Legislative Assembly of Alberta

The 29th Legislature
Second Session

Standing Committee
on
Public Accounts

Service Alberta

Tuesday, May 24, 2016
8:30 a.m.

Transcript No. 29-2-4

Legislative Assembly of Alberta
The 29th Legislature
Second Session

Standing Committee on Public Accounts

Fildebrandt, Derek Gerhard, Strathmore-Brooks (W), Chair
Anderson, Shaye, Leduc-Beaumont (ND), Deputy Chair

Barnes, Drew, Cypress-Medicine Hat (W)
Cyr, Scott J., Bonnyville-Cold Lake (W)
Dach, Lorne, Edmonton-McClung (ND)
Fraser, Rick, Calgary-South East (PC)
Goehring, Nicole, Edmonton-Castle Downs (ND)
Gotfried, Richard, Calgary-Fish Creek (PC)
Hunter, Grant R., Cardston-Taber-Warner (W)
Luff, Robyn, Calgary-East (ND)
Malkinson, Brian, Calgary-Currie (ND)
Miller, Barb, Red Deer-South (ND)
Renaud, Marie F., St. Albert (ND)
Turner, Dr. A. Robert, Edmonton-Whitemud (ND)
Westhead, Cameron, Banff-Cochrane (ND)

Also in Attendance

Anderson, Wayne, Highwood (W)

Office of the Auditor General Participants

Merwan Saher	Auditor General
Eric Leonty	Assistant Auditor General
Patrick Dunnigan	Principal
Mary Gibson	Business Leader, Systems Audit Practice

Support Staff

Robert H. Reynolds, QC	Clerk
Shannon Dean	Law Clerk and Director of House Services
Trafton Koenig	Parliamentary Counsel
Stephanie LeBlanc	Parliamentary Counsel and Legal Research Officer
Philip Massolin	Manager of Research and Committee Services
Sarah Amato	Research Officer
Nancy Robert	Research Officer
Corinne Dacyshyn	Committee Clerk
Jody Rempel	Committee Clerk
Aaron Roth	Committee Clerk
Karen Sawchuk	Committee Clerk
Rhonda Sorensen	Manager of Corporate Communications and Broadcast Services
Jeanette Dotimas	Communications Consultant
Tracey Sales	Communications Consultant
Janet Schwegel	Managing Editor of *Alberta Hansard*

Transcript produced by *Alberta Hansard*

Standing Committee on Public Accounts

Participants

Ministry of Service Alberta
Mark Brisson, Assistant Deputy Minister, Service Modernization
Tim Grant, Deputy Minister

8:30 a.m. **Tuesday, May 24, 2016**

[Mr. Fildebrandt in the chair]

The Chair: Good morning, everyone. I'll call this meeting of the Public Accounts Committee to order and welcome everyone in attendance. I'm Derek Fildebrandt, the MLA for Strathmore-Brooks and chair of the committee.

I'll ask members to introduce themselves for the record, starting to my right.

Mr. S. Anderson: I'm Shaye Anderson. I'm the MLA for Leduc-Beaumont. I'm the deputy chair of the committee.

Ms Goehring: Good morning. I'm Nicole Goehring, MLA for Edmonton-Castle Downs.

Ms Miller: Good morning. Barb Miller, MLA, Red Deer-South.

Mr. Dach: Lorne Dach, Edmonton-McClung.

Mr. Westhead: Cameron Westhead, Banff-Cochrane.

Dr. Turner: Bob Turner, Edmonton-Whitemud.

Ms Renaud: Marie Renaud, St. Albert.

Mr. Malkinson: Brian Malkinson, MLA for Calgary-Currie.

Ms Luff: Robyn Luff, Calgary-East.

Mr. Gotfried: Richard Gotfried, Calgary-Fish Creek.

Mr. Fraser: Rick Fraser, Calgary-South East.

Mr. Brisson: Mark Brisson, Service Alberta.

Mr. Grant: Tim Grant, Deputy Minister of Service Alberta.

Ms Gibson: Mary Gibson, business leader, systems audit practice, office of the Auditor General.

Mr. Saher: Merwan Saher, Auditor General.

Mr. Leonty: Eric Leonty, Assistant Auditor General.

Mr. Dunnigan: Patrick Dunnigan, audit principal with the Auditor General.

Mr. W. Anderson: Good morning. Wayne Anderson, MLA, Highwood.

Mr. Cyr: Scott Cyr, MLA, Bonnyville-Cold Lake.

Mr. Hunter: Grant Hunter, MLA, Cardston-Taber-Warner.

Dr. Massolin: Good morning. Philip Massolin, manager of research and committee services.

Mrs. Sawchuk: Karen Sawchuk, committee clerk.

The Chair: We may also have Mr. Barnes joining us via teleconference. I guess we'll hear him if he dials in.

A few housekeeping items. First, microphone consoles are operated by *Hansard*, so there's no need to touch them. Audio of committee proceedings is streamed live on the Internet and recorded by *Hansard*, and you can access the audio and transcripts via the Legislative Assembly website. Please turn your phones to silent as they may interfere with the audiostream and annoy us.

Are there any additions or changes to the agenda as distributed? Seeing none, would a member move that the agenda of the May 24, 2016, meeting of the Standing Committee on Public Accounts be approved as distributed? Moved by Mr. Malkinson. Discussion? All in favour? Opposed? Carried.

Do members have any amendments to the April 12 minutes as distributed? Seeing none, would a member move that the minutes of the April 12, 2016, meeting of the Standing Committee on Public Accounts be approved as distributed? Moved by Mr. Westhead. Discussion? All in favour? Opposed? Carried.

I would like to welcome our guests from Service Alberta here today to speak to the IT disaster recovery program, which the Auditor General addressed in his October 2014 report. Members should have the committee research document, the Auditor General briefing document as well as the updated status of the Auditor General's recommendations submitted by Service Alberta.

We'll begin by inviting ministry officials to provide opening remarks of 10 minutes or so, and we'll turn it over to the Auditor General for his comments. The remaining time will be offered to committee members to ask questions.

Please go ahead.

Mr. Grant: Thank you, Mr. Chair. The events of the past few weeks have reminded us of the importance of disaster planning. Albertans need to be confident that government services will be there when they need them. I'm pleased to be here today to provide an update on what Service Alberta has been doing to improve our disaster recovery plans within our core IT infrastructure.

