Fifth Session – Forty-Second Legislature

of the

Legislative Assembly of Manitoba

Standing Committee on Public Accounts

Chairperson
Mr. Jim Maloway
Constituency of Elmwood

Vol. LXXVII No. 3 - 1 p.m., Tuesday, June 6, 2023

ISSN 0713-9462

MANITOBA LEGISLATIVE ASSEMBLY
Forty-Second Legislature

Member	Constituency	Political Affiliation
ALTOMARE, Nello	Transcona	NDP
ASAGWARA, Uzoma	Union Station	NDP
BRAR, Diljeet	Burrows	NDP
BUSHIE, Ian	Keewatinook	NDP
CLARKE, Eileen, Hon.	Agassiz	PC
COX, Cathy	Kildonan-River East	PC
CULLEN, Cliff, Hon.	Spruce Woods	PC
DRIEDGER, Myrna, Hon.	Roblin	PC
EICHLER, Ralph	Lakeside	PC
EWASKO, Wayne, Hon.	Lac du Bonnet	PC
FONTAINE, Nahanni	St. Johns	NDP
GERRARD, Jon, Hon.	River Heights	Lib.
GOERTZEN, Kelvin, Hon.	Steinbach	PC
GORDON, Audrey, Hon.	Southdale	PC
GUENTER, Josh	Borderland	PC
GUILLEMARD, Sarah, Hon.	Fort Richmond	PC
HELWER, Reg	Brandon West	PC
ISLEIFSON, Len	Brandon East	PC
JOHNSON, Derek, Hon.	Interlake-Gimli	PC
JOHNSTON, Scott, Hon.	Assiniboia	PC
KHAN, Obby, Hon.	Fort Whyte	PC
KINEW, Wab	Fort Rouge	NDP
KLEIN, Kevin E., Hon.	Kirkfield Park	PC
LAGASSÉ, Bob	Dawson Trail	PC
LAGIMODIERE, Alan	Selkirk	PC
LAMONT, Dougald	St. Boniface	Lib.
LAMOUREUX, Cindy	Tyndall Park	Lib.
LATHLIN, Amanda	The Pas-Kameesak	NDP
LINDSEY, Tom	Flin Flon	NDP
MALOWAY, Jim	Elmwood	NDP
MARCELINO, Malaya	Notre Dame	NDP
MARTIN, Shannon	McPhillips	PC
MICHALESKI, Brad	Dauphin	PC
MICKLEFIELD, Andrew	Rossmere	PC
MORLEY-LECOMTE, Janice, Hon.	Seine River	PC
MOSES, Jamie	St. Vital	NDP
NAYLOR, Lisa	Wolseley	NDP
NESBITT, Greg, Hon.	Riding Mountain	PC
PEDERSEN, Blaine	Midland	PC
PIWNIUK, Doyle, Hon.	Turtle Mountain	PC
REDHEAD, Eric	Thompson	NDP
REYES, Jon, Hon.	Waverley	PC
SALA, Adrien	St. James	NDP
SANDHU, Mintu	The Maples	NDP
SCHULER, Ron	Springfield-Ritchot	PC
SMITH, Andrew, Hon.	Lagimodière	PC
SMITH, Bernadette	Point Douglas	NDP
SMOOK, Dennis	La Vérendrye	PC
SQUIRES, Rochelle, Hon.	Riel	PC
STEFANSON, Heather, Hon.	Tuxedo	PC
TEITSMA, James, Hon.	Radisson	PC
WASYLIW, Mark	Fort Garry	NDP
WHARTON, Jeff, Hon.	Red River North	PC
WIEBE, Matt	Concordia	NDP
WISHART, Ian	Portage la Prairie	PC
WOWCHUK, Rick	Swan River	PC
Vacant	Morden-Winkler	

LEGISLATIVE ASSEMBLY OF MANITOBA

THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

Tuesday, June 6, 2023

TIME – 1 p.m.

LOCATION – Winnipeg, Manitoba

CHAIRPERSON – Mr. Jim Maloway (Elmwood)

VICE-CHAIRPERSON – Mr. Shannon Martin (McPhillips)

ATTENDANCE – 9 QUORUM – 6

Members of the committee present:

Messrs. Guenter, Isleifson, Lamont, Ms. Lathlin, MLA Lindsey, Messrs. Maloway, Martin, Michaleski, Schuler

Substitutions:

Mr. Schuler for Mr. Smook

APPEARING:

Mr. Tyson Shtykalo, Auditor General

WITNESSES:

Mr. Joseph Dunford, Deputy Minister of Consumer Protection and Government Services

Ms. Lanette Siragusa, Chief Executive Officer, Shared Health

Mr. Hong Chung, Chief Information Officer, Province of Manitoba

Mr. Doug Snell, Chief Operations Officer, Shared Health–Digital Shared Services

MATTERS UNDER CONSIDERATION:

Auditor General's Report – Aging Information Systems, dated February 2022

Auditor General's Report – Information Systems–Privileged Access, dated October 2022

* * *

Mr. Chairperson: Good afternoon. Will the Standing Committee on Public Accounts please come to order.

