



Bell Canada

National Hosting Services

SOC 2 Type I Report

Report on the Description of Bell Canada's Co-Location Services Relevant to Security and Availability as of December 31, 2017



Letter to Clients

Dear customer,

Thank you for your interest in Bell Canada's Co-location Services. We are pleased to provide you with this report on the controls within our data centre services. This report contains the description of the system, the trust services criteria and the underlying controls designed to meet those criteria within the National Hosting Services (NHS) environment.

Bell data centre services helps businesses by:

- Providing a highly sophisticated IT infrastructure solution at a fraction of the cost to build or retrofit an in-house data centre and manage IT internally
- Providing skilled support resources to manage the network infrastructure connected to our customers' hosted environments
- Offering high level network availability and continuous Internet connectivity backed by aggressive service level agreements
- Reducing or eliminating upfront hardware and software purchase costs and license management
- Decreasing operational risk by providing 24/7 availability and uptime for business systems
- Allowing for full scalability for current and future needs
- Removing the burden of day-to-day IT resource management to allow for increased productivity of existing IT support resources
- Driving business growth by re-deploying IT management resources to revenue generating initiatives
- Maximizing return on current technology investments
- Providing a single point of contact for your network and hosting needs

Ernst & Young LLP has examined this report in accordance with attestation standards established by the American Institute of Certified Public Accountants, enabling them to express an opinion on whether the description of the co-location services is fairly presented and whether the controls described were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met as of December 31, 2017.

This report contains confidential information and should be treated as such. It is intended solely for use by Bell data centre service customers and any independent auditors of these customers. Any duplication and distribution to an audience other than those aforementioned without Bell's prior written consent is strictly prohibited. Please contact your Customer Solutions Architect (CSA) should you have any enquiries relating to the report. If you do not know who your CSA is, please contact the Bell National Hosting Services - Network Operations Centre at 877-358-3838 and your request will be directed to the appropriate CSA.

Alan Moote
Director of Data Centre Operations



Bell Canada
National Hosting Services
SOC 2 Type I Report

Table of Contents

Letter to Clients ii

Independent Service Auditors’ Report..... iv

Management’s Assertion..... vii

Description of the Bell Canada's Co-location Services..... 1

 Overview of Services Provided..... 2

 Components of the System Providing the Service 3

 Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring ... 5

 Control Activities 9

 Logical Security..... 9

 Physical Security..... 10

 Environmental Protection..... 111

 Availability 113

 Complementary User Entity Controls..... 14

Applicable Trust Services, Criteria and Related Controls..... 15

 Security and Availability Principles and Criteria..... 16

Independent Service Auditors' Report

Independent Service Auditors' Report

To the Management and Board of Directors of Bell Canada

Scope

We have examined Bell Canada's accompanying *Description of Bell Canada's Co-Location Services* (Description) as of December 31, 2017 for its Co-location Services (System) based on the criteria set forth in paragraph 1.26 of the American Institute of Certified Public Accountants (AICPA) Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* (SOC 2®) (description criteria) and the suitability of the design of controls included in the Description as of December 31, 2017 to meet the criteria for security and availability set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

The Description indicates that certain applicable trust services criteria can be met only if complementary user entity controls assumed in the design of Bell Canada's controls are suitably designed along with related controls at Bell Canada. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design, or operating effectiveness of such complementary user entity controls.

The information in the accompanying *Letter to Clients* is presented by management of Bell Canada to provide additional information and is not part of Bell Canada's Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

Bell Canada's responsibilities

Bell Canada has provided the accompanying assertion titled, *Bell Canada's Management Assertion* (Assertion) about the fairness of the presentation of the Description based on the description criteria and suitability of the design of the controls described therein to meet the applicable trust services criteria. Bell Canada is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would prevent the applicable trust services criteria from being met; and (5) designing, implementing, and documenting controls that are suitably designed to meet the applicable trust services criteria stated in the Description.

Service auditors' responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is fairly presented based on the description criteria, and (2) the controls described therein are suitably designed to meet the applicable trust services criteria as of December 31, 2017. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's System and the suitability of the design of controls involves:

- performing procedures to obtain evidence about the fairness of the presentation of the Description based on the description criteria and the suitability of the design of the controls to meet the applicable trust services criteria.
- assessing the risks that the Description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria.
- evaluating the overall presentation of the Description.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the System that each individual user may consider important to its own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risk that the System may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria:

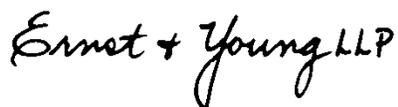
- a. the Description fairly presents the National Hosting Services System that was designed and implemented as of December 31, 2017.
- b. the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively and user entities applied the controls assumed in the design of Bell Canada's controls as of December 31, 2017.

Restricted use

This report is intended solely for the information and use of Bell Canada, user entities of the System as of December 31, 2017 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by Bell
- How Bell Canada's System interacts with user entities including complementary user entity controls assumed in the design of the Bell Canada's controls
- Internal control and its limitations
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Toronto, Ontario
January 12, 2018

Management's Assertion

Bell Canada's Management Assertion

January 12, 2018

We have prepared the accompanying *Description of Bell Canada's Co-Location Services* (Description) of Bell Canada (Service Organization) based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the American Institute of Certified Public Accountants (AICPA) Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®)* (Description Criteria). The Description is intended to provide users with information about the Co-location Services (System) that may be useful when assessing the risks from interactions with the System as of December 31, 2017, particularly information about the suitability of design of Bell Canada's controls to meet the criteria related to security and availability set forth in TSP section 100 A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Bell Canada's controls are suitably designed and operating effectively, along with related controls at Bell Canada. The Description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that:

- a. The Description fairly presents the System as of December 31, 2017, based on the following description criteria:
 - i. The Description contains the following information:
 - (1) The types of services provided.
 - (2) The components of the System used to provide the services, which are the following:
 - ▶ Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
 - ▶ Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).
 - ▶ People. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers).
 - ▶ Procedures. The automated and manual procedures¹.
 - ▶ Data. Transaction streams, files, databases, tables, and output used or processed by the System.
 - (3) The boundaries or aspects of the System covered by the description.
 - (4) For information provided to, or received from other parties:
 - ▶ How such information is provided or received and the role of the other parties.
 - ▶ The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

¹ The description of the procedures of the system includes those by which services are provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, delivered, and reports and other information prepared.

