Unclassified

Audit of the Wide Area Network – Capacity Planning and Availability

May 27, 2022

Office of Audit and Evaluation

Shared Services Canada
Services partagés Canada

Canada

TABLE OF CONTENTS

Contents

Executive summary

One of the foundational enablers for the Government of Canada (GC), per the *Digital Operations Strategic Plan: 2018-2022,* is to build a reliable network that is always available anywhere, from any device, and scales up based on changing needs. The wide area network (WAN) is a critical component to this *Plan.* Shared Services Canada (SSC) manages the Government of Canada WAN service which enables connectivity between major data centres and federal buildings. The Government of Canada WAN is the conduit that allows public servants to connect to business applications that are essential for the delivery of programs and services to Canadians.

The objective of this audit was to provide assurance that effective processes are in place to manage WAN services availability and capacity, aligned with Treasury Board policy instruments and SSC's priorities.

Overall, we found that:

- Senior management, led by the Executive Oversight Board (EOB) and other governance committees, provided sufficient oversight to ensure alignment with the strategic objectives identified in the Treasury Board policy instruments and SSC's priorities;
- Key performance indicators were used to track progress of WAN services. The vast majority of service standards for the availability of WAN services were met, with availability at 99.965% in October 2020, exceeding the service standard set by management of 99.15%;
- There was sufficient monitoring of the managed WAN services contracts to ensure that WAN services are provided in accordance with the terms and conditions of their respective contracts and service level arrangements. Vendor reports were reviewed monthly, and service credits were requested when warranted;
- SSC maintained separate risk registers to monitor WAN risks at project, branch and operational levels. WAN equipment was not scanned on a regular basis, which limited the identification of operational risks;
- The Networks, Security and Digital Services (NSDS) Branch had a draft human resources (HR) plan for 2020-2021. Succession planning, which includes knowledge sharing, documentation, and job shadowing, was limited and may not address gaps due to the number of employees that are expected to retire in the near future. The Branch had not undertaken an analysis to identify gaps between available and the needed skills to support WAN services;
- The WAN services capacity planning process was not documented and did not include WAN utilization and trending metrics, business intake, and partner input to effectively manage available capacity and forecast WAN services growth;
- Business Continuity Plans (BCPs) were not consistently updated and tested in alignment with Treasury Board's Directive on Security Management. IT continuity plans included in the BCPs were incomplete and Standard Operating Procedures (SOPs) were not established for all WAN services. There was a reliance on automated failover systems from vendors to deal with service disruptions;

- There was no rigorous WAN services testing program in place. Vulnerability assessments, capacity and availability testing, and stress testing were performed in a lab environment before implementation, for WAN circuits and equipment. Additional testing after implementation was not regularly performed;
- The IT Refresh program was not adequately prioritized to replace WAN components that reached end of life or had no vendor support; and
- There was no consistent approach to proactively assess WAN service performance. There was no enterprise GC WAN baseline, Key Performance Indicators (KPIs) varied from vendor to vendor, and different teams used different tools.

Begonia Lojk

Chief Audit and Evaluation Executive

A. Introduction

1. Background

The Treasury Board (TB) Policy on Service and Digital and supporting instruments serve as an integrated set of rules that articulate how Government of Canada (GC) organizations manage service delivery, information and data, information technology, and cyber security in the digital era.

To achieve its digital vision, the Government of Canada developed digital standards and released *Digital Operations Strategic Plan: 2018-2022*, which prioritizes user needs and leverages the latest digital technologies to deliver high-value services to Canadians. To make the digital transformation a reality, SSC was tasked with a significant part of this Digital Operations Strategic Plan. With this in mind, SSC implemented SSC 3.0, an enterprise approach for all of government. SSC 3.0 identified three priorities, one of which is "optimizing the network and strengthening security".

One of the foundational enablers for the Government of Canada, per the *Digital Operations Strategic Plan: 2018-2022,* is to build a reliable network that is always available anywhere, from any device, and scales up with changing needs.

A wide area network (WAN) is a network that uses various links such as, Multiprotocol Label Switching (MPLS), virtual private networks (VPNs), wireless (cellular), and the internet, to connect to data centres, GC buildings, and other locations. The GC WAN connects users from national and international locations, while supporting business applications for simultaneous voice, data, and video communication. The GC WAN, via the VPN, is also the conduit that allows public servants to connect to business applications that are essential for the delivery of programs and services to Canadians. Annex B provides an overview of the GC WAN topology.

SSC operates WAN services that connect over 80 service offerings in 3,500 buildings across 43 departments and agencies (includes SSC) within and outside of Canada. The WAN services have been operating independent of each other with different network infrastructures, operating standards, processes and security measures. Many of these networks are aging; some lack advanced security standards for protection against cyber threats.

SSC initiated the Government of Canada Network (GCNet) WAN Services Project to replace all of the existing 18+ contracts with a single national network service and an international service. The GCNet WAN Services Project was initiated to improve efficiency in SSC delivery of this telecommunications service. Efficiencies will include the reduction of operational resources required to manage the delivery of WAN services and the reduction of operating costs through converging, consolidating and standardizing of these services. These efficiencies are aligned with SSC's mandate of achieving cost savings while improving IT infrastructure services.

SSC regularly measures client satisfaction with its services through the Client Satisfaction Feedback Initiative (CSFI), which uses a scale of 1 to 5. The CSFI client satisfaction score obtained for WAN services in April 2021 was 3.79, which is above the target of 3.60 set by management.

In March 2020, Canada and the rest of the world were in the midst of a global pandemic (COVID-19) which continues as of the date of this report. Millions of Canadians, including most employees of the Government of Canada, were obligated to stay home to control the spread of the COVID-19 virus. In response to these daunting health and economic conditions, the federal government responded by implementing emergency programs to help businesses and displaced workers manage through the global pandemic. As an IT enabler in the development and implementation of programs that provide assistance to Canadians, SSC's priorities immediately shifted to support the Government of Canada COVID-19 response. SSC thus developed a Treasury Board approved solution to allow over 250,000 federal public servants to continue fulfilling their responsibilities while working from home.

The GC network had been designed to leverage network-based sensors and monitoring to ensure full visibility and compliance of all traffic destined to the internet. It did not have sufficient bandwidth capacity to support the entire GC workforce working remotely at the beginning of the pandemic. IT initiatives were thus launched and tools were implemented to improve network connections and ensure the continuity of essential GC operations.