First, some background. In 2009 the office of the Auditor General first called attention to issues regarding disaster recovery processes. Service Alberta took immediate action in response. We developed an IT disaster recovery framework to assist departments in developing their own IT disaster recovery plans that are consistent and effective. Included in that framework is a list of best practices, tools, guidance, monitoring, and reporting. We still maintain and fine-tune that framework to this day. Each ministry in the government of Alberta is responsible for developing and testing IT disaster recovery plans for their own critical applications, and all of their plans are based on our framework. Our ministry is responsible for maintaining the disaster recovery plan for the GOA's core IT infrastructure, that is located at the Neil Crawford centre in Edmonton, along with the John J. Bowlen Building, which is the backup data centre in Calgary. All in all, progress has been made.

At Service Alberta we've worked hard to promote crossgovernment co-operation and collaboration in an effort to continuously improve our IT disaster recovery capabilities. We do this by taking a leadership role in the government's IT disaster recovery, community of interest committee, and by participating in the provincial Alberta Emergency Management Agency exercises throughout the year.

I'm happy to say that the Auditor General has taken note of the progress we've made over the last several years, most recently with noting in 2014 that we had improved our disaster recovery plans since 2009. However, that 2014 report also had three more follow-up recommendations for us. One of the Auditor General's recommendations was to identify the actual period of time in which critical IT applications must be recovered. In other words, if those critical applications go down, what would be the objective or goal for getting them back up and running? In Service Alberta's IT disaster recovery framework developed in 2010, we noted that a critical application is one that must be returned to operation within 24 hours of the event of a disaster. In that same framework we also noted that vital applications were those that must be recovered within 72 hours.

Another of the Auditor General's recommendations was to identify the most critical IT applications across the GOA. We did this count during the large-scale government-wide test of IT infrastructure we conducted on January 8 of this year. Prior to the test we identified 212 critical applications across government. From a business perspective, business services cannot be provided when related critical application systems are down. To provide some perspective, that's 19.3 per cent of all applications across the entire GOA.

At the same time, we did a count of vital applications. We found there are 180 vital applications, representing 16.4 per cent of applications across government. With vital applications business services can still be provided, but overall response is significantly impacted.

In the other recommendation the Auditor General asked us to focus on ensuring the disaster recovery plans for critical applications had been tested and that there are adequate resources to activate those plans if they're ever needed. Service Alberta found that 70 per cent of the critical and vital applications had documented disaster plans and that 50 per cent of those plans had been tested during the last year.

Let me provide some more information on the January disaster recovery test conducted this year. The January test exercise was the first of its size and scope ever conducted across the GOA. Previously disaster recovery exercises were done by individual ministries within their own networks. Having migrated many shared assets, but not all, into one GOA enterprise IT environment, it was important to do a government-wide test. In January the Neil Crawford centre in Edmonton was taken completely offline to simulate a natural disaster. With it, we successfully transferred all services to the secondary data centre, the John J. Bowlen Building, in Calgary. Thanks to this test, we were able to identify some technical and communications issues that we're working on.

We've tentatively scheduled a follow-up test for mid-November, during constituency week, to make sure that those issues have been resolved. We picked constituency week because running a simulation at this time significantly reduces the potential impact on business and operations conducted in the Legislature, the individual ministries, and, by extension, Albertans in general. For that reason, we're also hoping we can make this an annual exercise and run the government-wide IT disaster recovery exercise the first weekend of the constituency week each November.

Looking ahead, we've got several other projects on the go related to this. We're currently developing new processes and procedures for communications and crisis notification. We've created a repository that contains disaster recovery planning guides, tools, templates to assist ministries with planning and to ensure consistency. We're also working with business and IT staff across government to find out if we can reduce the number of critical and vital applications so that in the event of disaster we can ensure we get things up and running in a more timely fashion.

In conclusion, it's critical that we regularly test our IT systems to make sure they're there when we need them. We also need to ensure both our planning and testing have minimal impacts on Albertans. In light of all that, we're working hard to meet the recommendations made by the Auditor General in 2014. It's a big task getting all the ministries together for a disaster simulation update and to maintain our disaster recovery framework, but we're proud of the work we've done so far. We're expecting to fully implement all three of the Auditor General's recommendations by April 2017.

Thank you for inviting me to speak today. I'd be happy to take any questions you may have.

8:40

The Chair: Thank you very much.

I'll give the floor now to the Auditor General for his comments.

Mr. Saher: Thank you, Mr. Chairman. Just a few brief comments. I believe this PAC meeting today should aim to get answers to the following three questions. First, if a disaster happened tomorrow, would the most important IT applications be restored within acceptable time frames? Second, do all of the critical IT applications have a tested disaster recovery plan? Three, who has the authority to identify the government's most critical IT applications and to ensure that they can be restored as needed? I believe the deputy minister in his opening comments has provided answers generally to those three questions, but I believe that the three questions are specifically important and are worth following through.

Thank you.

The Chair: Thank you very much.

I'll open the floor to questions from members. Please let me know if you have a question by raising your hand in our agreed-upon method.

If I could have Mr. Barnes introduce himself for the record, please.

Mr. Barnes: Okay. You bet. Drew Barnes, MLA, Cypress-Medicine Hat.

The Chair: If we could turn down the volume on Mr. Barnes. Sorry, Drew; it's not you.

Okay. We'll start. I've got Mr. Anderson, Ms Miller, and Mr. Gotfried. Any others to start? Mr. Dach. Okay.

We'll start with Mr. Anderson.

Mr. W. Anderson: Thank you, Mr. Chairman, and thank you, Tim and Mark, for your presentation. Much appreciated. I'm glad to see, in reading some of the briefing notes, that you've got a business continuity plan in place, but with all due respect I'm wondering: can you identify the actual disaster recovery team and who sits on that team? Who's part of that team? It goes to the question of the Auditor General regarding who has the authority to identify critical applications. Does that team, if it has been put together, consist of vendors and third-party contractors and other individuals? Could you please describe that team to me?

Mr. Grant: Are you talking about, if a disaster should take place, what team comes together to resolve the issues?

Mr. W. Anderson: Exactly. Who would be the team in place whether a man-made or a natural disaster happened to the technology infrastructure in the GOA? Has a team been identified? Is there a team lead, and if so, who does that team consist of? GOA people, third-party people, and vendors as well: have you included them?