- (5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
 - ▶ Complementary user-entity controls contemplated in the design of the Bell Canada's System.
 - (6) Any applicable trust services criteria that are not addressed by a control at Bell Canada and the reasons.
- ii. The Description does not omit or distort information relevant to Bell Canada's System while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the System that each individual user may consider important to his or her own particular needs.
- b. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met, if the controls operated as described and if user entities applied the complementary user entity controls and applied the controls assumed in the design of Bell Canada's controls as of December 31, 2017.



Description of Bell Canada's Co-Location Services

Overview of Services Provided

This report describes Bell Canada's (Bell) co-location services relevant to Security and Availability for its former Q9 operations. Bell Canada's former Q9 operations have 9 co-location data centre facilities in the Toronto, Brampton, Calgary, and Kamloops areas and are covered by the scope of this report. The co-location service is offered to customers who wish to use Bell Canada's data centres while still providing and maintaining their own hardware, operating system and applications. The service includes space, power, Internet connectivity, physical security and environmental controls.

Specifically, the facilities included in the scope of this report, referred to as "co-location data centre facilities" or "data centres", are:

Three co-location data centre facilities located in downtown Toronto, Ontario. These facilities are designated:

- Toronto-100
- Toronto-110
- Toronto-104

Two co-location data centre facilities located outside of Toronto in Brampton, Ontario designated as:

- Brampton-895
- Brampton-900

One data centre facility located in downtown Calgary, Alberta and designated as:

- Calgary-800

One data centre facility located in the north eastern quadrant of Calgary, Alberta and designated as:

- Calgary-930

One data centre facility located in the south eastern quadrant of Calgary, Alberta and designated as:

- Calgary-530

One data centre facility located in Kamloops, British Columbia and designated as:

- Kamloops-146

Components of the System Providing the Service

Infrastructure

NHS is responsible for all networking equipment (i.e. routers, switches) used to connect co-located customer servers to the Internet as part of the services offered and is responsible for maintaining this networking equipment. NHS also maintains a management network which is in scope for this report, which is used by NHS Network Operations Centre (NOC) personnel to access the systems used to manage the co-location services, such as those described in the following Software section.

Software

Bell Canada NHS is not responsible for any of the applications hosted on customer servers. NHS does utilize various applications and tools to support co-location services. In particular, NHS utilizes Control Panel and Security Panel, both of which are in-house developed applications. Control Panel is used to manages all change and incident management activities, and also serves as the front-end interface for customers to submit and track their customer requests. Security Panel is used by the Security Control Centre to manage physical access provisioning and revocation for all of the raised floor space at each of the data centres.

People

Bell Canada NHS uses several key departments and teams in the delivery of its co-location services. The two main customer facing teams include the Network Operations Centre (NOC) and the Security Control Centre (SCC). The NOC team is responsible for 7x24 monitoring of automated data centre alerts (e.g., bandwidth loss, storage capacity alerts), assessing, resolving, escalating customer inquiries, and requests for changes or access. The SCC team is responsible for 7x24 monitoring of site closed circuit camera feeds, provisioning of requests for temporary and permanent physical access, and administration of other activities pertaining to cage- and site-level physical access.

Bell Real Estate Services (BRES) is responsible for the maintenance of data centre physical and environmental protections. Facilities personnel execute, or sub-contract, periodic testing of protections to determine whether they can sufficiently support production data centre loads in the event that they are required.

Data Centre Technicians (DCTs) also form an internal group responsible for providing 7x24 support services for on-site customer personnel, or as remote "hands and ears" for the NOC and SCC.

Procedures

Formal IT policies and procedures exists that describe significant processes such as physical security measures, physical access provisioning and monitoring, equipment preventative maintenance, change management, reporting and dealing with incidents, and user access to tools and applications. Formal policies and procedures exists that describe the security requirements that are mandatory as a condition of employment as well as the code of conduct that all Bell Canada employees must adhere to. All employees are expected to adhere to the NHS policies and procedures that define how its' services are to be delivered.

Data

Data within the scope of this examination is limited to the customer reporting made available. Authorized customer contacts may request monthly or ad-hoc reports of the individuals that accessed their cages and/or cabinets. The reports detail the personnel name, date and time the area was accessed. Authorized customer contacts with access to Control Panel also have the ability to view service-specific information such as open tickets for system changes, access requests, or reported incidents.

Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring

Bell Canada's internal control framework was patterned after the COSO Internal Control Framework, issued by the Committee of Sponsoring Organizations of the Treadway Commission. The framework consists of five interrelated components:

- Control environment
- Risk assessment
- Information and communications
- Monitoring
- Control activities

Control Environment

Bell Canada's control environment includes the following factors:

- Integrity and ethical values
- Commitment to competence
- Board of Directors, Audit Committee and Corporate Governance Committee oversight
- Management's philosophy and operating style
- Assignment of authority and responsibility
- Human resources policies and practices

Integrity and ethical values

Bell Canada's reputation for integrity and ethical values are espoused in the Code of Business Conduct. The Code of Business Conduct provides rules and practical guidelines for ethical behaviour based on Bell Canada's mission and values, as well as applicable laws and regulations. Annually, Bell Canada employees confirm that they have read and complied with the Code of Business Conduct.

Commitment to competence

Bell Canada demonstrates a commitment to competence and employee development. Information regarding career assessment, planning, and development is available to employees. Basic employee orientation is provided to employees when hired and specialized training is provided as needed to perform their job responsibilities.

Online Learning & Development Solutions are available for employees through the Career & Development internal web site and Virtual Leadership Centres' internal web site. The web site is intended to help employees develop their leadership capabilities by providing, through a centralized location, best practices, resource information, and learning alternatives in key areas that support the Bell Canada leadership attributes.

Board of Directors, Audit Committee and Corporate Governance Committee oversight

Bell Canada operates under the direction of BCE's Board of Directors (Board). The Board has two committees that specifically address internal controls; namely the Audit Committee and the Corporate Governance Committee (CGC).

The Audit Committee and the CGC oversee business processes, the risks associated with these processes, and internal controls to mitigate these risks. Details of the committee responsibilities are described in the committee charters available in the respective sections of Bell Canada's Website (www.bce.ca).