The–this meeting has been called to consider the following: the Auditor General's Report–Aging Information Systems, dated February 2022; and Auditor General's Report–Information Systems–Privileged Access, dated October 2022.

Committee Substitution

Mr. Chairperson: I'd like to inform the committee that under rule 104(2), the following membership substitution has been made for this meeting only: Mr. Schuler for Mr. Smook.

* * *

Mr. Chairperson: Are there any–*[interjection]* oh, the other one. Okay.

For the information of the committee, there's been a request for the following witnesses to be able to speak on the record and to answer questions from members: Hong Chung, CIO for the Province of Manitoba; and Doug Snell, COO for Shared Health, Digital Shared Services.

Is there leave of the committee to allow them to speak on the record if required? Agreed? *[Agreed]*

Are there any suggestions from the committee as to how long we should sit this afternoon?

Mr. Shannon Martin (McPhillips): Mr. Chair, I'd suggest we sit 'til 3 p.m. and reassess at that time.

Mr. Chairperson: It's been suggested by Mr. Martin that we sit 'til 3:00 and reassess at that time.

Agreed? *[Agreed]*

Does the Auditor General wish to make an opening statement?

Mr. Tyson Shtykalo (Auditor General): With respect to my report on aging information systems, I'd first like to introduce the staff members I have with me today. I'm joined by Wade Bo-Maguire, assistant auditor general for IT and Innovation; Ian Montefrio, audit principal, IT and–IT audit and innovation; and Stacey Wowchuk, assistant auditor general, performance audit.

Mr. Chair, the Province of Manitoba relies on information systems to deliver a wide range of services that Manitoba depends on. This includes online registrations, program applications and fee payments. These information systems include hardware such as servers, firewalls, switches and routers as well as the software that runs on these devices.

As these information systems age, they become more susceptible to risks, including extended system outages, decreased system reliability and increased security vulnerabilities. Aging systems may also be unable to keep up with the evolving needs and expectations of Manitobans.

It's important that the age and suitability of information systems be monitored to make sure that they are replaced or upgraded when needed. In my report, Aging Information Systems, we found that the Province has not adequately identified and managed the risks associated with aging–with operating these aging information systems.

More specifically, we found there were limited factors used to determine the risks of continued use of these systems. Without considering more extensive risk factors, some of the current risk ratings could be either under- or overstated.

We found there's no centralized monitoring of risk assessment results. This is a missed opportunity to identify causes of risk across all departments and take a system-wide approach to risk mitigation. We also found limited involvement from the departments in assessing the risks of the systems they use and in verifying the accuracy of the information systems' inventory.

My report includes eight recommendations to help the Province improve risk assessment processes and reduce the probability of adverse impacts to information systems. My report includes the department's responses to my recommendations and indicates that management is aligned with the recommendations in principle.

I'd like to thank digital technology solutions and the departmental management and staff we worked with for their co-operation and assistance on this project. Also like to thank my audit team for their hard work.

With respect to the privileged access report, Mr. Chair, information systems help the Province deliver a wide range of services, including health care, online registrations, provincial program applications and fee payments. These systems contain a considerable amount of personal, health and corporate information, making them a target for cyber-threat actors.

The Province relies on privileged users, also known as system administrators or superusers, to oversee these information systems. Privileged users have more privileges and authority than general users. They can perform activities such as adding and removing users, modifying privileges, changing system configurations and security settings and altering data tables.

Cyber-threat actors specifically target privileged users with the intention of taking control of information systems. An unauthorized individual with privileged access could potentially steal data or funds, disrupt operations or cause a system outage. As a result, government standards mandate additional controls be applied to protect privileged access accounts.

In my report, privileged access, information systems, we found the Province is not adequately controlling privileged access rights to prevent unauthorized access to information systems. In previous reports issued by my office, we've noted issues regarding poor controls and a lack of monitoring of privileged activities. Unfortunately, we continue to identify similar issues in this report.

This report contains five recommendations to help the Province strengthen privileged access controls, and I'm pleased that the department and Shared Health agree with the recommendations and are committed to resolving the issues we identified.

In conclusion, again would like to thank the management and staff from the department as well as from Shared Health, for their co-operation and assistance during this audit, and I'd like to thank my audit team members for their dedication and hard work.

I look forward to the discussion today.

Mr. Chairperson: Does the deputy minister wish to make an opening statement, and would he please introduce his staff joining him here today?

Mr. Joseph Dunford (Deputy Minister of Consumer Protection and Government Services): My opening remarks will cover both reports as well.

* (13:10)

My name is Joe Dunford. I'm the deputy minister for the Department of Consumer Protection and Government Services. With me today is Hong Chung, the Province's Chief Information Officer and lead for Digital and Technology Solutions, or DTS.

And also with me is Ann Leibfried, the acting executive financial officer for the department.

First off, I would like to thank the Office of the Auditor General for the work on both reports. Consumer Protection supports and protects the

interests of Manitoba's consumers, citizens, business people, landlords, and tenants.

Government Services is responsible for the modernization of government services, including procurement, IT, capital planning, project delivery, and asset management for government's vertical and underground infrastructure.