To optimize network performance while maintaining the security posture of the network and assets, SSC implemented the split tunneling initiative which redirected selected internet traffic through GC approved destinations. This initiative granted remote users access to an approved domain using their local internet while reducing bandwidth usage on the GC corporate network. SSC also rolled out the M365 collaborative software to 43 departments and agencies. M365 enhanced the telework environment and supported continued collaboration among employees. These initiatives successfully ensured the continuity of services to Canadians while supporting the health and safety of federal public servants.

2. Rationale for the audit

The Government of Canada (GC) WAN service provides enterprise WAN connectivity for Data Centres and GC buildings and locations. It securely connects users and computers from national and international locations to each other, while supporting business applications for simultaneous voice, data, and video communications.

Poor bandwidth in regional and international locations is among the top three reasons cited for low scores in SSC's Customer Satisfaction Feedback Initiative (CSFI). Furthermore, as SSC migrates to Enterprise Data Centres (EDC), High Performance Computing (HPC), and Cloud Services, there may be an increased reliance and demand for WAN services. As such, the capacity and the availability of WAN services need to be carefully planned and managed to ensure they support the migration to EDC, HPC and Cloud Services, and ultimately contribute to meeting the objectives of SSC 3.0 and the *GC Digital Operations Strategic Plan.*

3. Audit authority

The audit was included in SSC's 2019-2022 Risk Based Audit Plan, approved by the President on March 5, 2019. This audit was executed under the authority of the Office of Audit and Evaluation (OAE).

4. Objective of the audit

The objective of this audit was to provide assurance that effective processes were in place to manage WAN *availability and capacity* aligned with Government of Canada (GC) policies and SSC priorities.

5. Scope

This assurance engagement focused on WAN services availability and capacity planning and its impact on existing and emerging service lines (e.g., High Performance Computing, Cloud, and Enterprise Data Centres) as well as Enterprise Architecture. The scope covers the period of July 1, 2019 to October 31, 2020, part of which reflected the impact of the COVID-19 pandemic which resulted in Government employees being sent to work from home in early March 2020. The pandemic triggered a change in SSC's priorities and impacted normal operations. Wi-Fi, Local Area Networks (LAN), satellite, mobile devices and the GCNet WAN Services project were excluded from the scope.

6. Methodology

The audit was conducted in accordance with the International Internal Audit Standards for audit engagements and the Treasury Board of Canada Policy on Internal Audit. The following audit procedures were conducted:

Audit Procedures

1. interviews with operational staff and senior management;
2. document reviews;
3. walkthroughs of key systems and processes and procedures;
4. identification of key controls;
5. solicitation of feedback from a sample of partner department Chief Information Officers (CIOs) concerning WAN operations supporting their business lines;
6. selection of a sample of vendor managed WAN service contracts to ensure that the contracts were being monitored and were in compliance with their respective terms and conditions; and
7. testing of controls.

7. Statement of conformance

In my professional judgment as Chief Audit Executive sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed to by management. The opinion is applicable only to the entity examined. The engagement was conducted in conformance with the requirements of the Policy on Internal Audit, its associated directive, the Internal Auditing Standards for the Government of Canada, and the Institute of Internal Auditors (IIA) Code of Ethics. The evidence was gathered in compliance with the procedures and practices that meet the auditing standards, as corroborated by the results of the quality assurance and improvement program of SSC's Office of Audit an Evaluation. The evidence gathered was sufficient to provide senior management with proof of the opinion derived from the internal audit.

B. Findings, recommendations and management response

1. Governance

1.1 Oversight

Audit criterion: SSC provides oversight to ensure that Wide Area Network (WAN) services align with the strategic objectives identified in the *Treasury Board (TB) Policy and Directive on Service and Digital, Treasury Board Secretariat (TBS) Digital Operations Strategic Plan* and SSC 3.0.

The audit team expected to find that there was efficient and effective oversight to ensure that WAN services were aligned with the strategic objectives identified in the *TB Policy and Directive on Service and Digital*, *TBS Digital Operations Strategic Plan,* and SSC 3.0. This includes the development and implementation of the key performance indicators (KPIs) that track progress for meeting these goals and objectives.

The audit team found:

- The SSC approved 3-year IT plan for 2019-2022 identified Government of Canada (GC) WAN and related network initiatives aligned with SSC 3.0 and the GC digital vision;
- WAN services were regularly discussed at senior management committees, including the SSC Services and Architecture Review Board (SARB) and the Executive Oversight Board (EOB). During the pandemic, the Networks and Security Services Branch (NSSB) provided regular updates to the EOB on the split tunneling and M365 initiatives, secure remote access enhancements, as well as network capacity, bandwidth utilization and related risks; and
- IT initiatives were discussed at the Government of Canada Enterprise Architecture Review Board (EARB), co-chaired by the Chief Technology Officer (CTO) of SSC and the Chief Information Officer (CIO) of the Government of Canada. To help track progress and ensure alignment to TB policy instruments and SSC 3.0, SSC updated the Departmental Results Framework (DRF) with revised KPIs for telecommunications and network operations, including WAN services. NSSB had started to report monthly on GC WAN KPIs to the Strategy and Engagement Branch (SEB) as part of the DRF rollup exercise.

In conclusion, there was sufficient oversight to ensure that WAN Services align with the strategic objectives identified in the *Treasury Board Policy and Directive on Service and Digital, Treasury Board Secretariat Digital Operations Strategic Plan* and SSC 3.0.

2. Risk

2.1 Risk Management

Audit criterion: Networks, Security and Digital Services Branch has developed and implemented a risk register that identifies risks, level of risk, ownership of risk and risk response, for WAN services.

The audit team expected to find a centralized and comprehensive risk register, which included risks pertaining to WAN services. We also expected to find documentation outlining the risk management process including stakeholder involvement and contributions to the risk register.

The audit team found several departmental and Branch documents identifying risks that could impact WAN services. These included an SSC-wide risk ranking exercise (November 2018) conducted by the Performance Management Executive Committee (PMEC) which identified eight (8) risks for the Department, including Aging IT Systems and HR Management.