As defined in the Audit Committee charter, the Audit Committee assists the Board by overseeing the following:

- The integrity of Bell Canada's financial statements and related information
- Bell Canada's compliance with applicable legal and regulatory requirements
- The independence, qualifications and appointment of the external auditors
- The performance of the internal and external auditors
- Management's responsibility for reporting on internal controls

The Audit Committee has overall responsibility for providing reasonable assurance that Bell Canada's internal control systems over financial reporting are adequate and effective. The Audit Committee reviews the policies in place, monitors compliance, and approves change recommendations.

The Audit Committee also ensures that Bell Canada's risk identification and management processes are adequate and that Bell Canada complies with its business ethics policies, including the conflict of interest policy for officers.

The Audit Committee oversees the requirements of the Sarbanes-Oxley Act (SOX) and related SEC rules and of the Canadian rules related to certification of Bell Canada's internal control over financial reporting.

The Audit Committee also oversees the internal audit function:

- Overseeing internal audit plans, staffing and budgets
- Evaluating the responsibilities and performance of the internal auditor
- Reviewing periodic internal audit reports and verifying that corrective actions are being taken

As defined in the CGC charter, the CGC assists the Board in:

- Developing and implementing Bell Canada's corporate governance guidelines
- Identifying individuals qualified to become directors
- Determining the composition of the Board and its committees
- Determining the Directors' compensation
- Monitoring the process to assess the effectiveness of the Board and its committees.

Overall responsibility for the Bell Canada NHS portfolio is shared between the Business Markets President, and the EVP and CIO. Sales, marketing and product roles and responsibilities report to the Bell Business Markets President while the information systems operational responsibilities report to the EVP and CIO. The Director of Data Centre Strategy & Operations, has overall responsibility for the hosting services in each of the regions where the Bell Canada NHS portfolio is provided.

Management's philosophy and operating style

Bell Canada's management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Importance is placed on maintaining sound internal controls and the integrity and ethical values of Bell Canada personnel. Organizational values and behavioural standards are communicated to personnel

through policy statements (such as the Code of Business Conduct) and training classes. In addition, Bell Canada management reviews and approves process and procedure documentation.

Bell Canada's operations are controlled and policies are set through management processes that include periodic meetings for executive management. Senior staff members hold frequent operating meetings and these meetings alternate with those held by senior staff and executives to discuss current issues and Bell Canada's direction. Meetings are held frequently to ensure focus and direction and to prioritize issues. Other management processes and control functions include individual evaluations, annual budgeting, and periodic forecasting. Committees are organized as necessary to address strategic initiatives and any issues requiring special attention. There are scheduled Board meetings, and additional director-level meetings are called as necessary.

Management closely monitors performance so that changes within the operation do not negatively affect Bell Canada or its customers.

Assignment of authority and responsibility

Bell Canada's organizational structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job responsibilities. George Cope is the incumbent President and Chief Executive Officer of BCE Inc. and Bell Canada and has overarching leadership responsibility across the business areas. NHS is a business unit within Bell Business Markets & Wholesale.

Bell Canada's organizational structure provides defined responsibilities and lines of authority for reporting and communication through documented organization charts, roles and responsibilities, job descriptions and formal performance evaluations.

Human resources policies and practices

Human resources policies and practices are communicated to new employees as part of new hire orientation.

Bell Canada has also implemented policies and procedures to address critical financial and operational processes including operations and information systems. These policies and procedures are retained by individual departments and available through departmental internal web sites that are accessible by employees.

Risk Assessment

The goal of the risk assessment process is to identify, assess and evaluate relevant risks that could impact the achievement of the business objectives and develop responses to manage these risks. Outcome of a service organization's risk assessment process may affect the services provided to the service organization's customers.

At Bell Canada, risk assessment activities are conducted within each business unit and/or functional group. While it is the business units' or functional groups' responsibilities to perform risk assessment activities, the Internal Audit (IA) and Risk Advisory Services (RAS) functions provide vital support to this process.

As determined by risk level, IA performs annual audits on selected risk assessment activities within the business units and/or the functional groups and provides recommendations for improvement.

The results of the audits with the related management action plan are reported to the Executive Management and the Audit Committee.

The RAS function also keeps abreast of the strategic and operational risks of the organization through the review and assessment of risks identified by the business units and functional groups through their engagement in the annual strategic business planning process.

Information and Communications

Systems and processes are in place to support the identification, capture, and exchange of information in a form and timeframe that allow people to carry out their responsibilities. This includes the ability of Bell Canada to perform the following:

- Initiate, record, process and report customer's transactions (as well as events and conditions) and maintain accountability for these.
- Provide an understanding of the individual roles and responsibilities pertaining to internal controls (including the extent to which Bell Canada understands how its activities relate to the work of others and their customers) and the means for reporting exceptions to higher management levels within Bell Canada and to customers.

Bell Canada provides various mechanisms for information sharing and communication with customers, employees, and external parties. Examples of these mechanisms include:

Customers

- Customer-initiated
 - Problems with network connectivity (call to specific Help Desks)
 - Problems and/or inquiries regarding billing (call to Single Point of Contact)
 - Additions, changes, deletions and/or cancellation of services (call to Sales)
 - Performance vs. service level agreements (through internet web portal)
 - Requests for additional services or inquiries (through internet web portal and/or email)
- Bell Canada-initiated
 - Proactive identification of problems (call to specific customer)
 - Verification of customer's network status prior, during and after the implementation of a potential service-impacting change (call to critical customers)
 - Advanced scheduling notification of potential service-impacting changes to critical customers

Employees

- Corporate-wide policies: through Bell Canada's internal Bell-Net web site, policies are available. These include: alcohol and drug policy, code of business conduct, diversity in the workplace, health and safety, internet access, new employee orientation, privacy in the workplace, and others.
- Corporate communications: through Bell Canada's main internal web site and different corporate-wide communications available.

External parties

- Media communications: through Bell Canada's Media Communications internal web site, news and other information is communicated to external parties and posted on Bell Canada's external web sites.

Monitoring

Monitoring is the process that assesses the quality of internal control performance over time. Business units are primarily responsible for deploying internal controls surrounding its processes and monitoring the operating effectiveness throughout the period. This function is accomplished as part of the risk assessment process.

