice after the previous automated order had failed. In addition to the direct impact to customers who were charged twice, the PRESTO contact centre received call volumes that were 18% higher, which impacted their overall service levels responding to all customer calls.
- About 3,000 customers were not able to add funds to their PRESTO cards for three hours on July 5, 2017. This issue was caused when a payment service provider vendor (Moneris) applied a change to its software that prevented customers from purchasing tickets on the website and PRESTO devices. We noted that according to Metrolinx documents, both Accenture and Metrolinx must approve changes as per Metrolinx's Change Management process. However, this change was not approved by either Accenture or Metrolinx. Again, this issue caused not only direct impacts to customers, but also a 6% increase in the total call volume to the PRESTO contact centre which impacted service levels responding to all customer callers.

In addition, we noted that Metrolinx did not always record details such as the root causes of these low priority incidents, and the steps taken to resolve them.

Figure 7: PRESTO Card Incidents, January 2016–March 2020

Prepared by the Office of the Auditor General of Ontario using Metrolinx data

Category	Issues Experienced	2016	2017	2018	2019	2020 (Jan–Mar)	# of Total Issues
Add Fund	• Card funds not added within 24 hours	0	159	755	1,569	679	3,162
Card Balance	• Card balance lost after buying monthly pass • Unable to load funds • Customer balance not updating as per transit usage • Unable to transfer card balance	0	37	166	537	95	835
Autoload	• Duplicate transactions • Charged multiple times • Delayed transactions	213	238	429	604	168	1,652
Concession	• Adults charged student fares • Students and seniors charged adult fares • Monthly pass concession not applied, instead charging full fare amount	64	71	126	640	201	1,102
Total		277	505	1,476	3,350	1,143	6,751

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;
- establishing a device lifecycle plan to ensure replacement of old and ineffective devices in a timely manner;
- improving the existing Change Management process to detect exceptions such as unplanned changes, duplicate and delayed transactions; and
- 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.

RESPONSE FROM METROLINX

Metrolinx appreciates the Auditor General's observations and will undertake the following actions to address the recommendations:

- While Metrolinx currently completes root-cause analysis for critical and high-severity incidents (type 1 and 2), an assessment will be performed to determine the benefits of completing root-cause analysis for lower priority incidents (type 3 and 4). Metrolinx will also complete an assessment of incident document management practices to improve documentation supporting incidents.
- Metrolinx is in the process of establishing an asset management plan that articulates the required lifecycle activities to maintain its assets in a state of good repair and ensure business continuity. Metrolinx recently implemented an asset management database

and has begun importing assets into its inventory, to be completed by October 2021.

- The change advisory board, which meets on a regular weekly basis, will review all changes, including unplanned changes. Metrolinx will continue to work with its vendors and will commit to conducting a process review to ensure alignment of expectations and accountabilities.
- Metrolinx will develop 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.

4.2.2 Contract Terms Do Not Enable Metrolinx to Effectively Monitor and Hold Vendors Accountable for Poor Performance

PRESTO Cards and Fare Payment Devices (Vendor – Accenture)

Metrolinx has not established an effective process to monitor Accenture's performance targets for delivering PRESTO operations as identified in their service level agreement. According to the agreement, Accenture is required to provide monthly reports with detailed summaries of performance targets achieved for operations such as incident resolution for PRESTO devices, card-related issues and website availability.

Based on our review of Accenture's performance reports, we noted that performance targets are reported collectively, with performance information for all three priority levels (Priority 1, Priority 2 and Priority 3) 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. For example, Priority 1 incidents must be resolved within three hours, while Priority 3 incidents must be resolved within five business days. By reporting on all priority levels together, Metrolinx does not receive the information necessary to know whether Accenture is

Figure 8: Number of Incidents by Priority that Exceeded the Resolution Time, January 2015–March 2020

Prepared by the Office of the Auditor General of Ontario using Metrolinx data

Priority Levels	Description	Expected Resolution Time	# of Incidents	Exceeded Resolution Time
P1	Severe business disruption affecting System Availability, Customers and Financial Integrity.	3 hours	6	4
P2	Major business disruption affecting system functionality and stability	24 hours	114	44
P3	Minor business disruption affecting System Functionality (non-critical)	5 business days	29,227	4,798
P4	Minor disruption standard and Ad Hoc work requests	Reasonable effort	3,113	n/a
Total			32,460	4,846

meeting its targets for resolving incidents according to priority level. See **Figure 8** for a detailed description of the different priority levels, and number of IT incidents that exceeded the required resolution time. We also noted that the contract between Metrolinx and Accenture was amended in 2020 to include a penalty clause to hold Accenture accountable for poor performance. However, we noted that the recently added clause does not provide detailed penalty information to determine the amount of penalties to be imposed in the event that Accenture misses a performance target.

As well, Metrolinx does not systematically analyze the information that is reported by Accenture to assess if targets are being met by individual priority level. We reviewed the monthly performance reports from Accenture for the last five years in their consolidated form, for which they did not report a missed target. After analyzing the information reported for the period of January 2015 to March 2020, we found that Accenture had actually missed Priority 1 and Priority 2 performance targets in 48 of 120 (40%) incidents. Priority 3 targets were missed approximately 4,800 out of 29,000 (16.5%) of the time.

We also found that Accenture miscategorized Priority 1 incidents as Priority 2 in 15 instances. By doing so, it provided more time (an additional 21 hours) to resolve these incidents.

In addition, we found that IT incidents are broken down into four categories—Priority 1, 2, 3 and 4—while the agreement requires only Priority 1, 2, and 3 incidents to be reported to Metrolinx. We noted that Priority 4 incidents reported, such as delayed transactions and customers being charged incorrect fares, are critical for Metrolinx and should have been included in required reporting. These incidents help to provide detailed insights into IT incidents that impact customers and Metrolinx operations. We also noted that Priority 3 incidents are sometime misclassified as Priority 4 incidents without an expected resolution time.

Ticket Vending Machines (Vendor – Flowbird)

Ticket Vending Machines at GO and UP Express stations are used by customers to purchase paper tickets and load PRESTO cards. These machines were procured by Metrolinx from a vendor, Flowbird, in 2010. In the past five years from 2015/16 to 2019/20, Metrolinx has paid approximately \$4 million for maintenance and support of these machines.