Both aging IT and HR capacity risks had been identified in the SSC 3-year (2019-2022) IT Plan and the draft Networks, Security and Digital Services Branch (NSDS) Branch Business Plan (2020-2021). The risk assessment conducted by the audit team also noted HR capacity and aging IT systems and equipment as high risks that could negatively impact the delivery of WAN services. These risks are further discussed under audit criteria 3.1 and 3.3, respectively.

The audit team found comprehensive risk registers at the project level (i.e., GCNet WAN project) with key elements including risk identification, description, impact, likelihood, ranking, accountabilities, mitigation plan, and status. The audit team found a risk register at the branch level. This risk register was missing key elements including risk impact, likelihood, ranking, and status. The audit team also found a risk register at the operational level. This risk register was missing the description of the risk impact.

One of the primary methods to identify operational risks is to scan WAN equipment for potential risks, such as security vulnerabilities, or misconfigurations. The audit team found that only limited network scanning was being conducted. Officials from the Chief Technology Officer Branch (CTOB) mentioned that some partners did not permit SSC to scan some network appliances, and that some brands of networking appliances could not be scanned with the existing tools. This limited risk identification capabilities for WAN services. Of note, the Enterprise Vulnerability and Compliance Management (EVCM) project, which was in an initial pilot phase, was expected to address limitations in scanning WAN equipment once fully operational.

Without a comprehensive risk register, including risk criticality, mitigation measures, ownership and risk monitoring status, urgent risks may be overlooked and not addressed. This could result in adverse impacts to networking operations, including WAN services. The lack of scanning of network appliances limited SSC's ability to identify vulnerabilities related to WAN services and to maintain a departmental security posture at a level commensurate with its mandate and business requirements.

In conclusion, SSC maintained risk registers to monitor WAN risks at project, branch and operational levels. These were not integrated which limited management's ability to develop risk mitigation strategies and monitor their effectiveness.

WAN equipment was not scanned on a regular basis, which limited the identification of operational risks.

Recommendation 1	**Priority**	**Medium**
The Assistant Deputy Minister, Networks and Security Services Branch should develop a comprehensive risk register that captures risk attributes and tracks the progress of WAN related risks.		
Management Response		
Management agrees with the recommendation. Currently branch risk, which also tracks the WAN services related risks, is being tracked in a number of locations across the department depending on the content: • Branch Risk Register • Operational IT Risk Register • Project Risk Register and Black books As the department moves to a more integrated Enterprise based organization, it would be beneficial to explore using an existing tool in order to create a standard approach for recording and tracking risk, as this has been an identified issue in several recent audits.		

Recommendation 2	**Priority**	**Medium**
The Assistant Deputy Minister, Networks and Security Services Branch should address scanning limitations and conduct regular scans of SSC managed network appliances to identify potential operational risks.		
Management Response		
Management agrees with the recommendation. The EVCM (Enterprise Vulnerability and Compliance Management) Project closed on March 31, 2021 and is now in the operational phase. It will provide ongoing vulnerability detection with logging and audit capabilities. The solution will deliver timely cyber vulnerability reports, address identified scanning limitations, as well as the ability to assess compliance and respond to audit requirements through the implementation of Vulnerability (VMS) and Compliance (CMS) Management Services. It should be noted, however, that we cannot enforce scanning of partner-owned equipment.		

As of January 2022, EVCM has established ongoing VA scanning and reporting coverage for 38 of the 43 departments, covering SSC managed devices. In the next 2 years, EVCM will continue to progress towards full VA coverage of all 43 departments and reach a level of maturity that will permit a more focused reporting for SSC managed network appliances. This will identify potential operational risks and feed the risk register from the first recommendation so that vulnerabilities are addressed.

3. Internal Controls

3.1 Human Resources Planning

Audit criterion: Networks, Security and Digital Services Branch has developed a comprehensive and approved human resources (HR) plan that identifies skills requirements, succession plans and training, for ensuring appropriate staffing for the delivery of Government of Canada (GC) WAN services.

The audit team expected to find a comprehensive and approved HR plan that identifies skills requirements, succession plans and training to ensure appropriate staffing for the delivery of WAN services. Effective HR planning helps organizations to meet future staffing needs and to establish a balance between the availability of resources and specialized skill sets.

HR capacity was identified as a significant risk for SSC, and as a specific risk for delivering networking services. The audit team found that the Networks, Security and Digital Services Branch (NSDS) had an HR plan for 2020-2021 which was in draft form in February 2020. With COVID-19, workload has increased substantially and training has been significantly deferred. Management was concerned about staff burn-out and overall wellness, which may further impact HR capacity and delivery of WAN services, especially if stakeholders expect that COVID-19 service levels will be maintained on an on-going basis.

It is estimated that 35% of the NSDS workforce was eligible to retire over the next 5 years. There was evidence of succession planning for executive positions and interviewees stated that some succession planning was taking place at the operational level. Operational requirements restricted the amount of time allocated to job shadowing, cross-training and job mentoring, and many critical positions had limited back up capacity. If key staff were to leave the organization or were unavailable for a prolonged period of time, SSC may not be able to support some critical WAN services.

Ensuring the availability of all required skills within an organization is a vital part of HR planning, which requires a skills gap analysis. SSC had a generic list of skills that had been developed by Treasury Board Secretariat for the CS classification conversion, but not a specific inventory of technical skills needed for WAN services. Without an analysis tailored to SSC's needs, it is difficult to determine if SSC has the required skills necessary to support WAN services.

The Branch had various HR initiatives underway, such as the CS Development Program, that may address some of the HR issues noted above. The CS Development Program was designed to enhance consistency of skills and competencies within the IT community across SSC. Early adoption of the Program had occurred within NSDS on a limited basis with 30 individuals in the fourth quarter of 2019-2020.

HR risks and issues related to capacity, succession planning, and the skills gap could jeopardize the delivery of WAN services and continuity of operations. The branch would benefit from a comprehensive HR plan for the delivery of WAN services that incorporates:

- Capacity planning that considers the impacts of COVID-19;
- Succession planning that includes knowledge sharing and cross-training; and
- Staffing plan that identifies the skills gaps.

In conclusion, NSDS had a draft human resources (HR) plan for 2020-2021. Succession planning that includes knowledge sharing and documentation, as well as job shadowing, was limited and may not address the gap resulting from the number of employees scheduled to retire in the near future. The Branch had not undertaken an analysis to identify gaps between available and the needed skills to support WAN services.