Mr. Grant: I'll start high level, and then I'll let Mark give the details. When we did our disaster recovery plan crossministry in January, we brought together, essentially, CIOs from every department in government, so we had the people who were dealing with applications and with the IT infrastructure on a day-to-day basis. We made sure that all of them were sitting around the table, able to address any issues that came up. On an ad hoc basis for disasters it would be the CIO Council, essentially, that's led by Mark, and that would be supported by IT experts in all the departments.

I'll let Mark go into the more sort of granular answer to the question.

Mr. Brisson: There is a DR community of interest working group that consists of CIOs and other technical individuals across government. Those technical individuals are all GOA-related individuals. That includes our base Service Alberta core infrastructure group, that obviously has to stay up and goes to support all of GOA, and the CIOs across government from the various ministries that could be impacted by an individual test or could be impacted by the disaster that we were simulating during that time. It's a community of interest that is brought together at a time when we're doing either all government-wide testing, or, if individual tests are taking place, Service Alberta would work with those individual ministries for their ministry DR tests that are taking place.

Mr. W. Anderson: Again, my other question is: do you include anybody from outside the GOA like specific strategic vendors or third-party individuals who've had experience in this area?

Mr. Brisson: We would include vendors that are contracted to us that have a nondisclosure agreement as part of their contract because if they are delivering some of the systems on behalf of the government for us through a contract, they would be responsible for helping us either bring a system back up or complete that test. An example would be our hardware storage vendors. If, in fact, we're testing whether the storage stays up when we do a transfer from one data centre to another, they would be sitting with us side by side to make sure that the test was being done correctly, completely, and confidentially as well.

Mr. W. Anderson: Thank you.

The Chair: Mr. Gotfried had a follow-up on that point.

Mr. Gotfried: Yes. Thank you, Mr. Chairman. Just a quick question on, obviously, the use of the private-sector vendors, following up on Mr. Anderson's questions here. I also wonder if we're using any sort of benchmarking and best practices against the private sector. I was in the airline business for many years, where obviously there are operational issues, and there is virtually a hundred per cent backup and immediate switchover. Have you looked at any private models in terms of larger corporations or operational models that we could model after and perhaps learn from in terms of a disaster recovery program here that is maybe in some respects less operational, less critical but still important to Albertans?

Mr. Brisson: In all of the research we've conducted on disaster recovery planning and business continuity planning, we do include benchmarks with the private sector, trying to scale to an organization as large as the government of Alberta but also looking at the different business lines across government in the different ministries. We do benchmark across industry from an information technology context.

Mr. Gotfried: Thank you.

The Chair: I'll also just remind members that we don't need to use up all the time today. If we exhaust our questions, we can always end the meeting earlier.

I think that next on the list we have Ms Miller.

Ms Miller: Thank you, Chair. On pages 4 and 5 the report talks about ensuring that departments have updated business continuity plans. It seems to me that this plan would be similar in nature to what is needed in a disaster recovery plan. For our benefit can you explain specifically what the difference is between business continuity planning and disaster recovery planning?

Mr. Grant: I'll try and do my best. From my perspective, business continuity planning focuses on business plans, processes, and procedures, and they're really designed to ensure there's no disruption to an organization's ability to deliver essential services due to loss of resources or infrastructure. Disaster recovery planning is one of many pieces of business continuity planning and really focuses on, in our case, restoring the critical information technology services that departments would need to deliver those services.

Ms Miller: Thank you.

A small follow-up: how do the two plans work together?

Mr. Grant: As I said, disaster recovery planning is really a subset of business continuity planning. BCP really assesses critical services, including dependency between critical functions and IT systems. The information used to determine the criticality of those IT systems really helps you to build a business continuity plan. You have to have a way to address the loss of those IT services, and that is your business continuity plan. What are you going to do, first of all, to mitigate the loss, and how are you going to bring it back online?

Mr. Brisson: I think I can add to that as well. If, in fact, as part of a disaster one of the IT systems went down, that's when it obviously would be unavailable, and that's when business continuity would kick in. The disaster recovery will do an assessment of what happens with the IT system. At the same time, then, business continuity kicks in and one of the manual procedures that you may need to put in place for a short period of time to deliver your services if, in fact, that system is unavailable during that period of time. Does that help?

Mr. Grant: If I could add to that, a practical example would be the offices that I use in the Telus building on the 29th floor, where most of the ADMs are. If the power went out in the Telus building, it becomes a business continuity planning issue. How would I continue to exercise control over the department if I had no power on the 29th floor or can't access my offices? So part of the business continuity plan that we have is that I would relocate my office to another office in Service Alberta, in all likelihood to the Access Building, which is where most of the IT services are located, out in the east end.

Business continuity planning is not just in the case of a disaster. Little things could pop up, and we still have to figure out how we can mitigate whatever those interferences, influences are to make sure we can continue to deliver services properly.

Ms Miller: Thank you.

8:50

The Chair: We'll go to Mr. Gotfried.

Mr. Gotfried: Thank you, Mr. Chairman. It seems there's lots of experience in the past. We seemed to make it through Y2K fairly well. I know that seems like the distant past, but that was obviously a big issue. I was in the flood in Calgary in 2013. I was out of my office there for two weeks because of a lack of a plan. There are 212 critical applications identified. We use the words "most important" and "critical" a lot in this discussion. I guess I'm a little curious about the sort of ranking of those 212. I maybe look at it that lives at risk, public safety, and then loss of productivity might be three of the bins.

Can you tell us if there is a grid available that tells us what the ranking of those 212 is in terms of importance across the departments and, again, how you are working at those? Again, there may be some which are lives at risk, public safety, or just loss of productivity. Again, looking back at 2013 in Calgary, there were certainly millions if not tens of millions of dollars of lost productivity, which is an issue for any organization. I'm just interested in the ranking and whether that's available for us to take a look at.

Mr. Grant: Let me start by saying that we do have the list of the 212 applications. In many cases they are specific to departments, and it would be difficult for us to kind of dictate, determine if it was critical or not. Much of this is actually left in the hands of departments, who understand their role in, as you say, delivering safety services and programs to Albertans and to other government departments. We believe that the 212 is probably too many and would agree with the Auditor General that we need to continue to refine that number and move it down. That is an ongoing process that we're in with the ministries to make sure that we truly have the critical systems that we need to bring back up.