As noted in **Section 4.2.1**, most PRESTO IT incidents are related to Ticket Vending Machines. We found that Metrolinx does not evaluate Flowbird's performance by assessing if the vendor has resolved the IT incidents according to the timelines in the service level agreement.

According to the service level agreement between Metrolinx and Flowbird, IT incidents

are categorized as Priority 1, 2 and 3. Priority 1 incidents must be resolved within six to 10 days, Priority 2 incidents must be resolved within 12 to 15 days, and Priority 3 incidents must be resolved within 20 to 25 days. When we inquired about the incidents that were escalated to Flowbird, Metrolinx informed us that they do not track or retain this information. As a result, Metrolinx does not know if Flowbird is meeting its resolution times for incidents as currently there is no process in place to track IT incidents that were escalated to Flowbird and its resolution time.

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.

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; and
- incorporate clauses in contracts to hold vendors accountable and incentivize them to meet targets, and allow for penalties where targets are not met.

RESPONSE FROM METROLINX

Metrolinx agrees with the Auditor General's recommendation:

- Metrolinx currently has all raw data and will require all vendors to provide reports for all priority levels to assess performance against targets and take necessary corrective actions.

- In 2019, Metrolinx began establishing a set of performance standards informed by lessons learned from previous contracts and market trends. Metrolinx has incorporated these performance standards into recent contracts. For all future contracts, Metrolinx is committed to incorporating detailed penalty clauses to hold vendors accountable and incentivize them to meet targets, and allow for penalties where targets are not met.

4.3 Overuse and Overreliance on IT Contractors

Metrolinx hires all of its IT contractors through staffing vendors, and has paid approximately \$157 million to these vendors over the last five fiscal years, ending March 31, from 2015/16 to 2019/20. Seven staffing vendors have had contracts awarded through the Metrolinx procurement or "request to qualify and quote" (RQQ) process (see **Section 2.4**). See **Figure 9** for a list of vendors including the total payments to them and the number of IT contractors they supplied over the past five years.

We selected a sample of 25 contract staff from the list of contractors working for Metrolinx from January 2015 to July 2020. For the samples, we reviewed the staffing requests (including justification and approval to hire contractors), staffing vendor selection, interview processes, contractor performance evaluations, contract extension processes, timesheet approvals and vendor invoices. Our detailed findings are discussed in the following sections.

4.3.1 Contractors Hold Key Decision-making Roles

The role of managers is critical at Metrolinx, as they are responsible for interviewing and hiring new contractors, as well as approving contractor timesheets and reviewing contractor performance. Although Metrolinx is not subject to all sections

Figure 9: Staffing Vendors Contracted by Metrolinx, IT Contractors Hired and Total Payments, as of March 31, 2015/16–2019/20

Source of data: Metrolinx

Vendors	Contractors Supplied		Cost	
	#	% of Total	(\$ million)	% of Total
Tundra Technical Solutions Inc.	334	44	51	33
Eagle Professional Resources Inc.	122	16	39	25
Teksystems Canada Inc.	150	20	39	24
Altis Human Resources Inc.	60	8	12	7
S.I. Systems Ltd	88	11	10	6
Infomaxium Inc.	8	1	5	4
Bagg Technology Resources Inc.	2	0	1	1
Total	764	100	157	100

of the Ontario Public Service (OPS) Procurement Directive, including **Section 4.1.1** of the directive that states that consultants must not perform management functions such as supervising and hiring staff and other consultants, we found that from January 2015 to July 2020, 11 contractors had management positions and were supervising about 40% (307 of 764) of IT contractors hired to support day-to-day IT operations and services. Of the 307 IT contractors, about 80% (246) of these IT contract staff reported to three contractors holding management positions.

We noted that these three contractors had key management roles. Each contractor was either a Director or a Senior Manager, responsible for overseeing one of Metrolinx's three largest IT projects, including Cybersecurity, Integrate Metrolinx (integrating human resources, payroll and finance IT systems) and Enterprise Asset Management (inventory of IT assets). Contrary to the OPS Directive, these contractors were making decisions about project budgeting, and recruiting contractors from staffing vendors.

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.

RESPONSE FROM METROLINX

Metrolinx appreciates the Auditor General's recommendation. Metrolinx has initiated the transfer of key management positions requiring management decisions from contractors to full-time Metrolinx employees.

4.3.2 No Assessment of Existing Resources Results in Metrolinx Paying More Than Needed for Contractors

According to the OPS Procurement Directive, the decision to procure external consulting services must include prior consideration of using internal resources. In addition, the use of consulting services for ongoing, long-term needs over the recruitment of internal full-time employees should be justified. Further, these elements of the decision-making process should be documented.

Over the last five years, 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. The

Figure 10: IT Contractors, Full-time IT Employees and Costs as of March 31, 2015/16–2019/20

Source of data: Metrolinx

	2015/16	2016/17	2017/18	2018/19	2019/20	Total Cost
IT Staff (#)						
Contractors	103	173	314	366	272	—
Full-time employees	156	166	172	166	163	—
Total	259	339	486	532	435	—
IT Staff Costs (\$ million)						
Contractors	13	20	29	50	45	157
Full-time employees	9	10	15	14	17	65
Total	22	30	44	64	62	222
Average cost per full-time employee	57,692	60,241	87,209	84,337	104,294	—
Average cost per contractor	126,214	115,607	92,357	136,612	165,441	—

total costs for IT contractors increased at a higher rate compared to the cost of full-time staff over the same five-year period. See **Figure 10** for the number of full-time and contract IT staff and related costs over the last five years. The high reliance on IT contractors over the last five years resulted in significantly higher costs, some of which Metrolinx could have saved by hiring full-time employees with the required skill sets and experiences, especially for multi-year IT projects.

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, or performed cost/benefit analyses for hiring contractors instead of full-time employees. Further, there were no documented records showing justification for new resources, or that approvals for procuring contractors were properly obtained by hiring managers. This is 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 addition, Metrolinx requires that the interview panel consist of at least two people, including the hiring manager and a Metrolinx full-time staff person. The interview panel makes the final hiring decision and is required to complete and submit the interview questions and scoring forms to the

resource coordination team (see **Section 2.4**).