DTS is Manitoba's central organization for IT systems and services, including cybersecurity. These information systems support a wide range of government programs.

In 2022, the Auditor General released two information system reports: Aging Information Systems; and privileged access. Both audits highlighted opportunities for improvement to mitigate operational risks linked to underlying information systems.

The department accepts and agrees with the recommendations in both reports and has begun implementation of the actions to address the findings.

Since the release of the Aging Information Systems audit report, the department has developed an action plan to address the recommendations outlined. Furthermore, many of the items have been completed or are in progress and targeted for completion within the fiscal year.

The department has updated its IT–or, ICT standards used as the basis for technology risk rating; updated ICT standards and application portfolio assessment processes to better align with the annual budget cycle; updated the classification framework for determining system risk, including the addition of stakeholder impact; updated the application portfolio management process to include increased stakeholder engagement; increase governance to reduce risk of errors, and frequent reviews to keep information relevant, and begun exploring automated systems and tools to improve existing processes.

The report identifies concerns with the limited distribution to stakeholders and the lack of a combined ICT asset condition report spanning all departments.

While the department agrees increased collaboration with stakeholders is important, due to the sensitivity or sensitive nature of the information contained with the ICT asset condition reports, authorized stakeholders receive only the information relevant to their programs.

Since the release of the privileged access report in October of 2022, the department has developed an action plan and has taken steps to increase controls for privileged access to reduce cybersecurity risk.

The department has updated the process to regularly verify each privileged access is necessary and authorized; initiated the development of an automated process to more tightly couple human resource events to the removal of privileged access; initiated an assessment to enhance privileged access, logging, monitoring and event detection with increased automation using the Province's security information and event management tool or sign; initiated a plan to introduce new automated privileged access management tools; initiated a privileged access policy review and initiate a planning to increase awareness and training efforts.

While the department agrees with the recommendations in both reports and accepts them, we are also cognizant that there are both technology limitations and dependencies on human input that will prevent the complete elimination of errors.

The department's approach to managing information systems' policies, prioritization and investments is based on a risk management framework and balances the business risk with the financial and operational costs. The framework continues to evolve and the department will collaborate with stakeholders to better define, refine and roll out across the province.

We also recognize the technology and cyber landscape continues to evolve at a rapid pace, and a cyber threat environment is far from static. To adapt, the department will continue to build upon the actions presented today and in the report to further reduce and mitigate current and new threats.

Given the sensitive nature of the topics being discussed today and the potential implications to cybersecurity, we may not be able to go into specific details when answering some of the committee's questions.

Lastly, I would like to thank the Office of the Auditor General for their efforts at helping us improve our controls and mitigate risk resulting from information systems. Hong and I look forward to the opportunity to respond to your–to any outstanding questions you have today.

Thank you.

Mr. Chairperson: Thank you.

Does the CEO for Shared Health wish to make an opening statement, and would she please introduce her staff joining her here today?

Ms. Lanette Siragusa (Chief Executive Officer, Shared Health): Good afternoon, and thank you for having us here today to present and respond to questions related to Shared Health's completed and ongoing work related to the October 2022 OAG Report on Information Systems, Privileged Access.

I am Lanette Siragusa, chief executive officer of Shared Health, and I am joined today by Doug Snell, chief operating officer of Digital Shared Services for Shared Health.

I would like to thank the committee for the opportunity to provide comments and respond to questions, and offer our thanks to the office of audit professionals. I want to acknowledge their professional and collaborative relationship with Shared Health and our staff.

On behalf of Shared Health, I want to acknowledge the findings and recommendations contained within the audit report. I will speak to the status of our response to a number of specific recommendations today, and both Doug and I look forward to the opportunity to respond to any outstanding questions you may have.

But first, I would like to offer a bit of background about Shared Health, the organization. Shared Health was formed in 2018, envisioned as a collaborative entity that would lead and co-ordinate the planning of patient-centred care across Manitoba, with an end goal of improving access, reliability, quality and equity of health services for all Manitobans.

As Manitoba's only provincial health authority, we also support a wide variety of centralized administrative and business functions for all health organizations throughout our province. This includes support for provincial technology services. In this function, digital shared services, led by Doug Snell–who is with me today–supports the digital systems for health organizations across Manitoba.

The audit report covers a period from January 2018 to March 2022. During this time frame, Shared Health and Digital Shared Services were in their formation, with information technology staff, infrastructure and services transitioning from a number of individual organizations into Shared Health to form a new operating entity and shared services model.

Throughout these transition activities, including both the audit interval and in the time since its conclusion, Shared Health initiated cybersecurity improvements to streamline processes and standards across the health infrastructure. This work included a number of initiatives that address findings within the scope of the privileged access report.

In our provincial role, Shared Health collaborates with the departments of Labour, Consumer Protection and Government Services, digital and technology services on forward-looking plans, opportunities for alignment and standards on matters of technology, procurement and cybersecurity. The report on Information Systems–Privileged Access lists five recommendations, which I will now go through individually, identifying the status of our organization's response to each.