As part of the corporate governance and SOX compliance effort, quarterly revalidation of internal controls is also performed. The revalidations are accomplished by management's self-assessment across business units and electronically sign-off via an internal web-based application. Almost 2,000 controls are monitored which include process controls, automated controls, IT general controls and other environmental controls.

Additionally, the effectiveness of internal controls is re-evaluated on a regular basis as a result of:

- Changes in the financial reporting process
- Changes in significance of accounts as business changes
- Reprioritization of inherent business risks as determined by the finance teams and business teams
- Identified issues or deficiencies requiring in-depth analysis and immediate remedy
- Periodic baselining of automated controls.

Control Activities

Bell's control procedures are set out in the section titled *Applicable Trust Services, Criteria and Related Controls*. This is to eliminate the redundancy that would result from providing this information in this section and repeating it in the following section. Although the control procedures are included in following section, they are, nonetheless, an integral part of Bell's Description.

Logical Security

Staff within the Infrastructure group of Bell Canada (formerly Q9) are responsible for administering and maintaining logical security for the Control Panel and Security Panel applications used to manage the co-location services.

To prevent unauthorized access, authorized users are assigned a user-ID, password and a privilege level (role), which allows the user to sign on and use the system. The responsibility for provisioning employee or contractor access is shared between Human Resources, the Executive Team and the Security support staff who defines the access level depending on the job role of the employee. The hiring manager submits a request and is validated by a member of the Executive Team. The request includes the employee's roles and access privileges for the logical and physical access. Request for changes in access are captured in the MACD system and IT ticketing system. When changes in an employee's job function occur, continued access must be explicitly approved to the relevant resources or it will be automatically revoked. User access and privileges to sensitive

information such as Security Panel and Control Panel access are reviewed on a periodic basis by a member of the Executive team.

In addition, the password complexity settings for user authentication are managed in compliance with corporate access control and password policies.

Physical Security

Bell Canada has implemented a series of systems and processes for maintaining and managing the physical security of the co-location data centre facilities. Co-location cabinets and custom-built cages provide secure, dedicated environments for customers within each facility.

Access into the co-location data centre facilities and into customer enclosures is controlled using Bell Canada's biometric authentication system. Using Bell Canada's customer portal (Control Panel), each customer retains direct 7x24 control of who is authorized to access their physical environment within the facility. Bell Canada is then responsible for managing the data centre access process.

For people who will be frequently working in the customer's enclosure, Bell Canada access procedures allow for 7x24 unescorted, unannounced access. Once someone in this category has been authorized by the customer, they must present themselves, along with government issued photo ID, at the facilities security enrolment station at each data centre. At this point a Data Centre Protection Officer (DCPO) will verify with Bell Canada's Security Control Centre that access is permitted, collect the person's biometric information, and issue an access card. Once an individual is verified and enrolled they may enter the facility and unlock the customer's enclosure using Bell Canada's biometric authentication system. Customers may revoke authorization for an individual at any time and Bell Canada will disable their access card. Logs of access to the customer enclosures are available to the customer on demand and are maintained a minimum of 90 days.

Bell Canada has procedures for situations where Bell Canada employees require access to a customer enclosure. Access to the co-location data centre facilities and to customer enclosures for Bell Canada employees is restricted based on job requirements. Except in emergency situations (e.g. fire), Bell Canada employees will not enter a customer environment without requesting permission from a customer escalation contact. Once permission is granted by the customer, the authorized Bell Canada employee is required to use the biometric authentication system to access the customer environment. When the authorized Bell Canada employee has completed their task and exited the environment, the permission is revoked from the employee's access card. Bell Canada documents the entire process in a ticket which can be reviewed by the customer on a 7x24 on-demand basis through the Bell Canada customer portal. The access control system logs Bell Canada employee access to the customer enclosures and these entries logs are available to the customer and are maintained for a minimum of 90 days.

Bell Canada has procedures in place to manage the hiring, termination, and transfer of Bell Canada employees between roles within the Company. Co-location facility access rights are based on job role and are revoked on termination or when a transfer to a new role eliminates the requirement for access.

Physical access for Bell Canada employees to the security rooms where the access control system is housed is also controlled through the Bell Canada biometric authentication system. This restricted access is based on job need and the access rights are managed via the same procedures that are used to manage access rights for all Bell Canada job roles. Logical access to the access control systems is restricted based on job need and is based on unique usernames and

there are no shared logins. Authentication of the logical access to the access control systems is based on strong passwords and password change policies.

Video cameras cover the interior and exterior of each co-location facility including doors and rooms containing Bell Canada's infrastructure. The video streams are available to the on-site security employees as well as to the Bell Canada Security Control Centre. Recordings of the video streams are saved for a minimum of 90 days.

Each Bell Canada facility is staffed on a 7x24 basis with uniformed DCPOs who are responsible for physical security through data centre patrols, on-site video surveillance, and for on-site management of data centre ingress and egress processes.

Environmental Protection

Overview

Each of the Bell Canada co-location data centre facilities covered by this report are designed, built, and operated to support customer computing environments that are designed to be available on a 7x24 basis and to allow for continuous operations during normal maintenance activities and equipment failures. The critical systems in the data centre that are the subject of the controls in this report are alternate power systems, UPS systems, cooling systems, and fire detection and suppression systems.

Power

Bell Canada's alternate power supply system at each co-location facility includes multiple high-capacity generators in a high availability configuration (i.e. N+1) that have sufficient output capacity to carry the entire data centre at maximum design load. The generators draw fuel from on-site fuel storage tanks that are sized to provide sufficient capacity to operate the system for a minimum of 24 hours without re-fueling. Bell Canada also maintains relationships with multiple fuel suppliers to mitigate the risk of fuel supply issues.

UPS

The primary and alternate power supply systems (i.e. utility power and onsite generators) are used as inputs to multiple UPS systems which are deployed in an N+1 configuration. The UPS capacity is sufficient to carry the full load of the data centre during the start-up of the alternate power supplies. This system allows for a seamless transfer of load from primary to alternate power and back without impact to the critical power circuits required to operate the data centre.