Recommendation 3	**Priority**	**High**
The Assistant Deputy Minister, Networks and Security Services Branch should develop and approve a comprehensive human resource plan in accordance with Treasury Board Secretariat policies based on a succession plan and a staffing plan that address capacity issues and considers the skills and training required to ensure that staffing needs are met for the delivery of WAN services.		
Management Response		
Management agrees with the recommendation and will continue to comply with all Departmental HR planning and reporting requirements in accordance with Treasury Board Secretariat policies. The WAN, LAN, Wi-Fi, and Cabling service lines are all under the umbrella of the Network Services would benefit from an integrated HR plan, with work performed by both the Network Services Directorate (mainly in the National Capital Region) and the Regional Services Delivery Directorate (mainly outside of the National Capital Region). Network Services adheres to all HR planning as part of Departmental processes in accordance with Treasury Board Secretariat policies. Human Resources sections of Departmental planning documents, including the Branch Business Plans (BBPs) are completed and approved by the Assistant Deputy Minister within the Departmental Planning Cycle. The 2022-2023 BBP further develops Integrated Human Resources and Workforce Planning and includes Workforce Planning, Recruitment, Succession Planning, Talent Management, Learning and Development and Workplace Wellness. In addition to the BBP, Network Services provides information to other Departmental HR planning-related activities including formally documented succession planning as part of the Executive-level performance management cycle; training opportunities as part of the Learning Needs Analysis exercise; mitigation plans for the Corporate HR risk; and capacity planning as it relates to annual budget allocations.		

3.2 WAN Capacity and Availability Strategy

Audit Criterion: Networks, Security and Digital Services Branch has a Government of Canada (GC) WAN capacity management strategy, including requirements for conducting routine assessments of the WAN services taking into consideration availability, capacity, partner management and engagement, and business and IT continuity planning.

The audit team expected to find a multi-year capacity management and availability strategy that included objectives, action plans, and performance measures. The strategy should have considered capacity, partner input, availability, business continuity planning, and IT continuity in determining how to set and meet strategic objectives.

We found that responsibilities for supporting WAN services capacity were split between the following groups:

- The Network Planning, Engineering and Managed Services (NPEMS) were responsible for ensuring that the Branch had a documented WAN capacity plan. NPEMS were also responsible for the service lifecycle management, planning and managed services, service architecture and design, and engineering for WAN services;
- The Network Operations Directorate (NetOps) were responsible for the implementation and ongoing support of WAN services and associated infrastructure including Wi-Fi, cabling, satellite, internet, Dynamic Circuit Network (DCN), foundational services, and Managed Secure File Transfer (MSFT), except where such services were fully outsourced; and
- The Policing Infrastructure Operations (PIO) were responsible for managing WAN services for the Royal Canadian Mounted Police (RCMP).

The audit team did not find an overarching WAN capacity management strategy for the annual planning and forecasting of WAN services.

The Networks, Security and Digital Services Branch (NSDS) had implemented an enterprise bandwidth monitoring tool, which amalgamated daily bandwidth utilization and performance information for the internet across all partners, and which provided enterprise-level bandwidth visibility. The tool, however, was limited to internet bandwidth and it was not clear how this information was being used for long-term capacity planning. There was no documented process that identified a planning methodology and forecast for WAN services, including bandwidth utilization. The current bandwidth forecast was not based on bandwidth utilization data, application requirements, business request (BR) intake, Workload Migration projects (WLM), and cloud migration needs. With regards to an availability strategy, the audit team was provided with Business Continuity Plans (BCPs) and emergency management plans from several WAN operation teams and found that some plans were incomplete, not regularly reviewed or tested, and did not fully comply with the *Treasury Board Directive on Security Management*. The plans did not include training and awareness requirements. There was insufficient evidence that a business impact analysis was performed to support the BCPs. It is also not clear how all of the BCPs and emergency management plans

were interconnected. There was no hierarchy or priority to these plans. BCPs included elements of IT continuity management in support of WAN services. Elements of IT continuity that were missing included communication with partners who may be affected by disruptions, measures to meet identified recovery strategies and restoration priorities, and regular testing of IT continuity management mechanisms.

The audit team found that there was a reliance across the Branch on automated failover systems from vendors to deal with service disruptions. NSDS provided a Standard Operating Procedure (SOP) for one of the departments sampled for this audit. Documented operating procedures are essential to the restoration of critical services. The lack of documented recovery procedures poses a significant risk to the availability of WAN services and business operations.

The audit team also found that BCP tabletop exercises were not completed on a regular basis to help ensure BCPs and SOPs were up-to-date and to ensure that staff were aware of how to implement the plans. It should be noted that notwithstanding the gaps noted in business continuity planning, SSC provided an effective response to the pandemic for WAN services by implementing various initiatives such as split tunneling and the M365 collaborative software to its partners to help alleviate the WAN-related impacts of the pandemic.

In conclusion, there was no overarching WAN capacity management strategy for WAN services. There was no documented process that considered bandwidth utilization data, application requirements, business request (BR) intake, Workload Migration projects (WLM), and cloud migration needs into the planning forecast for WAN services. BCPs were not consistently updated and tested, IT continuity plans included in the BCPs were incomplete and SOPs were not established for all WAN services. Network Services would benefit by having a WAN capacity and availability management strategy that takes into consideration the observations noted by the audit team, including the requirements for conducting routine assessments of the WAN services.

Recommendation 4	**Priority**	**Medium**
The Assistant Deputy Minister, Networks and Security Services Branch should develop, document and implement a process that incorporates WAN utilization, trending metrics, business intake and partner input into the planning equation for forecasting WAN services growth year over year.		
Management Response		
Management agrees with the recommendation. Networks Services already has much of this information for WAN services, such as WAN utilization, standards and metrics, and works with the partners to build realistic timelines for the delivery of WAN services.		

Network Services currently has various reports related to WAN that are prepared/received either on a weekly, bi-weekly, monthly, bi-annual or ad-hoc basis. These reports address the following but are not limited to: growth, utilization, intake, client satisfaction, contract management, service requests, service provisioning, service management, project status, service performance and capacity, monitoring, etc. The teams will continue to work towards a process that incorporates all of this information into a forecasting model.

In the interim, we will continue to use the metrics we have and share them with clients and partners where possible in order to assist in the planning process.