However, 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.

We also found that for 23 contract positions, Metrolinx obtained only one candidate's profile for the role before interviewing the candidate, instead of assessing the different contractors that were available through their pool of pre-qualified staffing vendors. Metrolinx could have benefitted from comparing hourly rates from other vendors for the same contractor roles to achieve better value for money.

In addition, we noted that in 2015, Metrolinx's former Chief Information Officer (CIO) directly referred four candidates to a staffing vendor for placement in Metrolinx roles already identified for them. Metrolinx did not interview other candidates. We noted that Metrolinx hired these candidates on contract at hourly rates that were higher, in one case much higher, than the standard rates for similar roles in 2015 and 2016. Specifically, of the four contractors referred by the former CIO and hired in 2015, one was paid \$210 per hour as a program manager, and three were paid \$150 per hour as IT program managers. In comparison, the hourly rates of three different staffing vendors for program manager roles in 2015 ranged from \$125 to \$142.

The \$210 per hour rate approved in 2015 was about 48% higher than the rate (\$142) charged for the same role by another staffing vendor (Eagle Professional Resources Inc.) in 2015. Two of the four contractors left Metrolinx in 2019, while two others still had active contracts as of July 2020.

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;
- 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; and
- perform and document interviews, and retain interview notes including the required approvals prior to hiring contractors.

RESPONSE FROM METROLINX

Metrolinx agrees with the Auditor General's recommendation and will annually monitor the following process improvements:

- All new hiring requests now begin with an analysis of internal skill sets and availability.
- The next step in the hiring request is to do an analysis of different delivery models (for example, vendor, internal plus contractors, internal only) and incorporate it into the business case for review and approval before a project is established.
- After it has been determined that there are no internal staff that meet both criteria of skill set and availability, the full-time hiring manager will follow the Resource Allocation Process (RAP). Multiple contractor candidates are interviewed by two interviewers,

at least one of whom must be a Metrolinx full-time employee.

4.3.3 Contracts Renewed Without Proper Business Justification or Performance Evaluations

Metrolinx's policy describes the typical duration of a staff contract as six months, with the potential to extend for up to six additional months at the end of the term. According to the policy, prior to a contract renewal or extension, the responsible manager is required to provide business justification for an extension, and confirmation that the contractor is performing at a satisfactory level.

Based on our sample of 25 IT contractors, 20 (or 80%) had their contracts extended by their managers. We found however that none of 20 contractors had business justifications for the extensions provided or had performance evaluations conducted by their managers to ensure the adequacy of their work.

From the list of IT contractors working at Metrolinx from January 2015 to July 2020, about one-third, or 281 contractors, had their contracts renewed for longer than two years. **Figure 11** provides a breakdown of all contractors and contract lengths. For long-term positions, at the time of extension, Metrolinx should have had proper justification for the use of contractors over hiring internal full-time employees. However, Metrolinx did not perform assessments of internal capacity,

Figure 11: Contractors with Multiple Renewals, January 2015–July 2020

Source of data: Metrolinx

Contract Length	# of Contractors	% of Total
Less than one year	301	39
1-2 year	182	24
2-3 year	134	18
3-4 year	89	12
4-5 year	41	5
Over 5 years	17	2
Total	764	100

or cost/benefit analyses to determine whether it was more beneficial for Metrolinx to hire full-time employees to replace the contractors. Upon reviewing these extended contracts and the contractors' roles, we noted that some of the roles did not require specialized skills and many candidates would have been relatively available in the job market.

Vendor-hopping Increases Hourly Rates Paid to Contractors

We noted that contractors received increases in their hourly rates, some of which were increases of up to 12%, without any documented rationale. For example, based on the sample of 25 contractors whose recruitment files we reviewed over the last five years, 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%.

We also found that five of the 12 contractors whose hourly rates increased had switched staffing vendors. For example, a contractor hired in 2016 for an IT enterprise architect role changed staffing vendors from Altis Human Resources Inc. to TEK-systems Canada Inc. in 2017. When this person's contract was renewed for the same role after the contractor had switched to a different vendor, the hourly rate increased by 8% from \$120 to \$130. Metrolinx records did not provide any explanation or justification for the rate increase, which was

approved by IT management. Currently, there is no process to flag to anyone at Metrolinx if a contractor switching staffing vendors results in a rate change.

Metrolinx is Exploring Outsourcing All IT Functions, Which Would Significantly Increase Reliance on IT Contractors

During our audit, we noted that as a result of Metrolinx's reliance on contractors over full-time employees, we encountered difficulties obtaining information about IT projects. For example, obtaining information about some IT projects was difficult, as there was a lack of documentation and because we could not interview contractors in key roles as they were no longer with Metrolinx. Best practices in organizational IT management warn against an overreliance on contract staff, due to difficulties transferring and maintaining corporate knowledge about these highly technical projects.

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. As shown in **Figure 12**, 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 CEO 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

Figure 12: Contractors and Full-Time Employees as of March 31, 2015/16–2019/20

Source of data: Metrolinx

Fiscal Year	Contractors		Full-Time Employees		Total
	# of Contractors	% of Total	# of Employees	% of Total	
2015/16	103	40	156	60	259
2016/17	173	51	166	49	339
2017/18	314	65	172	35	486
2018/19	366	69	166	31	532
2019/20	272	63	163	37	435

IT department in order to transfer the technology risks to an outsourced vendor.

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;
- confirm through performance evaluations that the contractor is performing satisfactorily and obtain the appropriate approvals prior to the renewal or extension of a contract;
- assess the rationale for increases in contractors' hourly rates so that the revised rates are economical; and
- 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.

RESPONSE FROM METROLINX

Metrolinx agrees with the Auditor General's recommendation and will annually monitor the following process improvements:

- All contract renewals and extensions are now reviewed and approved by a Metrolinx full-time manager. The renewal/extension rationale and justification are documented and centrally stored.
- Prior to the renewal/extension of a contract, Business Technology will conduct a performance report card.
- In order to support a rate increase, Metrolinx will review the tenure of the contractor (must be greater than one year) and when the last rate increase was given (must be greater than one year), and conduct a comparison against other contractors in the same role on

the same contract. The rate increase will not exceed the maximum rate for that role.