As was identified, if you look at the number of systems that we need to bring up in 72 hours, the critical and the vital, it's a lot of work. It's not just work done in my department, though. It's work that's done in every department across government, but still we need to continue to make sure we have refined that number as carefully as possible.

Mr. Brisson: Although they're identified in each of the DR plans at a ministry level, we're unable to share that ranking outside of the DR community of interest because what we're doing, then, is exposing those systems to public risk. It is private and confidential, but it is at the business level, so we know what those issues are, what the criticality is, and, depending on the issue, how we have to bring them back up.

The Chair: All right. Is this a supplemental you've got?

Mr. Gotfried: Yeah. I guess my sort of last ranking there is cost and loss of productivity. Has anybody put any numbers to – again, you've got your critical ones, you know, in 72 hours, but if there are ones beyond that – and looked at the loss of productivity issue and how that might affect cost to government over the long term? Is that something that's part of your broader review of this recovery program?

Mr. Brisson: That's where business continuity plans come into effect. So if, in fact, you did have loss of power in a building, your business continuity plan kicks in. Therefore, you're still able to deliver your service, but you're delivering in a different way. Assessing the loss of productivity there would only be able to be done once you actually see if your business continuity plan is effective as a result of the disaster that's there or the technical interference that may occur. It's hard to give a number when something hasn't happened. The importance of where we have put our efforts is to make sure that we are improving the number of DR plans that are in place and increasing the number that are being tested and working across government to increase those percentages in an effort to achieve the recommendations from the Auditor General.

Mr. Gotfried: Great. Thank you.

The Chair: Mr. Anderson.

Mr. W. Anderson: Thank you, Mr. Chair. My understanding is that – we talked with Service Alberta before – you're looking at centralizing your data systems, collapsing your number of data servers. One question is: how is that going to impact your DR piece strategy? Secondly, your two data locations, the one in Edmonton and the one in Calgary, are fully independent of each other and have independent power systems as well, but do you run a nonstop kernel? Do you have fully redundant systems built in, like a nonstop kernel, so there are full updates between each one on a regular basis? Is there a timeline of any sort? Can you please describe that for me? Thanks.

Mr. Grant: As we did in Committee of Supply, the technical questions can go to Mark.

Mr. Brisson: To the first question, we are looking at and working across government on the next phase of GOA domain migration, and that includes looking at the number of data centres and reducing them from the larger number we have today to many fewer. Obviously, there's an interest in better use of infrastructure, economies of scale, and efficiencies, but it brings it into the support of disaster recovery planning across government and business continuity. I think we would improve our situation across government as we go through this and as we're able to know all of the interfaces, all of the connections a bit better as we reduce this footprint of data centres. That strategy in itself: one of the business benefits and one of the goals that we're trying to achieve is to improve disaster recovery planning by reducing that footprint. I think that if we're – and we will be working on this over the next two years – able to move in that direction, we'll be improving those percentages of tested plans and implemented plans for critical systems.

For your second question, I don't believe I have been asked a question about a kernel in a long time, but I am sitting beside a general. In all seriousness, we have two independent data centres, one here in the NCC, the Neil Crawford centre, and then in J.J. Bowlen in Calgary. We have synchronization between the two. There are two separate data centres, two separate power centres, two separate backup centres between the two. We do have synchronization between both data centres. The purpose of the assessment for us in doing a test this last time with the GOA was to failover everything from Neil Crawford – we shut down the power there – and to send it over to our backup data centre in JJB. We did that successfully. So it does show that we have two separate ones and that if we had a problem in our main data centre, we'd be able to port it over to our backup data centre and maintain operations.

Mr. W. Anderson: Yeah. Sorry about the kernel comment. I'm just an old technical geek here. I'm sure you understood what I was talking about, so thank you.

Just a point of clarification. You mentioned your 212 applications. Those are 19 per cent of applications. Is that correct?

A second question. You mentioned the CIO Council. Does every ministry have their own CIO?

Mr. Grant: Not every ministry has their own CIO, but most ministries do.

Mr. W. Anderson: And the 19 per cent: is that correct?

Mr. Brisson: Yes; 19.3 per cent.

The Chair: A question from Mr. Dach.

Mr. Dach: Thank you, Mr. Chair. We all know that when it comes to IT and IT infrastructure, the technology is constantly changing, being updated, and we need to ensure that our testing is keeping up with these changes as well. You mentioned about large-scale IT testing recently in your comments. When was the last large-scale IT infrastructure test performed, and were there glitches that you care to comment about?

Mr. Grant: The last test that we did and the first crossgovernment test we did was in January of this year. We'd actually hoped to do it last fall, but there were a number of issues we needed to finalize before we did that and, really, from the standpoint of co-ordinating activities across government, to make sure that there was, as was mentioned in my opening comments, as little impact as possible on government activities.

The valuable lessons. From that standpoint, there were valuable lessons learned that allowed us to decide that we needed to do other tests and that we needed to do them on a yearly basis. I won't go into the details for similar reasons on why we wouldn't want to publicly state what all of the critical applications were. There were a number of technical glitches that were identified, that Mark and his team are working to resolve, but it has pointed us in the direction of: we need to do this every year. We need to do it on a regular basis, in large part because there are changes in each ministry on a yearly basis. There are new applications that come online. There are new connections going into the network system. That's probably the greatest learning that we took out of it, that we need to do it every year. We need to bring the community together to do that on a yearly basis.

9:00

The Chair: Do you have a follow-up?

Mr. Dach: Yeah. I was going to ask a bit of a follow-up. It's kind of surprising to me that these tests have historically not been performed on a more regular basis. Why haven't they been performed this way previously?

Mr. Grant: I would say that historically department IT groups have really operated independently, and it's only through incidents over the past few years that we have really focused our attention on a strategy to make sure that from a corporate standpoint we understand what's really happening with systems. You know, a good example is that we're migrating all the employees onto a GOA domain so that at least we all share the same e-mail, Outlook, file-sharing capabilities.

A question was asked earlier about productivity. I mean, the fact that you had departments who couldn't speak to one another and you had ministers who couldn't share calendars because they were on completely different systems was not great for productivity. As we start to move all of the employees onto one domain – and we're almost finished that; we're on the last department right now to move that forward – our next step would be to start to move the applications and the data centres into one domain. We believe there are tremendous efficiencies that would be gained by taking those steps.