Recommendation 5	**Priority**	**Medium**
The Assistant Deputy Minister, Networks and Security Services Branch should implement a common set of tools for collecting WAN metrics.		
Management Response		
Management agrees with the recommendation. While metrics already exist for managed services and there are various tools to collect these metrics, Network Services will develop and implement a common set of tools for collecting WAN metrics. Network Services is developing a strategy for establishing a standardized approach for deploying proactive network performance monitoring and management capabilities across SSC's networks.		

Recommendation 6	**Priority**	**High**
The Assistant Deputy Minister, Networks and Security Services Branch should ensure that Business Continuity Plans are updated and tested, and that standard operating procedures and IT continuity plans are documented for all WAN operations.		
Management Response		
Management agrees with the recommendation. As per the *Directive on Shared Services Canada's Business Continuity Management*, the Branch is responsible for maintaining Business Continuity Plans (BCPs) for the critical and key services and activities for which they are managerially responsible. Network and Security Services Branch follows the guidance of the Emergency Management and Business Continuity Planning (EMBCP) team (departmental lead of BCPs) to ensure regular testing of these processes. The SOPs and IT continuity plans must be reviewed and updated to reflect the Network Services workforce – which is distributed across the country.		

IT continuity plans will be reviewed. In the context of WAN services the majority of the equipment is vendor-owned and controlled, and as a result SSC employees manage limited infrastructure for this WAN equipment.

Networks and Security Services Branch (NSSB) will work to update these documents to ensure that WAN operations continue to support mission critical functions. NSSB will also ensure associated processes and procedures are appropriately documented, tested, and understood by the impacted service lines in accordance with Departmental policies.

3.3 WAN Availability

Audit Criterion: SSC's WAN availability is ensured by implementing a rigorous testing regime, an IT Refresh program, and continued investment for supporting innovation of the WAN services.

The audit team expected to find a rigorous testing program for WAN equipment and circuits, the use of innovative WAN technologies, and an IT Refresh program.

The audit team found that SSC did not have a rigorous WAN services testing program in place. SSC performed GC WAN vulnerability assessments, capacity and availability testing, and stress testing in a lab environment for circuits and equipment before implementation. Additional testing after implementation was not performed regularly due to difficulties obtaining maintenance windows required for testing from partners. Lack of regular testing increases the risks of failures and could result in potential issues with WAN resiliency and availability. Best practice methodologies recommend that organizations implement a WAN infrastructure testing program to ensure capacity and availability of critical WAN services.

SSC implemented an IT Refresh program to identify and replace aging IT equipment to reduce operational and cybersecurity-related risks. Branches were responsible for the collection and dissemination of data and replacement of assets. Teams supporting WAN services created a list, reviewed annually, of aging IT equipment that was no longer supported by the vendor or unable to meet technological requirements.

The list of aging IT equipment for WAN services was not fully prioritized. Not all equipment on the list was risk assessed. Some equipment past end-of-life did not include a rationale for the risk level and priority indicator. Many network components on the list had no vendor support and were past their life expectancy. Out of 12923 network components, 1790 (14%) were high risk and out of vendor support. Without an IT Refresh program that replaces aging equipment before it reaches end-of-life or end of vendor support, there is a high likelihood of equipment failure which may impact WAN services.

The 2020 Network and Security Vision and Strategy outlines several innovative technologies that SSC should implement to meet future network demands. This Strategy aims to increase SSC's network operational efficiency, agility, security and reliability with the goal to address current network and security challenges, such as manual management processes, network duplication, and aging networks. SSC had identified Software Defined-WAN (SD-WAN) as one such innovative technology and a critical component

to operate a resilient and available network. SD-WAN uses software to control network connectivity, management and services, and improve the speed and connectivity of the network, while giving organizations better performance and greater flexibility. SSC had recently implemented SD-WAN with one of its partners and was planning SD-WAN pilots with other partners in the near future. The audit team did not find evidence to support that funds had been allocated for innovative solutions such as SD-WAN initiatives. Management, however, informed the audit team that that there was a request for funding this in the next budget.

In conclusion, SSC did not have a rigorous WAN services testing program, an adequately prioritized IT Refresh program for WAN equipment, and evidence of continued investment supporting the innovation of WAN services. A rigorous WAN services testing program and an IT Refresh program that is adequately prioritized would reduce the potential risks to the availability of WAN services. Finally, securing ongoing funding for innovative technologies such as SD-WAN would maintain or enhance the availability of WAN services.

Recommendation 7	**Priority**	**Medium**
The Assistant Deputy Minister, Networks and Security Services Branch should develop, document and implement a rigorous WAN services testing program.		
Management Response		
Management agrees with the recommendation. The audit report has made reference to a lack of testing in production. While some services already have in production testing (i.e. Enterprise Internet is tested once a week), this is not feasible for all WAN production environments due to the criticality of the service they provide, and in some cases the clients will not allow us to perform such testing. Management accepts the risk of not testing in production environments, as it is of higher risk to test in production than to not test. One example of performance testing of WAN services is seen in the management of international networks. The process consists of verifying WAN provisioning after a carrier change is implemented and of testing performance as part of incident management on an ad-hoc basis. Given these restrictions, we will look at the options for testing within the impacted service lines and will implement a WAN services infrastructure testing program. There are currently several options that are being considered.		

Recommendation 8	Priority	Medium
The Assistant Deputy Minister, Networks and Security Services Branch should ensure that the replacement of aging IT equipment is adequately prioritized based on available funding, and ensure that monitoring, tracking and reporting mechanisms are implemented.		
Management Response		
Management agrees with the recommendation. The IT Repair and Replacement (ITRR) Program is centrally managed within SSC and obtains and distributes funding to repair and replace (or modernize when possible) components within the SSC IT infrastructure whose failure could cause service interruption putting government operations and service to Canadians at risk. As ITRR funding (or special allowances) is provided to NSSB, aging equipment is replaced. Equipment is prioritized so that the most urgent/critical equipment is replaced first. ITRR branch requirements are gathered once per year at Q3 via a call letter to NSSB Directors responsible for infrastructure to develop Prioritization Lists as per the ITRR Program Standards; prioritization is based on multiple variables such as risk, partner impact, project impact, role and age. The Prioritization Lists are then used by the ITRR Program to prioritize aging equipment within the Department based on the available funds. Currently there is a department-wide process in place that includes monitoring, tracking, and reporting. Monitoring and tracking is done at a Branch level by following the ITRR Program guidelines and schedule. Tracking spreadsheets are updated by the Branch as procurement activities go forward to indicate the procurement status (submitted, ordered, cancelled, etc.). Reporting is done by the ITRR Program back to TBS on a regular basis to show progress on infrastructure investment throughout the year. Governance (including Operations and Services Board and Finance, Investment, and Internal Management Board) is in place to ensure money is allocated and prioritized correctly across the department. Planning is also underway in the Operations Management Branch to transfer these functions to a corporate data solution (i.e. Operational Data Store (ODS) or Onyx) in the future.		