Recommendation No. 1: We recommend that Shared Health prepare a list of authorized officials who will approve access to applications, grant access only after validating access approval from the authorized officials and retain the access approval documents.

Status: Shared Health has implemented improvements to the processes and updated standards to reflect the recommendations, including maintaining a centralized list of authorized individuals who can approve access to applications, compliance processes, access standards and records retention practices.

***** (13:20)

Recommendation No. 2: We recommend that Shared Health investigate and implement automated solutions to improve management of privileged access and integrate access removal processes with human resources, to remove users promptly.

Status: Shared Health is actively deploying automated solutions and operating procedures to improve the management of privileged access across the provincial infrastructures. Completion of this work is anticipated to occur in the second quarter of 2023.

Shared Health is also collaborating with human resources to improve the integration of processes and technologies to remove user access promptly. Targeted completion of this work is fourth quarter of 2024.

Recommendation No. 3: We recommend that Shared Health regularly review all privileged users to verify their access rates align with job responsibilities and to ensure unauthorized privileges do not exist; remove unnecessary access promptly after the review, and retain the access rights review documents.

Status: Shared Health has operationalized a quarterly management review and compliance audit

process of all privileged access, including any adjustments to access as required, and retention of access rights requested documentation.

Recommendation No. 4: We recommend that Shared Health implement the identification and authentication standard and control recommendations presented in our letters to management.

Status: Shared Health is actively implementing the recommendations to address the findings to align to published standards and control recommendations. No additional resource is required or identified at this time.

And recommendation No. 5: we recommend that Shared Health log all privileged user activities; determine and regularly review risky activities and, where not already implemented, investigate methods to automate privilege user monitoring, including alerts of activities that should be reviewed.

Status: Shared Health is actively deploying automated solutions to log all privileged user activities including provisioning, elevation of privilege, alerts for activities requiring review and procedures to conduct reviews with an anticipated completion in quarter four, 2023.

We are now prepared to take questions on administrative-related items posed by the committee. We will endeavour to answer any and all inquiries here today. However, note that some questions may need to be taken as notice, in which case, we will provide a specific response in writing.

Questions may be directed to either or us; however, Doug is most familiar with the audit findings and field of discussion related to privileged access.

Doug has initiated the improvement projects to address the findings in the audit, and actively collaborates with the Department of Labour, Consumer Protection and Government Services on matters related to infrastructure, technology, procurement and cybersecurity standardization. He's able to take questions from committee members and to assist me in answering–in providing answers.

That's it.

Mr. Chairperson: Thank you.

Before we proceed further, I would like to remind the committee of the process that is undertaken with regard to outstanding questions. At the end of every meeting, the research officer reviews the Hansard for any outstanding questions that the witness commits to provide an answer to, and will draft a questions-pending response document to send to the deputy minister.

Upon receipt of the answers to these questions, the research officer then forwards the responses to every PAC member and to every other member recorded as attending that meeting.

I would also like to remind members that only questions of an administrative nature are to be placed to the witnesses and that policy questions will not be entertained and are better left for another forum.

The floor is now open for questions.

MLA Tom Lindsey (Flin Flon): Sorry. Trying to operate off a phone, because I'm really remote today; I'm up in Thompson.

So, my first question is in relation to the aging information systems audit. We know that there's a number of issues there, and part of the audit was to do the proper assessment to determine what were the highest risks, where they were and what the recommended changes would be.

So, I guess my first question is: Has that risk assessment been completed, or how far along in the process is it? And has this risk assessment resulted in any changes?

Mr. Dunford: Thank you for the question.

So, that risk assessment has been completed. It will be one that will continue to be ongoing, as well. There was items in that that we found that we have addressed since, so there's certain programs that we closed down or systems that we've had to deal with, without getting into specifics.

But yes, we have done that assessment.

Mr. Chairperson: Mr. Lindsey, would you please unmute your microphone.

MLA Lindsey: Sorry about that, thought I had.

So, you were saying that the risk assessment is completed and some issues have been addressed.

So, through this system, the–I'm assuming there's multiple different information systems used by different departments. Is there a move to reduce the number of those systems to integrate them into one system? Is that already, kind of, the process?

And you have some outstanding issues identified in the risk assessment. Could you tell us what the status is as far as mitigating those risks?

Mr. Chairperson: The deputy minister. *[interjection]*

Mr. Chung.

Mr. Hong Chung (Chief Information Officer, Province of Manitoba): Good afternoon.

So, yes, there are multiple systems, as you've identified. There are hundreds of systems within our government environment. Each will have its own individual risk profile.

So, the–we are working through the assessment and the report that came out of the assessment, and part of the strategy is to look at each individual asset and determine what the best action of approach is–or, the best approach to take is. In some cases, it's mitigating the existing risk based on some information and findings that we've uncovered. In other cases, it will include some migration, which means replacing to other, more modern technology.

***** (13:30)

And in many cases, we are looking at opportunities for us to consolidate and rationalize our applications.

Mr. Len Isleifson (Brandon East): I'm looking more at the process of shared network infrastructure. And I would understand that, if a report came in and it looks like it comes in on a regular basis, that there may be something that is creating risk within the IT infrastructure.