Cooling

Cooling in the co-location data centre facilities has been designed and deployed with an N+1 level of redundancy. The system was also designed to be able to remove the full power input capacity of the data centre and to maintain the temperature in the facility within acceptable tolerances for the majority of commercially available computing equipment. When a customer reserves data centre capacity, in addition to reserving a specific amount of power capacity, Bell Canada also reserves and allocates a matching amount of cooling capacity. This matching of cooling capacity to available power input is a feature of Bell Canada's power reservation model.

Fire

Bell Canada data centres are equipped with a combination of conventional smoke and heat sensors along with multiple aspirating smoke detection units deployed in a zoned system capable of detecting a wide range of particulate contamination. Bell Canada data centres are equipped with multi-stage, dry-pipe, pre-action sprinkler systems, supplemented in some areas of certain facilities with clean-agent fire suppression systems. In addition, manual fire extinguishers are located throughout each of Bell Canada's co-location data centre facilities.

Fire event response, systems monitoring and trouble reporting is coordinated 7x24 by Bell Canada's centralized Control and Security Coordination Centres. Audible and visual alerts are located throughout the data centre and Bell Canada's fire detection and suppression systems are designed to help our employees identify, contain, and resolve an event as early as possible, minimizing the risk and impact of such an event on our customers.

Maintenance and testing

All the critical systems in the co-location data centre facilities are maintained and/or tested as appropriate on a regular, scheduled basis. Maintenance of the critical systems serving the co-location data centre facilities is performed by a combination of qualified Bell Canada technicians, equipment manufacturers and third-party maintenance contractors.

System Operation, Service Monitoring and Reporting Programs

Bell Canada's business is organized around the consistent delivery of services to our customers. As this is the foundation of Bell Canada's business, adherence to the internal policies and procedures and monitoring of the systems is performed on a continuous basis. The Bell Canada 7x24 Control Centre and the Bell Canada 7x24 Security Control Centre are responsible for receiving logs and alerts relating to the health of key internal systems. In addition, logging and alerting for key applications running on certain internal systems (e.g. security servers and authentication servers) that are used by the Control Centre and/or the Security Control Centre are not directed to these groups but are sent to a separate System Administration group and/or directly to appropriate senior management members. This ensures that the users of the key systems cannot alter the audit trail related to these systems.

The organization of Bell Canada's physical security operations include a separation of the Security Control Centre (SCC) reporting lines (reporting to Technology & Operations) from the reporting lines for the Data Centre Protection Officers. These lines do not converge until the senior executive level. This separation includes a well-defined separation of duties where, for instance, the SCC can print an access control card but cannot enroll someone on the card or modify the access rights associated with the card. The DCPO's can enroll an individual on a card (i.e. associate someone's biometric information with a card) but cannot tell what access rights are associated with the card. The procedures relating to the printing of a card and associating an individual's biometric information with the card, is tracked and documented using an internal ticketing system which is retained as an audit trail. None of the Bell Canada employees using the ticketing system can alter the records in the system once they are committed.

The Bell Canada Control Panel has a change log that keeps track of changes that user entities make to the access rights of the people they want to grant access to their hosted environment. These logs are available to the user entity on a 7x24 on-demand basis and are typically used by the user entity as part of their controls. The Bell Canada access control system maintains logs of the unlocking of doors into user entity co-location enclosures. These access logs can be requested by a user entity on demand or on a scheduled basis and are typically used by the user entity as

part of their controls. Data centre managers are responsible for periodic audits of the access rights for Bell Canada employees who have access to strategic locations in the co-location data centre facilities. The Director, Operations, is responsible for reviewing the shift based activity logs generated by the Security Control Centre. These activity logs contain information about incidents that have occurred during the previous eight to twelve hours and significant issues that are brought to the attention of senior management as required.

Processes are monitored through service level management procedures that monitor compliance with commitments and requirements. Results are shared with applicable personnel internally. Service Key performance indicators (KPIs) are prepared by multiple groups at Bell Canada such as the Security Control Centre and the Network Operations Centre. This report is presented to Senior Management on a periodic basis to ensure that prioritization upon resolving issues noted. KPI reports are not customer specific but are based on the achievement of various KPI measures such as incidents raised and resolved during the period. Customer specific performance measures are presented to customers on as needed basis whenever the customer requests for an SLA presentation. The reporting enables management to monitor compliance with service level commitments and requirements.

Availability

Bell Canada's contingency plans, risk register and disaster recovery documents are maintained and updated to reflect emerging risks and lessons learned from past incidents. Plans are tested based on priority throughout the year and risks are reviewed on a semi-annual basis and both documents are reviewed by the Security Team.

Bell Canada has identified critical components required to maintain the availability of the system and recover service in the event of an outage. Critical system components are backed up across a secondary environment on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

Bell Canada continuously monitors service usage to its critical infrastructure needs to support availability commitments and requirements for the Co-location Services. Bell Canada maintains a capacity planning model to assess infrastructure usage and demands on a regular basis. In addition, capacity planning supports the planning of future demands to acquire and implement additional resources based on forecasted requirements.

Complementary User Entity Controls

In designing its system, Bell Canada NHS has contemplated that certain controls would be placed in operation by user entities. The effectiveness of the controls described in this report relies on the internal control structures in place at the user entities using Bell's services. At a minimum, the following controls should exist at user entities.