3.4 Monitoring of Vendor Obligations

Audit Criterion: Networks, Security and Digital Services Branch monitors external service provider (vendor) obligations to ensure that managed WAN services are being provided in accordance with terms and conditions of the contracts/Service Level Arrangements.

The audit team expected to find that the Networks, Security and Digital Services Branch (NSDS) was monitoring the terms and conditions of the vendor contracts and vendor performance[1], the quality of the

[1] COBIT 5.0, TB policy on Services and Digital, SSC Directive on Information Technology Service Management

vendor-provided services, and requested the service credits when Service Level Targets (SLTs) were not met.

The audit team found that NSDS adequately monitored vendor contracts.

SSC depends on telecommunication companies to provide managed WAN services to support its partners. These WAN services support many critical services delivered to Canadians. Outsourced network services include telecommunications, monitoring, reporting, and security. Given that there were a number of active telecommunications contracts valued in the hundreds of millions of dollars, it is important that SSC monitor contracts to ensure compliance with terms and conditions.

To assess the SSC compliance process, the audit team selected a sample of four vendor contracts from a population of eighteen (18). The audit team found that vendor contracts and statements of work defined SLTs used to monitor WAN service performance and outlined consequences for non-compliance. To meet contract requirements, vendors provided monthly managed WAN service reports on the majority of SLTs identified in the contracts, statements of work (SOW) and service level agreements (SLAs), except for the GCNet Stream 3 contract which reported SLTs on an exception basis when SLTs were not met. The monthly reports also provided information on SLTs not met and some bandwidth utilization metrics. The audit team found that SLTs varied from contract to contract.

Most of the enterprise contracts were monitored by Network Planning, Engineering and Managed Services (NPEMS) (the exception being GCNet Stream 3), and most legacy contracts were monitored by the WAN operation teams. The SLTs are reviewed monthly, and service credits for not meeting SLTs were documented, discussed and requested from the vendors. There were monthly discussions with vendors as part of the WAN service performance reviews. Meeting minutes from these meetings were captured, actioned and reviewed for contract compliance. For some of the legacy contracts or contracts in the migration stage, however, monthly meetings were not always held. WAN operation teams were capturing and using internally generated WAN bandwidth utilization and incident data as part of the monthly billing validation and service credit exercise.

In conclusion, there was sufficient monitoring of the managed WAN service contracts to ensure that services were being provided in accordance with the terms and conditions of the contracts and service level arrangements.

3.5 WAN Service Performance

Audit Criterion: Networks, Security and Digital Services Branch implements an effective WAN availability and capacity management plan, including baselining and the use of pertinent Key Performance Indicators (KPIs) to assess WAN service performance.

The audit team expected to find that the Networks, Security and Digital Services Branch (NSDS) implemented a WAN availability and capacity management plan and processes that included baseline information and the use of KPIs to assess WAN service performance.[2]

The WAN performance and capacity management processes are critical components for delivery of Government of Canada (GC) critical services. WAN service performance must be monitored and reported on and any service non-compliant incidents must be discussed with the vendors (as outlined in audit criterion 3.4). Furthermore, WAN and circuits capacity must be monitored to ensure that it meets the operational requirements of partners, as well as the SSC service standard for WAN availability of 99.15%.

The audit team found that there is an availability service standard defined for each of the 80+ service offerings within WAN services. As of October 2020, all but 4 availability service standards were met, and the overall availability was reported at 99.965%, exceeding the service standard of 99.15%.

The audit team also found that WAN operation teams used different service monitoring approaches and tools to capture and report on WAN service standards and KPIs. Information was not proactively analyzed to identify WAN performance and capacity bottlenecks, and to plan for future WAN services bandwidth requirements. Some WAN operation teams used only vendor provided tools and reports to identify WAN performance issues and bandwidth analysis. Vendor provided reports were used to determine if service standards were being met but were not detailed enough to identify causes of bandwidth spikes or bandwidth utilization increases, and to provide accurate trending analysis.

SSC reviewed service use baselines, bandwidth utilization, performance, and availability metrics using vendor provided monthly reports. The audit team found that remediation of WAN performance issues was not always timely and that there was no enterprise baseline established for the GC WAN which consolidated the collected view of WAN services across the GC. Without a consolidated view of WAN services performance, it is difficult to assess performance of enterprise-wide WAN services and future capacity requirements.

In conclusion, while the majority of availability service standards were met, there was no consistent approach to proactively assess WAN service performance. There was no enterprise GC WAN baseline, Key Performance Indicators (KPIs) varied from vendor to vendor, and different teams used different tools.

[2] ITIL V3 and Cobit 5

Recommendation 9	Priority	Medium
The Assistant Deputy Minister, Networks and Security Services Branch should develop a consistent approach to proactively assess WAN service performance with the baseline, KPIs and tools needed to identify potential performance issues and remediate them in a timely manner.		
Management Response		
Management agrees with the recommendation. Service performance is currently measured and existing tools are used to identify performance issues. This being said, we agree that the data has not been collected in a consistent manner or with the same tools. At the time of this response, a consistent approach has been developed via the GCNet WAN and Government of Canada Network Services (GCNS) contracting vehicles. Ninety percent of partners have been migrated to the GCNet WAN contracts and are on one system with the same KPIs. Remaining WAN services will be brought in through GCNS.		

C. Conclusion

There was sufficient oversight to ensure that the WAN services align with the strategic objectives identified in the *Treasury Board Policy and Directive on Service and Digital, Treasury Board Secretariat Digital Operations Strategic Plan,* and SSC 3.0.