I'm wondering–and I know we only have two departments here–but, how does it process so that we can be sure that every single department that is using shared infrastructure is aware of the risk, and how do they respond? Is there communication among departments through the IT process to ensure that everything has been addressed in each department so that one doesn't get overlooked?

Mr. Chung: Shared infrastructure is managed and monitored centrally. So, within my organization, within digital technology solutions, we do look at what applications and what departments are impacted by the underlying technology and, based on that assessment, we do have communication processes to inform and collaborate with the impacted departments.

Mr. Isleifson: So, just a quick follow-up, then. So, with that process coming out, how often and how wide are the reports released–through the Chair–how widely informing are the reports released from the IT department so that everybody stays on that page and keeps a look at–out for adverse effects that might happen within their departments?

Mr. Dunford: These reports come out on ad hoc and annual basis. So ad hoc, as needed, if there's certain event of some sort, they would come out.

In terms of their spread and their reach, the reports be very specific–the reports that our department gets will be very specific to them. For obvious security reasons, we want to make sure it's all compartmentalized for specific departments and that all of that broad knowledge is not spread everywhere for access. Okay?

MLA Lindsey: We're talking about aging infrastructure, particularly the IT infrastructure, and how to modernize it or ensure that things aren't being missed.

One of the issues that comes up often in Flin Flon–because it's a border town and people from Saskatchewan get their health care at the hospital clinic in Flin Flon, Manitoba–but the computer systems between the two provinces don't talk to each other. So, when people have to go to a specialist in Saskatoon or a PA, they land up having to take their files in paper in shared vehicles with other people and chances of it getting lost are increased and the wrong people looking at the personal information.

Is there any part of this process that would look at how to integrate interprovincial systems so that they're able to talk to each other, so that people don't have to carry paper files anymore?

Mr. Dunford: Thanks for your question.

In considering this one, this one does appear to be a little bit outside of the scope of the audit; but in saying that, you know, we work with the health authority any of these matters, and we'll continue to do so.

So, if there is a specific example here that–to be looked at, it would be probably best addressed outside of this audit today, or the hearing for this audit today. Doesn't seem to fit with the scope of it.

MLA Lindsey: Okay, well I certainly appreciate if someone could look into it if it's outside the scope of this audit, because it is an ongoing issue that people up there go through on a regular basis.

So, I guess to get back specifically to the audit then, one of the things that we're looking at is the collaboration with departments in assessing the risk for your IT assets, and pretty important that that all takes place.

So, has there been a change in the process on how to collaborate with the departments, and are there some roadblocks that you've identified in that collaboration process to ensure that the risk assessments can be done in a timely manner?

Mr. Chung: There have been updates to the process, which include deeper collaboration with the departments involved.

In terms of roadblocks, this is a new process for our organization as well as the departments, and most of the roadblocks are just related to helping people get up to speed and comfortable with the new process. No technical or no other roadblocks have been identified.

Mr. Dougald Lamont (St. Boniface): Thank you for coming today and presenting. I just had a couple of questions.

On a couple of the recommendations, several of them actually, there are challenges, and the response from Shared Health was–well, the recommendations are focused on former regional IT programs; responses to the recommendations must consider the standardization of a provincial IT program requiring additional funding and resources to implement and maintain.

So, you've–they've expressed that concern. I'm just wondering how that is impacting. Is it still the case that there are challenges with additional funding and resources in order to be able to achieve these goals?

Mr. Doug Snell (Chief Operations Officer, Shared Health–Digital Shared Services): Thanks very much for the question.

And at the time that the audit was ongoing, there was a number of items of discovery that we were still working through with the cybersecurity program.

Since that time, we've done the analysis and we don't require any further resources at this time based on the efficiencies we were able to extract and the standardization. It was just an unknown at that time.

Mr. Lamont: Just wondering when–there are a couple of areas under recommendation five about–and recommendation four, that the departments weren't agreeing with a blanket approach.

So, can you just elaborate on what you mean by what the challenges were around implementing a blanket approach, and how the departments are planning to, sort of, I guess, achieve what the Auditor General has set out without taking a different approach, taking a non-blanket approach, I guess.

***** (13:40)

Mr. Dunford: Thank you for the question.

Our comment on the blanket approach really had to do with the life cycle of a program and where it is. You know, some programs could be very new, very recent and more advanced in terms–far along in terms of where they are, whereas some other ones we might have could be a little bit older and much further along in terms of their age–the age of their system.

So, as a result, a blanket approach, because of technology limitations within those programs, is a little bit more difficult.

I mean, obviously, we accept this recommendation, but we have to acknowledge that, at times, we will encounter some of those technology limitations as well.

Mr. Martin: Again, thank you for attending and participating in this.

One of the comments–and this should be a very quick answer–but notes–in reference to recommendation No. 2 about implementation of automatic–automated solutions–notes that completion of this work is anticipated to occur in the second quarter of 2023.

Just a quick question, are we talking about the fiscal year or calendar year?