- As part of Metrolinx's information technology transformation, Metrolinx will conduct a comprehensive analysis of sourcing options. All appropriate formal approvals will be sought, including approvals from the investment panel, Metrolinx's Board of Directors and the Ministry.

4.4 Security Weaknesses in Metrolinx's IT Systems

Organizations typically perform security scans, such as penetration testing on IT systems and websites to identify and remediate security weaknesses before an attacker can exploit the weaknesses. Organizations also perform software code reviews to detect security weaknesses caused by unsecure or poorly written software code.

Testing and remediation of security weaknesses protects IT systems as well as the data and information organizations collect. Organizations collect and store confidential and personal information of customers and employees for business purposes. They also collect extensive amounts of sensitive and confidential corporate and financial data to make informed business decisions. According to industry best practices, organizations should assign appropriate classification levels of confidentiality and sensitivity to information. These classifications ensure different information types receive the appropriate level of security and access controls. As well, according to the *Freedom of Information and Protection of Privacy Act* (FIPPA), organizations must maintain customer and employee personal information along with information about data storage and protections employed, and the information's retention and disposal requirements.

4.4.1 Lack of Regular IT Security Testing Results in Breaches and Accidental Releases of Data

Industry best practices, such as Information Systems Audit and Control Association (ISACA) and National Institute of Standards and Technology (NIST), require security scans for critical IT systems, such as penetration testing, to be performed at least annually. However, 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. For security reasons, detailed information about our audit work was provided directly to Metrolinx management. We also noted that the tests that were performed, were scheduled on an ad-hoc basis or in response to a cybersecurity breach. Based on our review, some systems have not been tested for security weaknesses for many years and other systems have never been tested. As a result, we noted IT systems were vulnerable to attack, and resulted in two significant security breaches in the last five years. Hackers therefore were able to gain access to confidential information and customers' personal information. For example:

- The Eglinton Crosstown website, thecrosstown.ca, was hacked three times between February 15, 2019, and March 27, 2019. This website, managed by Pivotree, a third-party vendor, provides information on the Eglinton Crosstown's construction progress. Customers can subscribe to its email updates with their names, email addresses and postal codes. We found that hackers had gained access to the website server due to a security vulnerability that could have been addressed with a security patch. The hackers accessed customer names, email addresses and postal codes. We noted that Metrolinx had not performed a penetration test and vulnerability scan to identify security weaknesses since it launched thecrosstown.ca in September 2011. After the hack, the vendor remediated the vulnerability the next day, on March 28, 2019.

RECOMMENDATION 8

To minimize Metrolinx's vulnerability to cyber-attack 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.

RESPONSE FROM METROLINX

Metrolinx accepts the Auditor General's recommendation. Metrolinx will engage an independent third party to conduct a comprehensive security test including, for example, penetration testing to identify the areas of need for improvement. From that identification we will create a roadmap by early 2021 and establish the priorities, the timeline to implement, and the measures of success. Until such time as a new roadmap is developed and while it is being developed, Metrolinx will continue to run regular cybersecurity testing and assessments within our Payment Card Industry (PCI) environment in order to maintain our ongoing compliance.

4.4.2 Metrolinx Does Not Always Review Software Code for Transit Systems

Software code is a set of instructions written by a programmer that defines the way software works and the tasks it performs. According to industry best practices, organizations should perform software code reviews whenever changes are made to critical IT systems to determine security weaknesses. Based on our review, we noted that Metrolinx does not always perform software code reviews for critical transit systems for safety, dispatch, track allotment, scheduling and communications within the Network Operations Centre (NOC).

We found that the software code had not been reviewed for any of the 12 sampled IT systems for security weaknesses. Six of these 12 IT systems had

been developed and managed by vendors. However, we also found that Metrolinx does not require its vendors to perform software code reviews according to industry best practices. These reviews were not required in the initial vendor contracts, which resulted in a lack of security assurance from its vendors. We noted the following two significant privacy data breaches at Metrolinx:

- Metrolinx uses Google Analytics, a website data analytics service that collects website data such as customers visited, time spent on websites, and content accessed, using a software code. In December 2018, more than 100,000 customer email addresses, along with other customer personal information such as addresses and names, were captured in the website addresses that were sent to Google Analytics. This breach was caused by poorly written software code that had not been properly tested. Metrolinx could have prevented this breach by performing a scan of their software code to identify potential for accidental data breach. Metrolinx IT remediated the issue in January 2019 by implementing a fix to the software code script.
- Another privacy breach occurred in August 2020, when Metrolinx accidentally disclosed email addresses of about 2,000 customers in an attempt to gather feedback about their experiences with fines they had been assessed for not paying their fares. The email addresses of customers were added in the “To” email address field, instead of the blind-copy field. This resulted in customers who had been fined seeing the names and email addresses of other customers with a similar history. We also found that the breach was identified by a customer rather than Metrolinx.

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.

RESPONSE FROM METROLINX

Metrolinx agrees with the Auditor General’s recommendation. Metrolinx will include this review as part of the comprehensive security test, including, for example, review of software codes and creation of the roadmap relating to **Recommendation 8**.

4.4.3 Not All Metrolinx Customer Personal Information Is Protected

Metrolinx collects customers’ personal information for business purposes. 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. With the exception of PRESTO, we found in our review that that Metrolinx does not consistently identify, classify and protect customer and employee personal information. We noted that customer and employee personal information in two databases we reviewed is stored in plain text format without adequate security controls such as data masking or encryption. In the event of a successful cyberattack, data could be easily accessed by external hackers.

Metrolinx Access to Customer Personal Information

Industry best practices require limiting administrator accounts and restricting password-sharing among users. We noted, however, that Metrolinx currently has 7 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 7 IT database administrators were contractors, not full-time Metrolinx employees. We also noted that four

administrators of 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. This is not in line with best practices for information security. According to industry best practices, a system administrator account should be used instead of individual administrator accounts. A system administrator account, such as a “Firecall ID,” is a method that provides temporary and monitored access to sensitive and secured information.