There was sufficient monitoring of the managed WAN services contracts to ensure that services were being provided in accordance with the terms and conditions of their contracts and service level arrangements, and the majority of service standards for the availability of WAN services were met.

SSC maintained separate risk registers to monitor WAN risks at project, branch and operational levels. These were not integrated which limited management's ability to develop risk mitigation strategies and monitor their effectiveness.

The Networks, Security and Digital Services Branch had a draft human resources (HR) plan for 2020-21. Succession planning that includes knowledge sharing and documentation, as well as job shadowing, was limited and may not address the gap resulting from the number of employees scheduled to retire in the near future. The Branch had not undertaken an analysis to identify gaps between available and the needed skills to support WAN services.

There was no overarching WAN capacity management strategy for WAN services. Also, there was no documented process that considered bandwidth utilization data, application requirements, business request (BR) intake, Workload Migration projects (WLM), and cloud migration needs into the planning forecast for WAN services. Business Continuity Plans (BCPs) were not consistently updated and tested, IT

continuity plans included in the BCPs were incomplete and Standard Operating Procedures (SOPs) were not established for all WAN services.

SSC did not have a rigorous WAN services testing program and an adequately prioritized IT refresh program for WAN equipment.

There was no consistent approach to proactively assess WAN service performance. There was no enterprise GC WAN baseline, Key Performance Indicators (KPIs) varied from vendor to vendor, and different teams used different tools.

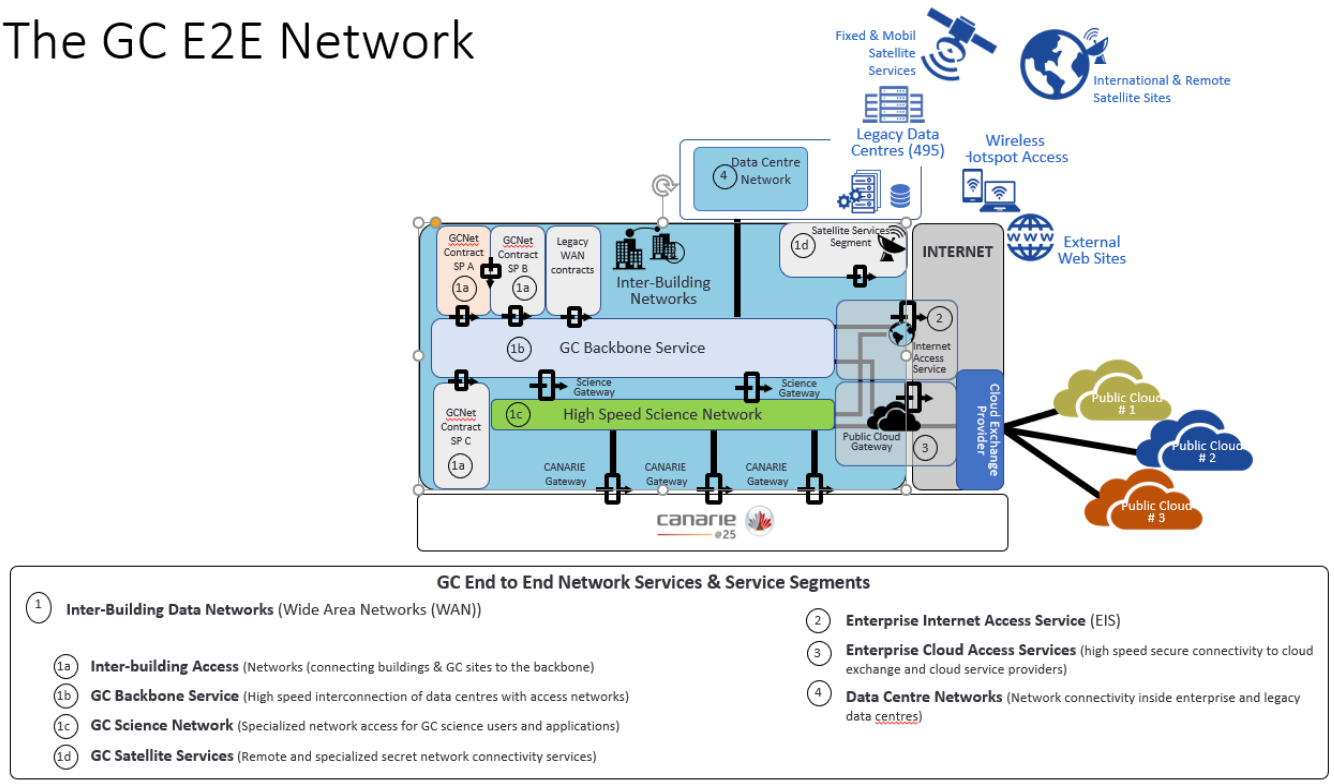
Annex A – Specific Lines of Enquiry and Audit Criteria

Audit of the Wide Area Network – Capacity Planning and Availability	
Criterion Title	**Audit Criterion**
Line of Enquiry 1: Governance[1,2,3,6]	
1.1 Oversight	SSC provides oversight to ensure that Wide Area Network (WAN) services align with the strategic objectives identified in the Treasury Board (TB) *Policy and Directive on Service and Digital, Treasury Board Secretariat (TBS) Digital Operations Strategic Plan* and SSC 3.0.
Line of Enquiry 2: Risk Management.[1,5]	
2.1 Risk Management	Networks, Security and Digital Services Branch has developed and implemented a risk register that identifies risks, level of risk, ownership of risk and risk response, for WAN services.
Line of Enquiry 3: Internal Controls [1,2,3,4,6]	
3.1 HR Planning	Networks, Security and Digital Services Branch has developed a comprehensive and approved human resources (HR) plan that identifies skills requirements, succession plans and training, for ensuring appropriate staffing for the delivery of Government of Canada (GC) WAN services.
3.2 WAN Capacity and Availability strategy	Networks, Security and Digital Services Branch has a Government of Canada (GC) WAN capacity management strategy, including requirements for conducting routine assessments of the WAN services taking into consideration availability, capacity, partner management and engagement, and business and IT continuity planning.
3.3 WAN Availability	SSC's WAN availability is ensured by implementing a rigorous testing regime, an IT Refresh program, and continued investment for supporting innovation of the WAN services.
3.4 Monitoring of Vendor Obligations	Networks, Security and Digital Services Branch monitors external service provider (vendor) obligations to ensure that managed WAN services are being provided in accordance with terms and conditions of the contracts/Service Level Arrangements.
3.5 WAN Service Performance	Networks, Security and Digital Services Branch implements an effective WAN availability and capacity management plan, including baselining, and the use of pertinent Key Performance Indicators (KPIs) to assess WAN service performance.