Mr. Dach: A small secondary follow-up: how often now, then, are the large-scale corporate disaster recovery tests actually performed?

Mr. Grant: The plan right now – and we're awaiting, you know, final approval from the Deputy Minister of Executive Council and the Premier – is to run them every fall. We believe that's probably the best place to do it. In the summertime is not good because we have forest fires or floods or other activities, people on leave. During the Christmas holidays is clearly not a good time. Then you have the shoulders of the holiday seasons with the Legislature sitting. We're looking for a point in time where there's minimum destruction to government services and to the operation of government, and we believe that is the constituency week in November.

Mr. Dach: Thank you.

The Chair: You didn't have a follow-up, did you, Mr. Gotfried? No.

Okay. We'll go to Mr. Cyr.

Mr. Cyr: Thank you for coming to speak with us today. My question is specifically for Mr. Brisson. When it comes to IT, this is a very specialized field. Do you have a succession plan for yourself and the CIOs that are involved with this? Because if we don't have a succession plan, it could be that you leave and that suddenly we have no direction again. If you could address that, that would be great.

Mr. Brisson: Let me address the succession planning for CIOs across government. I do sit on many of the recruitments for new CIOs into government as part of a development process for making sure that we have some of the best and brightest individuals coming in to deliver on information management technology services in each of the departments. We're always looking at our resources across government in a corporate way, and we're right now completing a governance review of how we have our services deployed across government from an information management and technology perspective. Part of that review is looking at how CIOs are working in each of the ministries and how we can start to look to working the same way consistently across government as well as looking at opportunities for education and development and training for each of those CIOs. Now, that's done at a department level, but I do provide some input back to the departments on where and how our CIOs are functioning and working together.

Mr. Grant: Chair, if I could add to that because I think it's important. Although Mark is looking specifically at CIOs and succession planning there, the deputy minister human resource council, which is chaired by the Deputy Minister of Executive Council, Marcia Nelson, has had this discussion with me specifically about succession planning in the IT world, quite frankly, starting at the ADM level and working its way down. We're trying to look at the entire picture of leadership in the CIO world, kind of starting with Mark and making sure that his executive directors, his direct reports inside this department, and CIOs across government are all being managed appropriately and that there is succession planning across the board. So it goes beyond just the CIOs in the departments.

Mr. Cyr: So there is a succession plan for you, Mr. Brisson?

Mr. Brisson: Within the department and working with Deputy Minister Grant, I have a succession plan. Part of my role as a senior leader in government is to work with my EDs as well as others across government in their development such that, in fact, if I were to move on to another position, we would have many credible candidates to fulfill that role.

Mr. Cyr: Thank you.

The Chair: Dr. Turner.

Dr. Turner: Thank you, Mr. Chair. This report highlights the importance of co-ordination between government departments and organizations when it comes not only to the recovery plans themselves but ensuring that when these systems are tested, we are effectively co-ordinating these efforts so that we aren't accidentally negatively affecting one department or another. We've heard a little bit about this, about how you're trying to schedule this so that it has the least-disruptive effect, but what are the potential disruptive effects of a disaster recovery test?

Mr. Brisson: Co-ordination across government is something that Service Alberta is responsible for in many of the services we provide for core infrastructure. We work closely with the departments. If we were to have, as we'd indicated in our test, a natural disaster to our main data centre as what we were simulating, we'd work closely with each of the departments' CIOs. We also work with, if there is a real disaster, AEMA to indicate whether there are further business issues across government or continuity issues that are there. And then we work closely in Service Alberta with our core infrastructure group to make sure that the services that we are testing or that we, in fact, are trying to bring back up are able to work with our internal vendors to make that happen.

So the co-ordination factor of this is us taking a lead role, meaning Service Alberta, across the departments, working with IT and some business individuals to ensure that services are up in a timely fashion.

Mr. Grant: If I could add two examples, that might shed light on your question, Dr. Turner. As we were going through the test in January, one of the concerns we had was access to the MOVES system, the motor vehicles system, which is probably the oldest legacy system we have, if not the oldest. It's used by a huge number of users both inside and outside of government, particularly registry agents and law enforcement. As we went into the test, we had to make sure that we catered to the ability for law enforcement in particular to be able to continue to access the MOVES system throughout the test. So that was a critical issue.

On a less significant note, inside government at that particular time Treasury Board and Finance was working on the budget. It was a critical weekend for them to do certain activities that were budget related, so having access to their databases during that test time was another issue that we had to cater to.

As Mark has suggested, working with all of the departments and with users both inside and outside government, it really is important to figure out what the unintended consequences may be if things do go wrong and how we would have workarounds to make sure that we could continue to provide those critical services during the test period.

Dr. Turner: Thank you very much. Actually, it's very reassuring to hear that all these things are being . . .

The Chair: Do you want a follow-up?

Dr. Turner: I do want a follow-up, though.

The main recommendation in the report has laid out the road map for ensuring future successes and, hopefully, ensures that we avoid the type of IT . . .

The Chair: Is this a follow-up or a new question?

Dr. Turner: This is a follow-up.

. . . disaster that led to the report. If we haven't fully identified where the potential weaknesses are, then our recovery plan won't be successful. Have the most critical IT applications – and this follows on what the Auditor General was asking – throughout the GOA actually been identified as the Auditor General recommended?

Mr. Grant: Yeah. We're comfortable that we have identified them in conjunction with the ministries that use them and our kind of owners of those critical systems. We have identified them. We believe that there may be too many. Practically, if they were to all go down, could we get them all back up and running in 24 hours? We're still not a hundred per cent sure of that.

We will continue to work with ministries to confirm that that is the actual number. Would I like to see it lower? Absolutely, and we'll continue to work with ministries to try and make sure we absolutely have only the critical ones identified.

9:10

Dr. Turner: Thanks.

The Chair: I would caution members about using supplemental questions as new questions. I'll let that one stand because I can tell you're very passionate about your question, but we're going to have to count that as a new question.

We're going now to Mr. Anderson.

Mr. W. Anderson: Thank you, Mr. Chairman. Again, you know, I'm glad to hear that you've got a continuity plan started and in place and that you've tested it. I'm hoping to hear that you're going to be testing it on a continuous basis, not just on an annual basis. Moreover, I'm assuming you've done a risk analysis and a business impact analysis. If so, have you done it for every department? If so, have you included telephony communications, off-site data storage systems, and retention schedules as well?