Ms. Siragusa: Fiscal. Fiscal year.

Mr. Martin: Thank you very much.

One of the situations I think that we're all facing, especially larger organizations, is the rise in the use of AI, artificial intelligence, when it comes to–whether it's ransomware, phishing or any number of cyber-led attacks.

So, I guess my question is: What is your level of confidence in your ability to identify new and emerging threats and, as well, whether or not you feel you have the necessary resources–because a lot of this is new and developing technology and, let's be honest, technology can be expensive and that–so, whether or not you feel you have the necessary resources to

address these new and emerging threats that have become highly sophisticated, to say the least.

Mr. Chairperson: Mr. Dunford–Mr. Chung.

Mr. Dunford: Sorry, this'll be a–oh. Go to Hong first.

Mr. Chung: As you correctly pointed out, this is an evolving space, and emerging technology does have implications on our processes and systems. And to keep up with it, we do continue to evolve our processes as well, as well as our technology.

Ms. Siragusa: I'm going to have Mr. Snell respond.

Mr. Snell: Yes, concurring with my colleague, it's an evolving space. As you point out, there are emerging threats. We work with partners to get the best information we can; however, programs–as Mr. Chung had mentioned–evolve day-to-day, week-to-week, and, in response, we put plans in place to mitigate or manage those risks internally.

The work we do is largely around evolving the practices that we have and the processes to manage the internal risk and administrative controls. Technical controls and the partners we work with evolve over time based on the persistent threats that we see in the environment, as was witnessed through COVID.

Mr. Brad Michaleski (Dauphin): Thanks, everybody, for coming here today.

My question–first question–relates to recommendation No. 5, the explanation that was given by Ms. Siragusa, and I appreciate the responses to all the recommendations that you provided. But my question is regarding deployed automated solutions. And, I'm not an IT professional by any means or familiar with these systems, but, you know, I understand these systems can help tremendously in, sort of, data management and efficiencies of management.

So–and you may not be able to answer–but my question is how–like, this software–and I think it was maybe mentioned–this is developed in-house constantly? Or is this–and you mentioned partners, so, can you elaborate a little bit more on that? On, like, is this plug-and-play stuff that you guys are buying and incorporating or are you developing and how does that work? And what is the, sort of, the legacy costs, management-wise? Is there–if you can elaborate a little bit more on that.

Mr. Snell: Thank you very much for the question.

Yes, so, it's really broken into two items. So, there's the processes and practices that we have which evolve, and that's part of the work that the Office of the Auditor General is doing. Those change over time, and we adjust our processes and practices.

And then, with respect to software to log–with respect to finding No. 5–or, recommendation No. 5–those are–again, that market evolves over time, so what was available last year, new systems are on the market. Those are typically commercial solutions.

There's configurations we put in place for our environment and, in our case specifically, in order to implement at scale, we've made decisions around partnering with the commercial solutions in order to maintain standards and capabilities for rapidly deploying and evolving with the needs of the marketplace.

Mr. Michaleski: Okay, so just a–then, a follow-up. Again, you said the commercial–this a commercial market that you're accessing and playing around in to help you develop your–incorporate what we're doing.

So, again, there's some legacy management issues in terms of proprietary software, things like that. You know, I'm–I don't know, I–if I'm off-track or not, but is there these costs–and how secure, then, are these technologies that you're adopting, and like, maybe that's part of what you're buying, is the ability to put in your own security.

***** (13:50)

So, is–like, how really secure is this? And what is being done–you know, I think it's been answered that there's processes in place to make sure people have heightened, sort of, emphasis on access–you know, how are we making sure and ensuring that the systems are secure?

And then, also, the users are being–I understand that's generally what the audit is talking to, but–again, I–my concern, generally, is incorporating software–commercial software. And you know, the liabilities, I guess, for the Province or for your department on maintaining these operating systems and updating, and those types of things.

Mr. Snell: Sorry. If I understand the question correctly, really it's about the management of risk with respect to solutions that we have in place, processes that we manage and operate.

In our case, in order to not only follow up with audits such as this and determine the achievement of the recommendations and the findings, as well as the management of risk, we engage–sorry, we engage

third parties to–third-party audit professionals to assist in the evaluation of the risk on those programs.

MLA Lindsey: So, looking at some of the reporting and how it works, it was noted in the audit that there was no input controls in–regarding the supporting technologies, and it noted there were several errors in how the risks were assigned.

In one case, certain application was deemed to be yellow–medium risk, when in fact, according to ICT standards, that operating system was already under the retirement phase, which had led it to be–should have led it to be classified as red.

So, I guess, who checks the information that's being inputted into your risk system? Who checks that information to ensure it's accurate, in a timely fashion, so that you're getting the best reporting, so that you can do the best mitigation practices?

Mr. Chung: Thank you for the question.

As part of the work that we've done recently in response to the audit, we have updated our processes and governance. And that governance includes peer reviews, management reviews, as well as stakeholder reviews.

And that'll help us mitigate and minimize any errors as a result of the–or, any errors in the system.

MLA Lindsey: Could you just explain a little bit about how the system works when you're doing things across multiple departments?