Sources of Criteria:

[1]Cobit 5.0
[2] ITIL v3
[3] TB Policy on Services and Digital
[4] SSC Directive on Information Technology Service Management
[5] TBS Guide to Integrated Risk Management
[6.] TBS Directive on Service and Digital

Annex B – Wide Area Network Topology



Annex C – Audit Recommendations Prioritization

Internal engagement recommendations are assigned a rating by the OAE in terms of recommended priority for management to address. The rating reflects the risk exposure attributed to the audit observation(s) and underlying condition(s) covered by the recommendation along with organizational context.

Recommendations Legend	
Rating	**Explanation**
HIGH Priority	• Should be addressed as priority for management (i.e., within the next six to 12 months) • Controls are inadequate. Important issues are identified that could negatively impact the achievement of organizational objectives • Could result in significant risk exposure (e.g., reputation, financial control or ability to achieve Departmental objectives) • Provide significant improvement to the overall business processes
MEDIUM Priority	• Should be addressed over the next year or reasonable timeframe • Controls are in place but are not being sufficiently complied with. Issues are identified that could negatively impact the efficiency and effectiveness of operations • Observations could result in risk exposure (e.g., reputation, financial control or ability of achieving branch objectives) or inefficiency • Provide improvement to the overall business processes
LOW Priority	• Changes are desirable within a reasonable timeframe • Controls are in place but the level of compliance varies • Observations identify areas of improvement to mitigate risk or improve controls within a specific area • Provide minor improvement to the overall business processes

Annex D – List of Acronyms

Acronym	Description
BBP	Branch Business Plan
BCP	Business Continuity Plan
BR	Business Request
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technologies
CMS	Compliance Management Services
CSFI	Customer Satisfaction Feedback Initiative
CTO	Chief Technology Officer
CTOB	Chief Technology Officer Branch
DCN	Dynamic Circuit Network
DRF	Departmental Results Framework
EARB	Enterprise Architecture Review Board
EDC	Enterprise Data Centre
EMBCP	Emergency Management and Business Continuity Planning
EOB	Executive Oversight Board
EVCM	Enterprise Vulnerability and Compliance Management
GC	Government of Canada
GCNet	Government of Canada Network
GCNS	Government of Canada Network Services
HPC	High Performance Computing
HR	Human Resources
IIA	Institute of Internal Auditors

Acronym	Description
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITRR	IT Repair and Replacement
KPI	Key Performance Indicator
LAN	Local Area Network
MPLS	Multiprotocol Label Switching
MSFT	Managed Secure File Transfer
NetOps	Network Operations Directorate
NPEMS	Network Planning, Engineering and Managed Services
NSDS	Networks, Security and Digital Services Branch
NSSB	Networks and Security Services Branch
OAE	Office of Audit and Evaluation
ODS	Operational Data Store
PIO	Policing Infrastructure Operations
PMEC	Performance Management Executive Committee
RCMP	Royal Canadian Mounted Police
SARB	Services and Architecture Review Board
SEB	Strategy and Engagement Branch
SD-WAN	Software Defined - Wide Area Network
SLA	Service Level Agreement
SLT	Service Level Target
SOP	Standard Operating Procedure
SOW	Statement of Work

Acronym	Description
SSC	Shared Services Canada
TB	Treasury Board of Canada
TBS	Treasury Board Secretariat
VA	Vulnerability Assessment
VMS	Vulnerability Management Services
VPN	Virtual Private Network
WAN	Wide Area Network
WLM	Workload Migration

Annex E – Glossary

The following table defines the terms used and adapted to the context of this audit:

Term	Definition
Aging IT Equipment	IT equipment that has been in use for a long time and runs the risk of failure in the long term, requiring upgrades or replacements to restore functionality.
Aging IT Systems	IT systems that have been in use for a long time and run the risk of failure in the long term, requiring upgrades or replacements to restore functionality.
Bandwidth	Bandwidth is the maximum rate of data that can be transmitted over a network.
Baseline	A snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. For example, a performance baseline can be used to measure changes in performance over the lifetime of an IT service.
Capacity Planning	Capacity Planning is the process of determining the capacity needed to meet current and future agreed capacity- and performance-related requirements in a cost-effective and timely manner.
Critical WAN Service	A critical WAN service is a WAN service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, or economic well-being of Canadians or the effective functioning of the Government of Canada.
HR Capacity	HR Capacity is the measure to ensure that an organization has a sufficient number of qualified people in the right place at the right time to achieve its objectives.
IT Continuity	IT continuity is a holistic approach to managing IT systems in the event of a major disruption. IT continuity includes preventing, mitigating, and recovering from disruptions to IT systems.
IT Refresh Program	The IT Refresh Program is an initiative to keep current information technology infrastructure assets up-to-date, through hardware and software updates and processes to identify the need to either upgrade or replace an information technology asset.

Term	Definition
Key Performance Indicator	A measure of performance that enables organizations to obtain information about many relevant factors such as the effectiveness and efficiency of their processes. The main function of KPIs is to help companies discover better ways to manage and optimize their internal operations.
Monitoring	Monitoring is a continuous process to detect compliance and risk issues.
Network Appliances	Network appliances are the switches, routers and other related telecommunications devices that support WAN services. The term should be interpreted broadly to refer to WAN assets that need to be managed throughout their lifecycle and for which security and availability risks need to be mitigated to ensure the integrity of WAN services.
Risk Register	A Risk Register is a repository of risks and mitigation measure for a system, service or entity.
Scanning	Scanning is the process of obtaining information about WAN assets to identify potential operational risks, such as security vulnerabilities and misconfigurations.
Vendor Contract	A Vendor Contract is an agreement between an organization and a vendor for the procurement of goods or services.
WAN Capacity	WAN capacity is the amount of traffic that a WAN can handle at any given time.
WAN Service	A WAN service is a fully managed network service that interconnects partner or client locations across metropolitan, regional, national or international boundaries.
WAN Service Performance	WAN service performance is the quality of service provided by a WAN.