Mr. Brisson: Risk analysis and business impact analysis are key components as part of a business continuity plan. Those are held by each of the ministries for each of their individual applications. As well, Service Alberta has business continuity and DR plans for its applications, that it houses on behalf of government. You know, to answer your question, included in each of those would be data centre components but also: what if your telephones went down, right? If you lose power in a building . . .

Mr. W. Anderson: You'd still have telephones.

Mr. Brisson: . . . everything goes down except for maybe cell, which maybe will go down because the wireless access point is located in the building. By way of example, your business continuity plan would have to be enacted and you may have to in fact move buildings to keep running your business operations while that is brought back up, depending on the length of time that we think it would be down. The two risk factors and impact analyses that you spoke of should be included in business continuity plans and DR plans.

Mr. W. Anderson: And you've done that for every department?

Mr. Brisson: We have completed on behalf of Service Alberta those two plans. We're working with each of the departments to ensure that they have not only disaster recover plans but also that they have tested them. Have we done that for every one of these systems and had them all tested? No. We've put the percentages forward of where we are. We're working with the DR community of interest and across the ministries to improve those percentages.

Mr. W. Anderson: Okay. Is there a timeline for that?

Mr. Brisson: The intent is to have that completed and have an updated percentage by April 2017.

Mr. W. Anderson: That includes on-site and off-site?

The Chair: I would just request, members, if you have a supplemental to ask the chair.

Mr. W. Anderson: Sorry.
Does that include on-site and off-site?

Mr. Brisson: Sorry. I don't know what . . .

Mr. W. Anderson: On-site technologies as well as off-site technologies? You've got data systems backed up off-site, correct?

Mr. Brisson: Yes.

Mr. W. Anderson: Your risk analysis includes both of those?

Mr. Brisson: It would have to, yes. Sorry.
Thank you.

Mr. W. Anderson: Thank you, Mr. Chair.

The Chair: Mr. Gotfried, was yours a follow-up or a new question?

Mr. Gotfried: A new question.

The Chair: Okay. Well, in that case let's go to Ms Luff, who had a follow-up.

Ms Luff: No. It was a new question.

The Chair: A new question as well. Okay.
Mr. Gotfried, then.

Mr. Gotfried: Thank you, Mr. Chair. There's been lots of talk around sort of the responsibility and co-ordination, and it sounds like we're in pretty good hands with that. But the other issue that's come up is the authority to actually, maybe, have a little bit more control across the ministries. I know there's been some reference to the Deputy Ministers' Council. I guess my question is: is there a will at the ADM and the deputy minister level to give that authority to Service Alberta or to a specific entity that would be not only responsible for co-ordinating it but would actually have authority over the process to ensure that this is really taken as a critical issue for government?

Mr. Grant: Let me start by saying that Marcia Nelson as the new Deputy Minister of Executive Council has taken immediate steps to revitalize a number of deputy minister committees. One of those is the deputy minister information management and technology integration committee. It didn't used to have "integration" in the name, in its previous form, as it does now. At the last meeting of Deputy Ministers' Council, last week, it was agreed to accept the terms of reference for this new committee. I'll just read part of what Deputy Minister Nelson has put in place as a key deliverable for this group: to provide IM/IT security guidance and leadership in the assessment of government of Alberta systems and ensure disaster recovery and contingency plans are in place, tested, and that the necessary resources are aligned with defined timelines. As the chair of that committee I take this as clear guidance, clear direction from my colleagues at the deputy ministers' table that I am truly responsible for this. That is reinforced by the direction my minister has given me that she expects me to make sure that in working with peers and colleagues, we're delivering on behalf of the government of Alberta.

The question was raised earlier and was alluded to by the Auditor General: what is the role of the Deputy Ministers' Council? What is the role of deputy ministers going forward? Given these new terms of reference for this revitalized, reinvigorated committee, the authority clearly has been given to me from my colleagues to make sure that we can deliver on disaster recovery testing and have a plan in place that will protect the assets of the government of Alberta.

Mr. Gotfried: Just a quick follow-up. Mr. Grant, do you feel that the authority as vested through that committee gives you what you need to do that job in terms of having that authority through that committee across the ministries, or is there something more that you would require to actually enact that in the most effective manner?

Mr. Grant: There are lots of tools that could be available. I mean, it could be legislated. It could be through an order in council. It could be through regulation. But, quite frankly, given that my colleagues have said, "Yes, Tim, go forth and do the right thing," I'm very comfortable that this gives me the authority and the tools I need, in conjunction with my colleagues who sit on the committee with me, to deliver the framework for the GOA.

Mr. Gotfried: Very reassuring. Thank you.

The Chair: A follow-up from Ms Renaud.

Ms Renaud: Thanks. I wonder if you could just expand on how this committee is invigorated other than the integration piece, I guess, that was added to the title, specifically allowing you to manage the work.

Mr. Grant: There are a couple of things that this committee is now being asked to do. To go back, the committee has actually been in place for about four years. I sat on it when it was first established, and it was a little bit – people would avoid it if they could because it was IT tech stuff that wasn't very exciting. The Deputy Minister of Executive Council has given clear direction that we have a number of things we have to do. Taking a role in IT disaster recovery is one small piece.

The other thing that has happened is that a fair amount of capital funding for IT systems has been provided to my minister, to Service Alberta, and this committee has been tasked with oversight of the expenditure of that money in other departments, so there are a number of programs in departments where the money is in my department. Those deputies happen to sit on this committee, so there is a little bit of a hook to be able to make sure that the right people are sitting at the table, because there's now money involved, but by extension they're there to make the decisions we need to make not only for IT but for information management as well.

Whether it's the control of – I mean, the IT infrastructure is one piece, but it's the information we generate and we use and we store and we dispose that is perhaps more important to me at the end of the day. Having all of these deputies from Education, Environment and Parks, Health, Human Services, Infrastructure, Treasury Board and Finance sitting on this committee, we have the right people to make the decisions.

Mr. Gotfried: Just as a follow-up, it's the information management integration committee?

Mr. Grant: The information management and technology integration committee.

Mr. Gotfried: Okay. It was a long one. I didn't have that down. Thank you.