If one department identifies it a certain way, another department identifies it somewhat differently based on the information they have, that there has to be some system to ensure the right balance and how those assessments are determined.

And is part of the problem the personnel, ensuring that it's the same personnel or the right personnel continuing through the assessment process? Does change in personnel affect what someone determines is a high risk, low risk or medium risk.

Mr. Chung: Thanks for the follow-up.

The process also includes the introduction of a new classification framework which does include both the technology and support element, as well as a business impact elements.

From a technology perspective we do look at each system on an individual basis as we–and we look at not just the application itself, but the various components that are required to support that application.

We do store the information in a system and the way the process is defined is that the technology teams and my team would be responsible for leading the work–leading the analysis from a technical perspective and we would engage the business stakeholders on the business side of things.

And if an application supports multiple business stakeholders we would bring that collectively in and that would actually assist in the weighting of the risk, right? So if multiple departments are using the same application that would then, in practice, raise the business impact of that application.

Mr. Martin: And I'm cognizant, obviously, about your earlier comments about sharing certain information and that. But one of the most fundamental and easiest actions that any one of us can do, obviously undertake, when we're dealing with issues of cybersecurity, is backup.

Now, the issue comes that often we don't personally and organizationally often check our backups until the time is needed. So, without getting in too much detail, again, for obvious reasons, I'm just looking for assurances that you're confident that the systems are in place, that the data is backed up should the need arise for a–if the system is compromised in such a way that backup is required. And if it isn't, if the necessary backup isn't available, why isn't it?

Mr. Dunford: Thank you for your question.

The question, as I understand this, really what you're referring to is data centres and that type of backup system. For the scope of this audit that would be outside of this, so if you did want to get some information on that, it would be something that we could address outside of this Chamber.

Mr. Martin: Thank you very much for that question.

The other question I have is specifically more to the health department, as we're obviously dealing with a lot of personal–potentially a lot of personal information. I'm just curious: what are the–when a situation occurs, such as, you know, ransomware or some sort of cyberattack in which a–which individuals' personal data may have been accessed now, what are the protocols in terms of alerting those individuals or alerting, you know, the public at large that there has been a data breach and what actions and undertakings that they can take personally to protect their data and then, as well, protocols within Shared Health as to

what actions they would undertake after the effect to protect people's data and personal information?

* (14:00)

Mr. Snell: Thank you very much for the question.

The scope of the privileged access audit for Shared Health didn't include matters of privacy; this is a matter of privacy in the legislation. However, you know, if that needs to be taken on advisement or notice, we can certainly follow up after.

Mr. Lamont: I just had a question related to, I guess, the security when it comes to potential travel abroad or department officials with privileged access bringing IT assets, whether it's government phones or laptops, where security might be compromised.

So does the department have–or do the departments have a way to track the travel of IT assets or ensure that if anybody has something of an aging asset that there is that extra level of security when travelling abroad or even travelling domestically?

Mr. Dunford: Thanks for the question.

Yes, we do have processes in technologies to enable us to track any government-owned assets as they travel, yes.

Mr. Lamont: Just a question around recommendation 3 in audits: You've implemented a quarterly management review and compliance audit process of all privileged access. Can you just talk a bit about how that audit works? I mean, is it all top-down or are there ability–do people have that capacity to also register that there's an issue or red-flag an issue if they're in a department? Are the people able to report complaints like that as part of the audit–outside of the audit process as well?

Mr. Snell: Thanks very much for the question. This–assuming it's for Shared Health, given the response.

So, in answer to the question, the process that we go through is on the provisioning and approval side first. So, there's a request, there's only three executive directors that have access to the approvals in our organization, and they can only delegate laterally or up.

And once those approvals are met, that approval includes also what the access is for, limited to the scope of the applications and the work required by that individual for the time required for that individual, and then we do quarterly audits to make sure that any revocation or the timely removal of inappropriate access is dealt with.

Mr. Chairperson: Mr. Lindsey. Mr. Lindsey, you need to unmute your microphone.

MLA Lindsey: It seems that the IT asset condition reports have limited distribution and lack of sufficient risk information that would make it hard for everybody to be able to use the report properly. Plus, I understand that these condition reports are not necessarily always released in a real timely manner so people can take the appropriate action when they need to.

So, perhaps you could just tell us what the game plan is to rectify those two conditions that have been identified.

Mr. Dunford: The comment around timeliness of the reports, so, there was two aspects of that. One is–so, we will be producing these reports on an ad hoc basis, as needed. The other piece had to do with, if you look at the audit, had to do with lining up with our budget cycle. So, we have rectified that as well. That was a comment around timeliness in that.

As for the distribution of the reports and the information that's in them, that's one where–I spoke to it a little bit earlier in that the distribution does have to be limited. It has–be to the departments, key people in the departments, but obviously, for security reasons, there's a reason why those are limited in their distribution as well as the information that's in them has a–very specific to the department, for security reasons, obviously.

MLA Lindsey: So, thank you for that.