Weak Password Controls for Critical IT Systems

Metrolinx has established a password policy that defines password requirements for IT systems and databases. These requirements include characteristics such as minimum length, requiring more complex passwords with a combination of numbers, uppercase and lowercase letters and special characters (such as @!\$&#%). The policy also requires its staff to change their passwords every 90 days. We found that password settings for Metrolinx’s Oracle databases does not comply with Metrolinx’s own password policy, as the minimum length is set to one character, instead of an eight-character minimum as required by the policy. We also found that Oracle database passwords never expire, increasing the risk of unauthorized access if passwords are never changed. Passwords act as the first line of defence against hackers, and therefore, it is important for Metrolinx to adhere to its established password policy.

Lack of Audit Logging for Administrator Activities

IT systems store data in database tables that are managed by database administrators. We noted that although Metrolinx systems log basic activities performed by database administrators, they do 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.

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;
- restrict access to sensitive corporate information according to industry standards and best practices;
- review password settings for all critical IT systems and enforce its password policy to reduce the risk of unauthorized access; and
- implement audit logging capabilities and alerts for events that are necessary for ensuring accountability and protecting information.

RESPONSE FROM METROLINX

Metrolinx agrees with the Auditor General’s recommendation. On June 2, 2020, Metrolinx’s senior management team approved an Information Security Classification Policy, which will provide a standardized mechanism to identify which corporate assets will require specific levels of security controls to ensure their security and integrity. In accordance with this policy, Metrolinx will:

- review Metrolinx’s personal information holdings and develop a plan to apply the classification and security protections such as encryption required by the policy, aligned with industry best practices;
- implement controls to validate and enforce policy-based protection requirements to access controls;
- implement controls to review password settings and enforce compliance to policy for

critical systems to ensure compliance with Metrolinx's password policy; and

- develop a plan to implement access tracking, and review processes for specific events that pose a risk to the disclosure of personal information based on Metrolinx policies.

4.5 Lack of Disaster Recovery Strategy

Organizations develop disaster recovery strategies and establish alternate facilities to ensure business continuity. A disaster recovery strategy includes identifying and classifying critical and non-critical IT systems, and establishing the order of recovery for those systems in case of a disaster. For example, IT systems used for Metrolinx's critical transit operations should be recovered before corporate IT systems used for human resources and finance. Disaster recovery plans should include step-by-step instructions for handling IT systems in a disaster, and regular testing of disaster recovery plans and procedures. Disaster recovery locations are alternate facilities equipped with hardware, such as servers and network equipment, data and critical software, in the event that the primary data centre is unavailable.

Critical IT systems for transit operations, such as scheduling, transit safety, and communications are hosted at the Guelph Data Centre. We noted that Metrolinx had not established an organizational disaster recovery strategy to ensure continuity of business operations. In the event of an actual disaster (such as a cyberattack, earthquake, power outage, extreme weather event or vandalism) at the Guelph centre, Metrolinx would not have a plan for how to respond to the disaster. Metrolinx transit operations such as tracking, scheduling, dispatching, signals and crossings, and platform assignments for UP Express, and GO trains and buses would have to be operated manually, according to its Business Continuity Plan.

We noted that Metrolinx's Kingston Data Centre already functions as an alternate data centre for

testing purposes, such as developing and testing changes to existing IT systems. However, the Kingston centre is not equipped with the necessary servers, software and data to function as an alternate location in case of a disaster. Because any disaster affecting the Guelph centre could result in significant delays to transit operations, back-ups and redundancies should be established so that service outages can be minimized.

In the last five years, from January 1, 2016 to May 1, 2020, we noted that there were about 360 IT incidents affecting systems used for transit operations. If Metrolinx had developed a disaster recovery strategy, established a recovery facility, and performed disaster recovery exercises, the impact caused by these incidents could have been minimized. **Appendix 3** shows a detailed breakdown of IT incidents, along with a brief description and related service impacts.

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; and
- perform a cost/benefit analysis for establishing a functional disaster recovery location for continuity of transit operations.

RESPONSE FROM METROLINX

Metrolinx agrees with the Auditor General's recommendation, and will:

- as part of the development of the roadmap relating to **Recommendation 8**, establish a strategy to implement an overall disaster recovery plan and schedule, where regular testing exercises are performed; and
- in conjunction with the third party conducting the vulnerability assessment, perform a cost/benefit analysis as part of

establishing the roadmap of disaster recovery activities.

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

Organizations develop IT strategies to ensure that hardware, software and IT projects are managed economically and effectively. The centralized procurement of IT systems and websites required for business operations is a key element of an enterprise IT strategy. A well-defined and implemented strategy can help organizations avoid duplicating costs and efforts.

4.6.1 Lack of IT Governance, Oversight and Strategy Squanders Public Funds

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. We noted that 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.

We examined the types of systems and services that departments were using, and found that some departments had procured additional IT systems and services when other departments already possessed the same systems or functions that were needed. For example, we noted:

- The Capital Projects Group is currently in the final phase of contract negotiation with Accenture to provide Internet and network connectivity services for PRESTO fare payment devices at the Eglinton Crosstown's LRT stations. The total contract value is estimated at \$8.5 million. As noted in **Section 2.1**,

in the past, the IT department has implemented Internet and network services for fare payment devices and wireless Internet at GO stations. Although Metrolinx has the internal IT resources with the skill sets to provide Internet services, Metrolinx did not perform an assessment of internal capabilities before procuring these services externally, resulting in potential additional, unnecessary project costs.

- Two groups within Metrolinx have purchased ServiceNow for their own use. ServiceNow is an incident management system used to create IT tickets for tracking and reviewing IT incidents and changes made to systems. The system was independently procured by the Metrolinx IT department for approximately \$318,000 in 2016, and by the Network Operations Centre for approximately \$56,000 in May 2020. Both departments pay annual costs of approximately \$220,000 and \$68,000 respectively to different vendors for maintenance and support of this system. If the Network Operations Centre had leveraged the IT department's existing ServiceNow contract, it could have avoided both the purchase and maintenance costs it incurred. Metrolinx could have saved approximately \$100,000 in procurement and maintenance costs by leveraging the existing IT system.
- Two groups, Metrolinx's Capital Projects Group and Marketing, individually procured the Salesforce IT system. Salesforce is used for project tracking and customer relationship management. The Capital Projects Group paid approximately \$665,000 to procure the system in 2019, and Marketing procured the same system for approximately \$109,000 in 2020. Metrolinx could have purchased the second IT system using the same terms as the first IT system. The second system was procured by Marketing with limited scope and staff. Metrolinx could have saved approximately \$109,000.