Complementary User Entity Controls	Criteria
User entities are responsible for providing the information required by Bell Canada NHS to support the delivery of data centre services in accordance with user entity SLAs, MSAs, Service Schedules, Acceptable Use Policies and customer guides.	CC5.2, CC5.4, CC5.5, CC5.6, CC6.2
User entities are responsible for implementing appropriate logical access security measures over the system components for which they are responsible, per the user entity SLAs, MSAs, Service Schedules, Acceptable Use Policies and customer guides.	CC5.2, CC5.4, CC5.8
User entities are responsible for implementing measures to protect information during transmission, movement, and removal within the components of the system for which they are responsible.	CC5.7
User entities are responsible for implementing controls to prevent or detect, and act upon the introduction of unauthorized or malicious software within the components of the system for which they are responsible.	CC5.8
User entities are responsible for identifying appropriate "superuser" personnel, to request Control Panel and physical access for other user entity personnel.	CC5.2, CC5.4, CC5.5
User entities are responsible for providing timely notification to Bell Canada NHS when user entity Control Panel users no longer require access.	CC5.2, CC5.4
User entities are responsible for implementing controls to restrict Control Panel access to authorized personnel only.	CC5.2, CC5.4
User entities are responsible for carrying out periodic reviews of user entity Control Panel users and communicating any required access changes to Bell Canada NHS timely.	CC5.2, CC5.4
User entities are responsible for reviewing cage/cabinet access reports provided by Bell Canada NHS and communicating any discrepancies noted to Bell Canada NHS timely.	CC5.5
User entities are responsible for identifying user entity personnel who will have unescorted access to their cages/cabinets.	CC5.5
User entities are responsible for submitting requests for physical access via Control Panel, for personnel who do not have unescorted access privileges.	CC5.5
User entities are responsible for providing timely notification to Bell Canada NHS when user entity personnel no longer require physical access.	CC5.5
User entities are responsible for implementing controls to notify Bell Canada NHS when they become aware of issues such as temperature alerts within their equipment or loss of power within an enclosure or to a specific piece of equipment.	CC6.1, CC6.2
User entities are responsible for implementing controls to ensure that changes to system components are authorized, tested and approved by the user entity, if required.	CC7.4
User entities are responsible for monitoring their processing capacity and resource usage and requesting additional resources as required.	A1.1
User entities are responsible for defining backup and system availability and recovery requirements	A1.2