So, now, to–for me, anyway, I realize others have got there before me–just talking about the access–privileged access. So, we know that the auditor has identified that the Province is not adequately controlling privileged access rights. So, there's actual staff that have these access rights. There's also vendors that have privileged access rights.

So, could you just briefly give us a–I guess, a high-level snapshot of what is in place, what system is in place to ensure that only the right people have that privileged access, and that is it isn't too broadly given out, recognizing that there's vendors and others that would have that access.

Mr. Chung: Thanks for the question.

So, first off, we are, as the Auditor General had recommended, we are updating our provisioning and de-provisioning processes for privileged access, more tightly aligned with our HR processes. So, when

there's a change in staff or a change in–like a movement in staff or departure of staff, we will be able to more promptly remove that access. So, that's the first thing.

In addition to that, there are still approval processes that are required before somebody can get access to a privileged access account, which requires both the department that's asking for the access to approve as well as the central–like, so–as well as my organization to approve.

And lastly, similar to what my colleague at Shared Health had talked about in terms of their audit process, we are implementing–we have updated our process to implement something very similar, which will utilized to catch anything that might have been missed throughout the processes.

* (14:10)

Mr. Michaleski: On–in the aging information system of February 2022 report, on page 6 and 7, it talks about BTT–but I know that's not the right term–but they produce asset reports which are sent to departments to be considered as part of a department IT demand planning. So, the language there is, it's produced and it's to be considered but not required.

So, my question, then, is two part. Is this–is there no assurance, then, that government has integrated control of operating systems and that they're working together?

Because I think the basis of this report and a number of reports is questioning the control, on a number of levels, of management. And–case, I think, with Shared Health, we're talking about 2018 is sort of the start of a new model–operating model, so prior to is raising a lot of questions about just how the system was functioning.

So, is there no assurance, now, that the government has integrated control of operating systems, and that they work together?

And number two, then, the Auditor General has referenced this move towards centralized–central monitoring. So, is this also sort of a catch-all that's being incorporated into, let's say, the shared–I can't use the Shared Health model because I think that centralized thing is meant to cross all departments. So, is that–what's the status of that as well? And is that a–you know, a major component of the transition that's going on right now, is incorporating centralized monitoring?

Mr. Chung: So, I'll answer the two questions directly.

So, the integrated controls question related to the demand plan, the annual cycle and the inputs from the departments. So, we do–as part of our updated process, we do engage and we will engage, continue to engage with department stakeholders on an annual basis to understand the risk of the specific system, and share that risk with them. And based on their inputs–and our inputs–will prioritize and action accordingly. So, it is integrated from that perspective.

As related to the central monitoring question, within the government we do centrally manage IT for–I mean, there's some exceptions, but we manage–essentially manage IT. And because of that we are able to leverage the central controls–or, central monitoring that you're talking about, in terms of understanding how systems are accessed. And it'll actually create more synergies for us to further enhance our solutions as we roll out more evolved technology and processes to further mitigate risk.

Mr. Michaleski: No further questions.

Mr. Chairperson: While I–we're all here, I would like to know whether–Mr. Chung, whether you could arrange a meeting of the PAC committee over at your offices.

I assume you have the same offices you had many years ago, where you have all the IT systems over there, and you can give us a presentation on what the functions are of each, you know, SAP, you know, all the updates and so on, about these things.

Is it possible for you to do that, just for the members of the PAC committee?

Mr. Dunford: We'll be happy to accommodate that request.

Mr. Chairperson: Okay, thank you very much.

Mr. Lamont: I'll just–just one other question. It's on recommendation 2, the recommendation Shared Health integrate access removal processes with human resources to remove users promptly.

I see that Shared Health is collaborating with human resources to improve the integration of processes and technologies. Targeted completion of this work is fourth quarter of 2024.

So you can just–I mean, that is 18 months from now. I'm just wondering, is–what's happening in the interim, in order to be able to make sure that user access is removed promptly, and is this simply the automation aspect of it that's being broadened?

Mr. Snell: Yes, thank you very much for the question. So, correct: Right now we have integrated processes, and we get reports from HR as timely as they can provide us. What that is talking about is the targets date, where we have integration into the HR systems and payroll, so that we can get notified as soon as there's action on those systems to automate the removal of that access.

Mr. Lamont: That's it, thank you.

Mr. Michaleski: Just one final question. And it refers to the move in 2018 that Shared Health–and we're moving into a different system.

So, where is–is Manitoba carving its own path, or where are we relative to other provinces in Canada?

Mr. Snell: Thank you very much for the question.

Unclear at this time how that question relates to the scope within the privileged access audit for Shared Health, but would be happy to take the question away on notice for follow-up.

***** (14:20)

Mr. Chairperson: Are there any other questions? No more questions?

Hearing none–hearing no further questions or comments, I'll now put the question on the report.

Auditor General's report titled Aging Information Systems, dated February 2022–pass.

Auditor General's report titled Information Systems–Privileged Access, dated October 2022–pass.

The hour being 2:21 what is the will of the committee?

Some Honourable Members: Committee rise.

Mr. Chairperson: Committee rise.

COMMITTEE ROSE AT: *2:21 p.m.*