- Digital signs that display transit departure information and service alerts information to customers at GO and UP Express stations were procured from two different vendors. As a result, there are two different contracts and related costs for the signage and maintenance for the same service. In the past five years, Metrolinx has paid approximately \$300,000 to one vendor to manage 68 GO Train stations. However, Metrolinx also paid approximately \$350,000 to another vendor to manage four UP Express stations. Metrolinx could have saved approximately \$350,000 if it had leveraged the existing contract from its original vendor.
- Two groups, Metrolinx's Capital Projects Group and Finance, each procured Oracle software. The Capital Projects Group has paid approximately \$11 million in 2015 for the procurement of the Oracle IT system. The same IT system was procured independently by Metrolinx Finance in 2016. Finance has paid approximately \$3.5 million for the same system and support. Again, Metrolinx could have saved these costs if it had leveraged the contract from the first purchase.

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; and
- 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.

RESPONSE FROM METROLINX

Metrolinx agrees with the Auditor General's recommendation. Metrolinx will:

- develop an overall IT strategy with a centralized procurement process for IT systems and services; and
- 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.

4.6.2 Websites Developed Result in High Costs with Poor Integration

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. We also noted that Metrolinx was unable to provide the capital cost for two of its websites, smartcommute.ca and Triplinx.ca. Refer to **Appendix 4** for a list of websites, their descriptions and cost information.

Websites that Provide Similar Information

We found that three of the eight websites (metrolinx.com, metrolinxengage.com and thecrosstown.ca) provide similar information with overlap, such as corporate information and construction updates. In another example, we found that customers are able to check for GO Transit schedules on both GOtransit.com and Triplinx.ca. Similarly, customers are able to check for UP Express train schedules and service updates on UPEXpress.com and Triplinx.ca. The information on Triplinx.ca is also available on Google Maps for free; as noted in **Appendix 4**, Metrolinx has paid approximately \$2.4 million to the vendor for maintenance as operating cost.

Websites with Overlapping Functionality

We also noted that Metrolinx has two different websites (UPExpress.com and GOtransit.com) for purchasing tickets and checking transit schedules. Although there are some similar purposes within the two sites, UP Express was launched as a separate brand in 2015 with a different customer segment to GO. Instead of having separate websites to purchase tickets and check schedules, the same functionalities that already existed in GOtransit.com could have been leveraged instead of creating UPExpress.com.

Website Development and Usage

We reviewed average annual visits by customers for all eight websites for 2019. See **Figure 13** for this information. We noted that most of these websites are not frequently visited—only GOtransit.com and prestocard.ca are consistently used by a significant number of customers. We noted that instead of using existing websites and leveraging existing customer awareness, Metrolinx has instead created new websites. As a result, six of the eight main websites have only a fraction of the visitors and usage compared to the two most-visited websites.

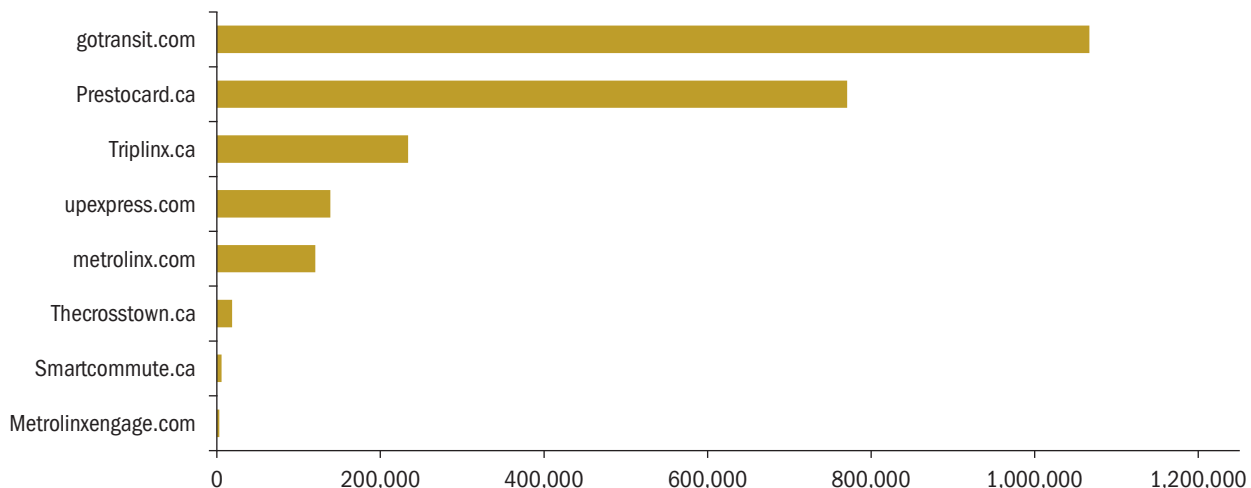
We benchmarked Metrolinx websites against other transit agency websites such as Transport for London, which covers the London Metropolitan

Area in the United Kingdom, Translink.ca, the regional transportation authority that operates public transit system in Greater Vancouver, British Columbia, and TransportNSW, which covers the state of New South Wales in Australia. We found that these websites provided easy and consolidated information all on a single website. For example:

- The Transport for London website provides easy and consolidated access to trip planning, transit schedules, service updates, fare payments, ticket purchasing, corporate information and project updates on one website. The scheduling feature provides schedules for all trains without having to navigate to other websites.
- Translink.ca is the website used in the Greater Vancouver area by Translink, the local transit agency. We noted that the different features, such as ticket purchasing, trip planning, transit schedules and services updates are all available on the same website.
- TransportNSW is the government's lead public transport agency for the state of New South Wales in Australia. We noted that through the transportnsw.info website, all the information needed to access public transport is available, similar to the other websites reviewed.

Figure 13: Monthly Average of Total Unique Visitors Across Eight Metrolinx Websites, January–December 2019

Source of data: Metrolinx



RECOMMENDATION 13

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

- review and consider existing websites; and
- 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.