Applicable Trust Services, Criteria and Related Controls

Security and Availability Principles and Criteria

Ref.	Criteria Description	Controls Specified by Bell Canada
CC 1.0	Common Criteria Related to Organization and Management	
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability.	<p>NHS.01: The entity has an up-to-date organizational chart to define reporting lines, authorities and responsibilities and revises this when necessary to help meet changing commitments and requirements.</p> <p>NHS.02: Role and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.</p> <p>NHS.03: Employee performance, personal and career goals are reviewed by management on an annual basis. During the review, job duties may be identified for changes and required training are established accordingly.</p>
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.	<p>NHS.02: Role and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.</p> <p>NHS.04: Job descriptions are reviewed for needed changes and updated accordingly when a job is open for hiring.</p> <p>NHS.05: Bell Canada has defined a formal risk management process that specifies risk tolerances, roles and responsibilities and the process for evaluating risks based on identified threats and the specified tolerances.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC1.3	<p>The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.</p>	<p>NHS.06: Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.</p> <p>NHS.07: Bell administers and monitors skills and continued training commensurate with its commitments and requirements for employees through the corporate HR performance management tool.</p> <p>NHS.08: Personnel are required to attend annual security, confidentiality, and privacy training. Management monitors compliance with training requirements through the corporate HR performance management tool.</p> <p>NHS.09: Management evaluates the need for additional tools and resources in order to achieve business objectives, as part of monthly KPI meetings, and weekly Tools Alignment meetings</p>
CC1.4	<p>The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability.</p>	<p>NHS.10: Management monitors employees' compliance with the code of conduct through external customer surveys and internal monitoring of employee complaints via formal and informal reporting channels such as a Business Conduct Helpline.</p> <p>NHS.11: Personnel are required to read and accept the Code of Conduct and the statement of security, confidentiality, and privacy practices upon hire and annually thereafter within the HR performance management tool.</p> <p>NHS.06: Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.</p> <p>NHS.12: Personnel must pass a criminal background check before they may be hired by the entity.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC 2.0	Common Criteria Related to Communications	
CC2.1	<p>Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.</p>	<p>NHS.13: SLAs, MSAs, Acceptable Use Policies, Service Schedules, and customer guides are available to authorized external users that delineate the boundaries of the services and describe relevant services components as well as the purpose and design of the services.</p> <p>NHS.14: Internal procedure documents and operating manuals are posted on the intranet and are available to the internal users. This description delineates the boundaries of the system and services and key aspects of processing.</p> <p>NHS.15: SLAs, MSAs, Acceptable Use Policies, Service Schedules, and customer guides delineate the parties responsible, accountable, consented, and informed of changes in design and operation of key system components. Bell identifies responsible personnel and communication channels with customers, e.g., a generic NOC email address, customer account managers.</p>
CC2.2	<p>The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.</p>	<p>NHS.16: Bell Canada's security and availability commitments regarding the services are included in the master services agreement and customer-specific service level agreements.</p> <p>NHS.14: Internal procedure documents and operating manuals are posted on the intranet and are available to the internal users. This description delineates the boundaries of the system and services and key aspects of processing.</p> <p>NHS.08: Personnel are required to attend annual security, confidentiality, and privacy training. Management monitors compliance with training requirements through the corporate HR performance management tool.</p> <p>NHS.11: Personnel are required to read and accept the Code of Conduct and the statement of security, confidentiality, and privacy practices upon hire and annually thereafter within the HR performance management tool.</p> <p>NHS.17: Network and device availability, incident resolution, service commencement commitments, and available capacity are monitored at weekly and monthly meetings. Results are shared with applicable personnel, and actions are taken and communicated to relevant parties as required. Customer responsibilities are listed in the SLA and in system documentation.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC2.3	<p>The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.</p>	<p>NHS.14: Internal procedure documents and operating manuals are posted on the intranet and are available to the internal users. This description delineates the boundaries of the system and services and key aspects of processing.</p> <p>NHS.08: Personnel are required to attend annual security, confidentiality, and privacy training. Management monitors compliance with training requirements through the corporate HR performance management tool</p> <p>NHS.11: Personnel are required to read and accept the Code of Conduct and the statement of security, confidentiality, and privacy practices upon hire and annually thereafter within the HR performance management tool.</p> <p>NHS.17: Network and device availability, incident resolution, service commencement commitments, and available capacity are monitored at weekly and monthly meetings. Results are shared with applicable personnel, and actions are taken and communicated to relevant parties as required. Customer responsibilities are listed in the SLA and in system documentation.</p> <p>NHS.15: SLAs, MSAs, Acceptable Use Policies, Service Schedules, and customer guides delineate the parties responsible, accountable, consented, and informed of changes in design and operation of key system components. Bell identifies responsible personnel and communication channels with customers, e.g., a generic NOC email address, customer account managers.</p>
CC2.4	<p>Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.</p>	<p>NHS.14: Internal procedure documents and operating manuals are posted on the intranet and are available to the internal users. This description delineates the boundaries of the system and services and key aspects of processing.</p> <p>NHS.17: Network and device availability, managed device incident resolution, service commencement commitments, and available capacity are monitored at weekly and monthly meetings. Results are shared with applicable personnel, and actions are taken and communicated to relevant parties as required. Customer responsibilities are listed in the SLA and in system documentation.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC2.5	Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	<p>NHS.14: Internal procedure documents and operating manuals are posted on the intranet and are available to the internal users. This description delineates the boundaries of the system and services and key aspects of processing.</p> <p>NHS.17: Network and device availability, incident resolution, service commencement commitments, and available capacity are monitored at weekly and monthly meetings. Results are shared with applicable personnel, and actions are taken and communicated to relevant parties as required. Customer responsibilities are listed in the SLA and in system documentation.</p>
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.	<p>NHS.18: Proposed system shutdowns associated with changes that affect external parties are communicated before their implementation.</p> <p>NHS.19: The system change calendar that indicates CAB approved changes to be implemented is posted on the entity's intranet.</p> <p>NHS.20: For high severity incidents, a root cause analysis is prepared and reviewed by operations management which is then communicated to the customer. Based on the root cause analysis, additional change or incident requests are created as necessary.</p> <p>NHS.15: SLAs, MSAs, Acceptable Use Policies, Service Schedules, and customer guides delineate the parties responsible, accountable, consented, and informed of changes in design and operation of key system components. Bell identifies responsible personnel and communication channels with customers, e.g., a generic NOC email address, customer account managers.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC 3.0	Common Criteria Related to Risk Management and Design and Implementation of Controls	
CC3.1	<p>The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises as necessary, risk assessments and mitigation strategies based on the identified changes.</p>	<p>NHS.21: A master list of Bell Canada's system components is maintained on Bell's asset management tool, accounting for additions and removals. The tool captures key system components, technical and installation specific implementation details, and supports ongoing asset and service management commitments and requirements.</p> <p>NHS.05: Bell Canada has defined a formal risk management process that specifies risk tolerances, roles and responsibilities and the process for evaluating risks based on identified threats and the specified tolerances.</p> <p>NHS.22: During the risk assessment and management process, security team personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.</p> <p>NHS.23: Identified risks are rated using a risk evaluation process and ratings are reviewed by management.</p> <p>NHS.24: The Security team executes or assigns risk mitigating activities, evaluates the effectiveness of controls and mitigation strategies in meeting identified risks and recommends changes based on its evaluation. Recommendations are reviewed and approved by the CISO.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC3.2	<p>The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, and updates the controls, as necessary.</p>	<p>NHS.25: Control self-assessments are performed by operating units on a quarterly basis.</p> <p>NHS.26: Internal audits are performed based on the annual risk- based internal audit plan.</p> <p>NHS.27: IT DR plans and data centre BC plans plans are tested annually.</p> <p>NHS.24: The Security team executes or assigns risk mitigating activities, evaluates the effectiveness of controls and mitigation strategies in meeting identified risks and recommends changes based on its evaluation. Recommendations are reviewed and approved by the CISO.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC 4.0	Common Criteria Related to Monitoring of Controls	
CC4.1	<p>The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.</p>	<p>NHS.17: Network and device availability, incident resolution, service commencement commitments, and available capacity are monitored at weekly and monthly meetings. Results are shared with applicable personnel, and actions are taken and communicated to relevant parties as required. Customer responsibilities are listed in the SLA and in system documentation.</p> <p>NHS.25: Control self-assessments are performed by operating units on an annual basis.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC 5.0	Common Criteria Related to Logical and Physical Access Controls	
CC5.1	<p>Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.</p>	<p>NHS.30: Access to Management Network is reviewed periodically to confirm that access privileges remain authorized and appropriate. Any required changes of access privilege are modified in a timely manner.</p> <p>NHS.31: Management Network is accessed via a jumpbox, users require a different user ID and password for access to the sensitive environment. Access to management applications require separate credentials.</p> <p>NHS.32: Control Panel is configured to require users to change their password upon initial sign-on and every 90 days thereafter.</p> <p>NHS.33: Security Panel is configured to require users to change their password upon initial sign-on and every 90 days thereafter.</p>
CC5.2	<p>New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</p>	<p>NHS.34: For Bell Canada employees and contractor/vendors, access to systems is removed within a timely manner.</p> <p>NHS.35: Customer accounts are removed for users that no longer require access from the Control Panel in a timely manner.</p> <p>NHS.36: Customer accounts are created based on authorization of the designated customer point of contact through the Control Panel.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.	<p>NHS.37: External access to the Management Network by employees is permitted only through an encrypted virtual private network (VPN) connection and Lightweight Directory Access Protocol (LDAP).</p> <p>NHS.38: Two factor authentication and use of encrypted VPN channels restrict access to IT components to only valid users.</p> <p>NHS.39: Password complexity standards are established to enforce control over access control software passwords.</p> <p>NHS.31: Management Network is accessed via a jumpbox, users require a different user ID and password for access to the sensitive environment. Access to management applications require separate credentials.</p>
CC5.4	Access to data, software, functions, and other IT resources is authorized and modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.	<p>NHS.41: Role-based access controls limit access to Control Panel and Security Panel.</p> <p>NHS.35: Customer accounts are removed for users that no longer require access from the Control Panel in a timely manner.</p> <p>NHS.30: Access to Management Network is reviewed periodically to confirm that access privileges remain authorized and appropriate. Any required changes of access privilege are modified in a timely manner.</p>
CC5.5	Physical access to facilities housing the system (for example, data centres, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.	<p>NHS.41: Access control devices have been installed that limit access to the co-location data centre facilities.</p> <p>NHS.42: The physical access security system segregates access to the various rooms within the co-location data centre facilities. Clearance levels are determined based on job needs.</p> <p>NHS.43: Bell Canada's employee and customer access to co-location data centre facilities is restricted and is appropriately authorized based on access required.</p> <p>NHS.44: Valid identification and sign-in is required for visitors and contractors requesting access to the co-location data centre facilities. The access card issued to the visitor or contractor is only valid for the specified time of the visit and is required to be returned to Bell Canada at the end of the visitation.</p> <p>NHS.45: Visitor access cards are recorded in the system and do not permit access to any secured areas of the facility.</p> <p>NHS.46: All visitors must be escorted by a Bell Canada employee when visiting facilities where sensitive system and</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
		<p>system components are maintained and operated.</p> <p>NHS.47: Access to the system controlling access card reader is granted based upon an appropriate approval.</p> <p>NHS.48: Access to the system controlling access card readers is appropriately restricted. Users are assigned unique user IDs and passwords are required.</p> <p>NHS.49 Access for terminated Bell Canada customers, employees and contractors who no longer require access are removed in a timely manner.</p> <p>NHS.50: Owners of sensitive areas of the facilities review the list of names and roles of those granted physical access to their areas on a semi-annual basis to check for continued business need. Requests for changes are made through the change management record system.</p> <p>NHS.51: The MACD system sends a notification to the manager of Security Services of terminated employees for whom access is to be removed. A reminder is sent periodically until the access is to be removed.</p> <p>NHS.52: The sharing of access badges and tailgating are prohibited by policy.</p> <p>NHS.53: Mantraps or other physical devices are used for controlling accessing highly sensitive facilities.</p> <p>NHS.54: Mantraps and equipment traps can only be bypassed by security booth staff.</p> <p>NHS.79: The co-location data centre facilities have video cameras deployed such that critical areas of the facility (ingress and egress points, entrance to customer enclosures, corridors, and areas containing Bell Canada environmental systems as well as external areas around the facility) are captured by the cameras. The video streams from the cameras are monitored on-site by a central Security Control Centre.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC5.6	<p>Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.</p>	<p>NHS.55: External points of connectivity are protected by a firewall complex.</p> <p>NHS.56: Firewall hardening standards are used to configure new firewalls and are based on relevant applicable technical specifications, and product and industry recommended practices.</p> <p>NHS.29: Network scans are performed annually for infrastructure elements to identify variance from entity standards.</p> <p>NHS.28: Vulnerability scans are performed monthly and results are tracked for remedial action based on their severity.</p>
CC5.7	<p>The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.</p>	<p>NHS.37: External access to the Management Network by employees is permitted only through an encrypted virtual private network (VPN) connection and Lightweight Directory Access Protocol (LDAP).</p> <p>NHS.57: Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted per the Code of Conduct.</p>
CC5.8	<p>Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.</p>	<p>NHS.58: Patching for devices is performed on at least a quarterly basis. Patching follows the change management process.</p> <p>NHS.59: The ability to patch devices is restricted system administration personnel.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC 6.0	Common Criteria Related to System Operations	
CC6.1	<p>Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.</p>	<p>NHS.17: Network and device availability, incident resolution, service commencement commitments, and available capacity are monitored at weekly and monthly meetings. Results are shared with applicable personnel, and actions are taken and communicated to relevant parties as required. Customer responsibilities are listed in the SLA and in system documentation.</p> <p>NHS.60: Operations personnel follow documented procedures for evaluating, classifying, escalating, and resolving reported events as required, e.g., security related events are assigned to the security group for evaluation.</p> <p>NHS.61: IT DR plans and data centre BC plans plans are tested annually.</p> <p>NHS.62: DR test results are reviewed and the contingency plan is adjusted.</p>
CC6.2	<p>Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.</p>	<p>NHS.60: Operations personnel follow documented procedures for evaluating, classifying, escalating, and resolving reported events as required, e.g., security related events are assigned to the security group for evaluation.</p> <p>NHS.17: Network and device availability, incident resolution, service commencement commitments, and available capacity are monitored at weekly and monthly meetings. Results are shared with applicable personnel, and actions are taken and communicated to relevant parties as required. Customer responsibilities are listed in the SLA and in system documentation.</p> <p>NHS.63: Internal and external users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.</p> <p>NHS.20: For high severity incidents, a root cause analysis is prepared and reviewed by operations management which is then communicated to the customer. Based on the root cause analysis, additional change or incident requests are created as necessary.</p> <p>NHS.64: Bell Canada policies include probation, suspension, and termination as potential sanctions for employee misconduct.</p>