9:20

Mr. Hunter: I'm actually not very technically savvy in the IT sector, so my question will be very rudimentary. Disaster recovery: it's a fairly broad, I guess, description of disaster, considering that there could be a disaster from fire or flood or hack or EMP. I mean, it could be a lot of stuff. Do you have a scale saying, "If this type of disaster struck, then it would take us this amount of time" versus saying, "Two hundred and some-odd will be up and going in 24 hours or 72 hours"?

Mr. Grant: Perhaps I could start by saying that the aim of the testing is to develop a system that won't go down, whether it's a flood or a fire or the Shaw Court fire, which caused water damage to servers, or whether it would be what we practised in January, which was, you know, that an ice storm was coming and the system would be shut down by a natural disaster. The aim is to make sure that irrespective of what the natural disaster or the man-made, induced disaster is, we will have a system that continues to function out of either Edmonton or Calgary.

From that standpoint, the aim is always to make sure that the systems run. If we do have a disaster, though, and the system does go down and we do have to start to bring systems back online, it is through the CIOs, that Mark talked about earlier, that would have to come together to make sure that they function as a team to bring things back up across the board, all 212 applications.

Mr. Hunter: I'll go back to my original question, though, Mr. Grant, and that is: have you been able to identify types of disasters and how long it would take to get those systems up and going based upon that type of disaster? If it was a localized disaster, a flood or a fire in a certain area, then that would be one issue, but if it was a little more widespread, you know – like, a hack would be more widespread – have you identified that?

Mr. Brisson: I can answer this in two parts. One would be preventative work that we continue to do on integrating systems across government. As we go from the 30-plus data centres down to a handful – and that's the strategy we have over the next two to five years as we integrate these into the GOA environment – we are firming up all of those applications to make sure that we have redundancy and resiliency in the system so that they can be backed up and will move over. Regardless of the disaster, that's preventative maintenance to make sure that over time, as these systems are better and well integrated, if we do have a disaster, we have a plan that will push them over to the backup data centre. So it's staying disaster agnostic, I would say.

If I were to then use an example of a cyberattack, through our corporate information security office in Service Alberta we are very resilient and vigilant on working at what cyberattacks would be hitting us, so we do a lot of preventative testing of our systems. We have our own what I would call computer hackers that would test some of our systems with, you know, a potential intrusion into one of the systems to slow it down or to stop it. We do a lot of preventative maintenance and testing for that type of disaster because there are a lot of knowns, and we're working very hard at that.

To look at different types of disasters around a flood or a fire, we have some, I guess, sample references just from our own experiences, and we work at improving the resiliency of our infrastructure with what we know, but for other, unknown disasters we don't do any analysis because they're unknown, right? We do a certain amount of preventative work. On the ones where we know a bit more, we can do a lot more analysis and testing.

Mr. Grant: I guess I would add to the answer if I could, that we plan for the worst case. So if a GOA data centre, one of our big data centres, goes down, that is the worst case for us. How do we recover from that? We haven't looked at individual data centres or server farms that individual departments would have. It would fall to them to have their own disaster recovery plan for their applications as they're stored in their own data centre. From our standpoint, it's kind of the megadisaster, when one of our big data centres goes down. If we can respond to that, then we believe we can respond to anything less than that as well.

The Chair: Mr. Malkinson.

Mr. Malkinson: Thank you very much, Chair. We know that there are a significant number of people involved in disaster recovery efforts. The report itself notes that the data centre owners, IT groups, application owners and users are just a few that play a role in this work, and it has been alluded to in some of the other questions that have been asked as well. With so many different moving parts, is there one central department or group that's leading, co-ordinating everything that's essential, and who has the overall accountability and responsibility for the IT systems disaster recovery in the event of a significant disaster?

Mr. Grant: The short answer is me. Based on what Marcia Nelson had given me last week and the guidance my minister has provided to me, kind of the buck stops here. Everything flows downhill, so a little bit of that will absolutely go to Mark and his team as the technical experts. As the chair of the new IM/IT committee it does fall to me, working with my colleagues, to make sure that we are providing the leadership required to recover from a disaster but absolutely relying on Mark as the ADM of service modernization and the CIO community to make sure that we're bringing all the resources of government together to make sure that we are responding as quickly and effectively as we can.

Mr. Malkinson: Thank you.

The Chair: Mr. Gotfried, you had a follow-up?

Mr. Gotfried: A new question.

The Chair: Well, we'll just go to you.

Mr. Gotfried: Thank you. Just quickly looking at some of the ministries here online, there seem to be, obviously, a lot of individuals involved with information management and who, I'm assuming, then, would be responsible for disaster recovery as well. In the new role that you've taken on, Mr. Grant, will you have an opportunity to look at the various structures of the information management and records management systems across the ministries to see if there's an opportunity to perhaps look at the structure, the personnel, and the productivity there to perhaps bring some streamlining into that so that there is not only the co-ordination but perhaps best practices brought across the various ministries, which would obviously aid not only in the information management but in that disaster recovery as you move forward, and perhaps have somebody on each one of those teams who also is responsible specifically for disaster recovery so that you've got that common role that's across the different ministries?

Mr. Grant: The short answer to your question is yes. The longer answer would be that in my department I have another ADM, Cathryn Landreth, responsible for open government, and she is by statute responsible for records management. This is an area that is very much like IT. I would suggest that it's much like a report that the Auditor General did on cash management, that there are lots of decentralized activities in government right now that we are moving to try and bring some consistency and standards to across the board. Information management is very much that way.

Again, this new committee and the terms of reference for the committee will allow me and the committee members to reach out across departments to make sure that we are bringing that standardization, those efficiencies where we can to how we manage information, how we create it, how we store it, how we dispose of it at the end of the day. An example would be: could we move to the electronic version of a record as the official record? We have a warehouse in the west end, like a Costco building, full of boxes to the ceiling with paper records that we've maintained, not just because of the Provincial Archives. As we move forward, we absolutely need to make sure that all of the departments have disposal schedules, that they understand what the rationale is for keeping or disposing, and that everyone follows those certainly to a higher standard than perhaps they have in the past.

9:30

Mr. Gotfried: Okay. Thank you.

The Chair: Mr. Westhead.

Mr. Westhead: Thank you very much, Mr. Chair. In terms of improvements outlined in the Auditor General's report, I know that Service Alberta has received additional capital funding this year for IT projects, so my question is: will some of the capital funding that was provided go towards implementing changes that were recommended by the AG's report?