RESPONSE FROM METROLINX

Metrolinx agrees with the Auditor General's recommendation that existing websites together with broader digital customer communication channels must provide customers with easy access to information. As part of the Customer Digital Transformation Strategy, Metrolinx will review existing websites to 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.

4.6.3 Poor Project Management Results in Project Cost Overruns, Delays and Cancellations—and Inefficiencies

Metrolinx spent approximately \$336 million on 122 IT projects completed from March 2014 to November 2019. These projects include IT systems for tracking and dispatching buses and trains, website redesigns, UP Express e-ticketing, and customer communications for service delays and schedule updates. **Figure 14** shows the number of projects by budget category.

We reviewed the IT projects in Metrolinx's project management system, used to track projects for monitoring and reporting purposes. We analyzed 122 completed IT projects from March 2014 to November 2019 and compared the actual costs and time to complete the projects to initial budgets and estimated end dates, as shown in **Figure 15**.

Figure 14: Completed IT Projects and Costs, March 2014–November 2019

Source of data: Metrolinx

Project Cost Category	# of Projects	Total Cost (\$ million)
Below \$1 million	48	19
Between \$1 million and \$5 million	55	120
\$5 million and above	19	197
Total	122	336

Figure 15: Actual Results of Metrolinx IT Projects Compared to Initial Budgets and Estimated End Dates, March 2014–November 2019

Source of data: Metrolinx

	# of Projects Completed	Cost (\$ million)
Results against Budget		
Over budget	88	288
Within budget	29	36
Without having an initial budget	5	12
Total	122	336
Results against Estimated End Dates		
Later than estimated end date	66	134
Within estimated end date	0	0
Without having an estimated end date	56	202
Total	122	336

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.

Specifically, we noted:

- 88 projects, or 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. Of the 88 projects that went over-budget, 42 projects cost more than double their initial budgets.

- Completion dates noted for 66 projects indicated that they were not completed within their estimated timelines. We noted that the time to completion ranged from four months to almost 10 years past targeted completion dates. In addition, Metrolinx was unable to provide estimated completion times for 56 projects, as this information was not tracked in project documents or in the project management system.

We selected five projects with a total value of approximately \$78 million for detailed reviews to determine if there was effective oversight, and if the projects adhered to project management requirements. Refer to **Appendix 5** for our sample selection. The projects were also selected as projects that had more direct impacts on customer experience, such as websites and GO train and bus services. We also considered projects with significant differences between budgeted and actual costs, and estimated and actual dates of completion. Based on our review, we identified systemic issues in IT project management and operations. These issues include:

- lack of project scope in project plan, or not enough detail in scope,
- poor project documentation practices, or lack of these practices, including use of Metrolinx's project management system,
- lack of senior management approvals at milestones, and moving from one project phase to the next without required approvals,
- lack of appropriate budget controls, and allowing projects to run overbudget without senior management approval,
- approvals provided by senior management for budget increases with inadequate justification and
- mid-project changes to scope, resulting in a reduction in deliverables and expected service improvements.

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;
- properly document and monitor project timelines, budgets and costs; and
- ensure proper oversight over project changes with well-documented justification and appropriate approvals.

RESPONSE FROM METROLINX

Metrolinx agrees with the Auditor General's recommendation and as such:

- a new centralized project management system is being implemented that will lock down project scope and review scope performance. All IT projects will be migrated to the new system by July 2021;
- the new system will strengthen the current collection of documents, establish a baseline, and manage any changes to the timelines, budget and costs during the project life cycle; and
- any changes will follow the approved organizational project management framework from the Technology Change Control Board and Investment Panel.

Appendix 1: Summary of PRESTO Fare Payment Devices, February 2016–March 2020

Source of data: Metrolinx

Type of PRESTO Device	Vendor	Functionality	# of Incidents* (approx.)	# of Devices	Device Age	Expected Lifespan for the Devices (Years)	Price per Asset with Maintenance (\$)	% of Incidents
Ticket Vending Machine (TVM)	Flowbird	<ul style="list-style-type: none"> Purchase tickets and PRESTO cards Reload balance to PRESTO card Check balance and transaction history 	40,000	225	<ul style="list-style-type: none"> 120 devices: 11 years 80 devices: 9 years 25 devices: 7 years 	10	42,000	82.71
Station Fare Transaction Processor (SFTP, Green tap machine)	Accenture	<ul style="list-style-type: none"> Fare payment Display trip cost Display green light for successful fare payment Display red light for unsuccessful fare payment Display balance 	3,500	697	<ul style="list-style-type: none"> 670 devices: 10–12 years 27 devices: 7 years 	7–10	9,083	7.24
Station Point of Sale Machines (SPOS)	Accenture	Used by GO station attendant to issue tickets	2,500	249	Reached end of life	7–10	2,163	5.17
Card Query Device (CQD)	Accenture	<ul style="list-style-type: none"> Display balance Card activation for cards purchased online 	40	88	Removed	7–10	3,016	0.08
Handheld Card Reader (HCR)	Accenture	Used by ticket inspectors GO Transit and UP Express	100	275	End of life	7–10	1,724	0.21
Driver Control Unit (DCU)	Accenture	Bus driver interface and printer for issuing tickets	2,200	506	End of life	7–10	3,757	4.55
Self-Service Reload Machine (SSRM)	Accenture	<ul style="list-style-type: none"> Purchase PRESTO cards Reload balance to a PRESTO card Check your balance and transaction history 	20	102	Reaching end of life	7–10	25,109	0.04

* Total number of incidents (approximately) 48,000.