Ref.	Criteria Description	Controls Specified by Bell Canada
CC7.0	Common Criteria Related to Change Management	
CC7.1	The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	NHS.65: Production change requests are evaluated at key points to determine the potential effect of the change on security and availability commitments and requirements.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.	NHS.09: Management evaluates the need for additional tools and resources in order to achieve business objectives, as part of monthly KPI meetings, and weekly Tools Alignment meetings. NHS.20: For high severity incidents, a root cause analysis is prepared and reviewed by operations management which is then communicated to the customer. Based on the root cause analysis, additional change or incident requests are created as necessary.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.	NHS.20: For high severity incidents, a root cause analysis is prepared and reviewed by operations management which is then communicated to the customer. Based on the root cause analysis, additional change or incident requests are created as necessary.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.	NHS.65: Production change requests are evaluated at key points to determine the potential effect of the change on security and availability commitments and requirements. NHS.66: Changes are reviewed and approved by the change advisory board prior to implementation. The CAB is comprised of Change Managers and Subject Matter Experts. NHS.67: Changes are tested prior to implementation, or validated post-implementation if pre-implementation testing is not feasible.

Ref.	Criteria Description	Controls Specified by Bell Canada
Additional Criteria for Availability		
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	NHS.68: The nature and extent of the protections in place for critical infrastructure components, e.g., backup power, are assessed to be appropriate for the level of risk faced by the components, e.g., sufficient redundancy. The assessment is annual.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	<p>NHS.69: Environmental protections have been installed including the following:</p> <ul style="list-style-type: none"> o Cooling systems o Battery and generator back-up in the event of power failure o Fire detectors o Fire suppression. <p>NHS.70: Operations personnel monitor the status of environmental protections during each shift.</p> <p>NHS.71: Environmental protections receive maintenance on at least an annual basis.</p> <p>NHS.27: IT DR plans and data centre BC plans plans are tested annually.</p> <p>NHS.72: The entity has redundant facilities to permit the resumption of IT operations in the event of a disaster at it data centres.</p>
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	<p>NHS.27: IT DR plans and data centre BC plans plans are tested annually.</p> <p>NHS.62: Test results are reviewed and the contingency plan is adjusted.</p>