Mr. Grant: Let me start by saying that, yes, indeed, we did get additional funds this year, and we continue to invest in both capital and operating funds towards building a more resilient infrastructure and, by extension, to approve disaster recovery capabilities. Many of these changes, though, will have to take place over time. It is significant, and it won't all happen this year, but absolutely we're getting more resources in order to address these specific issues.

Did you want to add to that, Mark?

Mr. Brisson: Yeah. In addition, I guess more specifically, as we have spoken about on a few of the other questions and answers, we're looking at consolidating some of our data centre footprint across government. Some of the capital investment that we've received will go towards the flattening of that footprint so it is then aiding our disaster recovery planning exercise and efforts.

Mr. Westhead: Thank you.

The Chair: A follow-up from Mr. Gotfried.

Mr. Gotfried: No. A fresh question, please.

The Chair: Okay. A follow-up from Mr. Cyr. I thought you asked for a follow-up.

Mr. Cyr: No, a new question.

The Chair: Okay. A new question from Mr. Cyr, then.

Mr. Cyr: My question is about the unfortunate circumstances happening in Fort McMurray right now. Is there anything that the IT disaster recovery is doing with the information in Fort McMurray? If so, which departments is it that we are doing things with? Have there been any learnings from that? I understand that the data centres aren't in Fort McMurray, but we do have a disaster happening right now.

Mr. Grant: If I could start, you're right. Fort McMurray is a disaster of monumental proportions.

Mr. Cyr: Sorry. We're running out of time here. Is there any way I could get the answer to that one tabled?

Mr. Brisson: We can answer that right now.

Mr. Cyr: Is it a quick answer? Sorry. Okay. Thank you.

Mr. Grant: Practically, there's no IT impact on Fort McMurray. There have been some issues with the delivery of SuperNet services, but that's because of access to points of presence because of the fire. Those have been remedied. Practically, is this an IT disaster in Fort McMurray? Not at all. Are we providing IT services to other departments who are delivering services in Fort McMurray? Absolutely.

Mr. Cyr: Thank you.

The Chair: A follow-up?

Okay. Ms Goehring.

Ms Goehring: Thank you. We've had the report now for over a year, and I'm happy to hear from our conversation so far today that it sounds like a considerable amount of work has been done to ensure that we're prepared. If an incident were to take place today, can you speak to how IT recovery would be handled in comparison and what additional steps have been taken to prepare?

Mr. Grant: Okay. I would say that the state of awareness of disaster threats has absolutely been heightened over the course of the last year, both because of the wildfires in Fort McMurray but also because of the work in the CIO community and the IT community inside of government because of the testing that we've done. Acknowledging that there is that threat is probably the first step, and I think that that's an important first step that everyone has taken. Overall, the planning and communication work has been assigned and taken care of. An example of that would be the briefings that Mark and I have provided to the Deputy Ministers' Council. Leading up to the IT test, deputy ministers were briefed on a number of occasions on what the tests would be, what the issues were, what were the expectations of their departments. So there's certainly a greater understanding at all levels of government as we go forward. We feel that the government is ready to deal with disasters, and we believe that our communications plan would facilitate a strong and quick reaction.

Ms Goehring: Thank you.

The Chair: All right. Mr. Anderson.

Mr. W. Anderson: Just a quick question. The Shaw Court fire was mentioned. In my day that was Shell's data centre, and it was outsourced, sold off to EDS system house as an outsourcing centre. Did the GOA have data located in that facility?

Mr. Brisson: Yes.

Mr. W. Anderson: Okay. There was no disaster program in place at that time, so it was a third party that was managing the GOA's data.

Mr. Brisson: Yes.

Mr. W. Anderson: Okay. It's the only question I have. Thank you.

The Chair: Mr. Gotfried.

I'll just note that I think there is general agreement. I think that most of the parties have exhausted their general line of questioning. So if you want to ask the last one.

Mr. Gotfried: I would be happy to. There was reference in the Auditor General's notes with respect to ATB and the impact on them from the Shaw Court incident. I'm assuming that that's a little bit at arm's length, but obviously their IT platform is within the GOA. Could you tell me what contingencies they've taken, maybe separate from what you're doing, from a customer service and data perspective or whether that's still very much under the umbrella of the GOA's information systems?

Mr. Grant: At the current time agencies, boards, and commissions, ATB being an agency, do not fall under Service Alberta's disaster recovery framework. All the actions that ATB would take would be specific to them, and I would assume that only they would be able to provide an answer to your question, unfortunately.

Mr. Gotfried: Right. So they're not going to be affected by your committee at all.

Mr. Grant: No. We don't hold any of their data. We don't provide IT services for them at all.

Mr. Gotfried: How were they then affected by the Shaw Court incident if it's held separately? It sounds to me like their data impact was no different than another department within government. Maybe the Auditor General has some information in that regard as well.

Mr. Saher: I'll just ask my colleague. Patrick, can you remember? Just simply, what was the effect on ATB of the Shaw Court disaster?

Mr. Dunnigan: Certainly. The effect on ATB was that their e-mail systems were housed as well as some of their applications, and they were unable to failover immediately, so their banking services, ATB transactions, were all affected. That was the effect on ATB.

If I may just answer the other question, the reason why ATB was affected but is not part of the GOA domain is that the Shaw Court data centre is a third party. They outsource it to other companies. Some of the radio stations in Calgary also held their servers and their data there, and they were offline. That's the reason why ATB was affected.

Mr. Gotfried: So it wasn't through the government specifically.

Mr. Dunnigan: No.

Mr. Gotfried: It just happened to be a coincidence that they were housed there as well.

Mr. Dunnigan: Yes, sir.

Mr. Gotfried: Okay.

Mr. Dunnigan: And AHS as well.

Mr. Gotfried: Oh, okay. Great. Thank you.

The Chair: Are there any further questions of the committee members?

Seeing none, I'd like to thank the officials from Service Alberta for their presentation today and for responding to our questions.

Are there any items for members to discuss under other business?

If not, our next meeting is Tuesday, May 31, with Alberta Treasury Board and Finance, scheduled from 8:30 to 10 a.m. Prebrief will be at 8 a.m.

I'll call for a motion to adjourn. Would a member move that the meeting be adjourned? Very eager. Moved by Ms Goehring. Discussion? All in favour? Opposed? Carried.

[The committee adjourned at 9:39 a.m.]

Published under the Authority of the Speaker
of the Legislative Assembly of Alberta