Appendix 2: Audit Criteria

Prepared by the Office of the Auditor General of Ontario

- | | |
|----|--|
| 1. | Critical IT systems for transit operations are being operated and maintained economically and monitored to have safe and reliable operations. Timely corrective action is taken to mitigate any service disruptions. |
| 2. | Reliable backup and disaster recovery plans are in place for critical IT services. |
| 3. | Adequate controls and procedures are in place to restrict access, and detect, prevent and mitigate Cybersecurity threats to Metrolinx operations in an efficient and timely manner. |
| 4. | Effective oversight is in place to ensure that IT project and procurement processes are managed economically and in accordance with applicable legislation, regulations, directives and trade agreements. |

Appendix 3: Key IT Systems and Related IT Incidents, January 2016–May 2020

Prepared by the Office of the Auditor General of Ontario

IT System	Description	Impact	Incidents (#)
Automatic Train Locating System/Trip Movement Manager (ATLS/TMM)	IT System used to display maps on trains in real-time.	GO train trip information updated in a delayed manner and missing information for certain GO trains due to IT Issues.	101
Computer-Aided Dispatch/Automatic Vehicle Location (CAD/AVL)	IT System used for dispatching GO buses, tracks information on trips with arrival times and passenger count.	Metrolinx was unable to track GO buses, dispatch drivers and feed arrival information.	24
Customer Communication Management System (CCMS)	Communication IT system to send messages to customer via communication channels such as email, text message, social networking (Facebook, Twitter etc.)	Unable to send notifications to customers on service delays and alerts.	40
CCTV Indigo	CCTV cameras that are used to monitor GO train, GO buses, UP Express stations and Metrolinx corporate offices	CCTV Cameras were not working as they were out of service due to IT network errors. In addition, Metrolinx was unable to access or review footage certain stations or facilities.	31
Giro - Hastus	IT system used by Bus Operations for planning, scheduling, driver assignment, etc.	Giro - Hastus IT system was out of service due to IT performance issues.	14
GO Transit Website	GO Transit public website used for customers to ticket purchases, check schedules, plan a trip, calculate fare and get service updates on alerts and service disruptions.	Website was out of service as a result customers were unable to view schedules and other transit related data.	39
Service Guarantee Program System (RTSI)	RTSI framework is a suite of IT systems used for various functionalities such as submit service guarantee claims, track claims and reporting purposes.	RTSI servers not working due to low storage space.	3
Station Service Status System	IT system used to display information such as schedule and announcements on digital signs (TV monitors and signage) at stations.	S4 systems were unavailable or unresponsive at multiple stations. S4 screens did not display schedule information.	50
Trip Manager	IT system for scheduling GO and UP Express trains.	Trip Manager systems was not able to track certain trains and was showing incorrect information regarding origin, departure time, platform information.	38
UP Express Website	UP Express public website	Customers were unable to pay for the ticket and find schedule information.	21
Total			361

Appendix 4: Website Project Information, Including Capital and Operating Costs

Source of data: Metrolinx

Web Site	Information	Detailed Description	End User	Developer	Management	Capital Cost (\$)	Operating Costs (\$)
Metrolinx.com	Corporate	Corporate website that provides general information about Metrolinx, their projects, programs, transit news and senior management	Commuters, Stakeholders	OpenText Corp. TEKsystems Canada Deloitte	Metrolinx	22,505,584	933,016
UPexpress.com	Customer	Website that provides Information on fares, train schedules, stations, flight-related information on trips from and to Pearson Airport on the UP Express train.	Commuters	Deloitte Capital Infosys Ltd.	Metrolinx	16,700,741	4,049,385
GOtransit.com	Customer	Website that offers access to a range of information and services such as trip planning, ticket purchases, bus and train schedule, fare, station information and real-time service alerts on bus, train and station delays, closure or cancellation	Commuters	OpenText Corp. TEKsystems Canada Deloitte	Metrolinx	Part of metrolinx.com	1,476,516
Metrolinxengage.com	Customer	Website that provides Information on GO, UP, light rapid transit (LRT) and subway-related extension or development projects; also allows the general public to comment, submit questions or discuss their projects	Commuters, Stakeholders	OpenText Corp. TEKsystems Canada Deloitte	Metrolinx	Part of metrolinx.com	Part of metrolinx.com
Smartcommute.ca	Customer	Website that provided smart travel options such as walking, cycling, transit and carpooling for commuters within the GTHA	Commuters	108 Ideaspace	Metrolinx	Metrolinx unable to provide	776,463
Thecrosstown.ca	Project	Website that provides up to date details on the Eglinton Crosstown LRT which is expected to be completed in 2022	Commuters, Stakeholders	Pivotree	Metrolinx	202,093	n/a
Triplinx.ca	Customer, Transit agencies	A trip planning website and for transit related information for the Greater Toronto and Hamilton Area (GTHA)	Commuters, Transit agencies	Cityway	Metrolinx	Metrolinx unable to provide	2,555,847
Prestocard.ca	Customer	Account/card management website that enables users to manage their PRESTO cards, allowing them to purchase, activate, register, check balance, view transaction history, load and pay for adding funds and report a lost or damaged PRESTO card	Commuters	Presto Accenture Deloitte	Presto Deloitte	4,517,893	4,405,796
Total						43,926,311 *	14,197,023

* The total capital cost does not include capital costs for Smartcommute.ca and Triplinx.ca because Metrolinx was unable to provide the capital costs for these sites.

Appendix 5: IT Projects Delayed and Overbudget

Source of data: Metrolinx

Project Name	Project Description	Actual Start Date	Estimated End Date	Actual End Date	Initial Budget (\$ million)	Actual Cost (\$ million)
Web Redesign for Metrolinx and GO Transit Websites	Refresh the customer digital experience via the Metrolinx.com and GOTransit.com websites and implement a web content management system	Mar 2016	Apr 2017	Sep 2018	9.3	22.5
Dispatch and Tracking System for Rail and Bus (CAD/AVL)	Implement an IT software solution to provide station specific train service status information at GO stations, trains and buses	Mar 2011	n/a	Apr 2017	6.9	12.2
E-Ticketing System for UP Express	Provide an online ticketing system to allow customer to purchase UP Express train tickets on the UP Express website and Mobile Application	Jul 2015	Jan 2016	Apr 2018	4.3	6.4
Cybersecurity Risk Management	Implement action plans such as incident response plan, system access control and system patch management to strengthen Metrolinx's cybersecurity	Jul 2017	Jul 2021	In progress	34.9	25.6*
Information Protection for Emails and Human Resources Files	Implement IT software to protect the content of Metrolinx staff email communications and human resources files from unauthorized access through encryption	Dec 2016	Jan 2019	Cancelled	8.7	11.2
Total					64.1	77.9

* As of July 2020.



Office of the Auditor General of Ontario

20 Dundas Street West, Suite 1530
Toronto, Ontario
M5G 2C2
www.auditor.on.ca