# Bell Canada

## National Hosting Services

SOC 2 Type II Report

Report on the Description of Bell Canada's Co-location Services Relevant to Security and Availability

For the period from January 1, 2018 to December 31, 2018

# 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 design and operating effectiveness of 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 and implemented to provide reasonable assurance that the applicable trust services criteria would be met, and whether the control procedures that were tested were operating effectively to meet the applicable trust services criteria from January 1, 2018 to December 31, 2018.

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

# Bell Canada
# National Hosting Services
# SOC 2 Type II Report

## Table of Contents

# Independent Service Auditors’ Report

Building a better
working world

Ernst & Young LLP
EY Tower
100 Adelaide Street West
P.O. Box 1
Toronto, Ontario
M5H 0B3

Tel: 416 864 1234
Fax: 416 864 1174
ey.com/ca

# 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) of its co-location services system (System) throughout the period January 1, 2018 to December 31, 2018, in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period January 1, 2018 to December 31, 2018, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for Security and Availability set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Bell Canada uses data centre facilities operated by Cologix, Inc., (subservice organization) for the co-location of its Rene-Levesque data centre. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Bell Canada, to achieve Bell Canada's service commitments and system requirements based on the applicable trust services criteria. The description presents Bell Canada's System; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Cologix, Inc. Our examination did not extend to the services provided by Cologix, Inc., and we have not evaluated whether the controls management assumes have been implemented at Cologix, Inc., have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2018 to December 31, 2018.

The Description also indicates that that Bell Canada's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved 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 the service organization. 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. This additional 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 is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved. Bell Canada has provided the accompanying assertion titled, *Bell Canada's Management Assertion* (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on 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 threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description.

*Service auditors' responsibilities*

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness 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 American Institute of Certified Public Accountants (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 presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would achieved if the applicable trust services criteria throughout the period January 1, 2018 to December 31, 2018. The nature, timing, and extent of the procedures selected depend on our judgement, 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 and operating effectiveness of controls involves:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Performing procedures to obtain evidence about whether the controls stated in the description are presented in accordance with the Description Criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitable designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- 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 or operating effectiveness 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.

*Description of test of controls*
The specific controls we tested and the nature, timing, and results of those tests are listed in the accompanying Applicable Trust Services Principles and Criteria, Bell's Related Controls and Ernst & Young LLP's Tests of Controls and Results (Description of Tests and Results).

*Opinion*
In our opinion, in all material respects:

a. The Description presents the co-location services system that was designed and implemented throughout the period January 1, 2018 to December 31, 2018 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively, and if the subservice organization and user entities applied the controls assumed in the design of Bell Canada's controls throughout the period January 1, 2018 to December 31, 2018.

c. The controls operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust service criteria throughout the period January 1, 2018 to December 31, 2018, if the subservice organization and user entity controls assumed in the design of Bell Canada's controls operated effectively throughout the period January 1, 2018 to December 31, 2018.

*Restricted use*
This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Bell Canada, user entities of Bell Canada's National Hosting Services system during some or all of the period January 1, 2018 to December 31, 2018 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 Canada
- How Bell Canada's system interacts with user entities, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization'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.

Ernst + Young LLP

Toronto, Ontario
January 25, 2019

# Management's Assertion

# Bell Canada's Management Assertion

January 25, 2019

We have prepared the accompanying *Description of Bell Canada's Co-location Services* (Description) of Bell Canada (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the co-location services system (System) that may be useful when assessing the risks arising from interactions with the System throughout the period January 1, 2018 to December 31, 2018, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for Security and Availability set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Bell Canada uses data centre facilities operated by Cologix, Inc., (subservice organization) for the co-location of its Rene-Levesque data centre. The Description includes only the controls of Bell Canada and excludes controls of Cologix, Inc. The Description also indicates that certain trust services criteria specified therein can be met only if Cologix Inc.'s controls assumed in the design of Bell Canada's controls are suitably designed and operating effectively along with the related controls at Bell Canada. The Description does not extend to controls of Cologix, Inc.

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 the Service Organization. The Description does not extend to controls of user entities.

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

*a.* The Description presents the System that was designed and implemented throughout the period January 1, 2018 to December 31, 2018 in accordance with the Description Criteria.

*b.* The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Bell Canada's controls throughout the period January 1, 2018 to December 31, 2018.

*c.* The Bell Canada controls stated in the description operated effectively throughout the period January 1, 2018 to December 31, 2018 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Bell Canada's controls throughout the period January 1, 2018 to December 31, 2018.

# Description of Bell Canada’s Co-location Services

## Overview of Services Provided

This report describes Bell Canada National Hosting Services' (NHS) co-location services relevant to Security and Availability. NHS offers these services to its customers through data centres in in the Toronto, Brampton, Markham, Calgary, Montreal, Vancouver, Ottawa and Kamloops. A subset of these data centres were formerly owned and operated by Q9 Networks, Inc. In 2016, Bell Canada Enterprises, Inc., completed an acquisition of Q9 Networks, Inc., including these data centres. The data centres that are in-scope for this report are identified below.

Four data centres located in Toronto, Ontario. These facilities are designated:
- Toronto-100
- Toronto-110
- Toronto-104
- Canniff (CNF)

Two data centres located in Brampton, Ontario. These facilities are designated:
- Brampton-895
- Brampton-900

Two data centres in located in Montreal, Quebec. These facilities are designated:

- Vanden-Abeele (VDA)
- Rene-Levesque (RLM)

Four data centres located in Calgary, Alberta. These facilities are designated:
- Calgary-800
- Calgary-930
- Calgary-530
- Maynard (MRD)

One data centre in Ottawa, Ontario. This facility is designated:
- Lepine (LEP)

One data centre in Markham, Ontario. This facility is designated:
- Warden (WRD)

One data centre in Vancouver, British Columbia. This facility is designated:
- Still Creek (STC)

One data centre in Kamloops, British Columbia. This facility is designated
- Kamloops-146

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.

## 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 utilizes various applications and tools to support co-location services.  These include commercially available network management and monitoring tools, ticketing systems, and proprietary information systems used communicate with authorized customer personnel.

NHS utilizes Control Panel, Security Panel, and the NHS Portal, all of which are in-house developed applications. Control Panel and NHS Portal are similar and are used by customers to request changes, report incidents and view information about customer personnel authorized to carry out the above. The application used depends on the data centre(s) out of which customers receive NHS services. Control Panel also hosts documentation accessible by authorized customer personnel pertaining to customer responsibilities, communication channels, and access to services. Control Panel and NHS Portal are accessed by Bell NHS personnel to review and respond to customer requests and reports. Security Panel is used by the Security Coordination Centre (SCC) to manage physical access provisioning and revocation for the raised floor space at the following data centres: Toronto-100, Toronto-110, Toronto-104, Brampton-895, Brampton-900, Calgary-530, Calgary-800, Calgary-930, and Kamloops-146.

People

Bell Canada NHS uses several 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 Coordination 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 and NOC teams collectively carry out 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 Analysts (DCAs) also form an internal group responsible for providing 7x24 support services for on-site customer personnel, or as remote "hands and eyes" for NOC, SCC, or other internal teams as part of change implementations, or incident resolution.

Procedures

Formal IT policies and procedures exist that describe significant processes such as physical security measures, physical access provisioning, service and device deployment, change management, reporting and dealing with service incidents, and user access to tools and applications.

Formal policies and procedures exist 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 it's services are to be delivered.

Data

Data within the scope of this examination is limited to the customer reporting made available and data used to support Bell NHS controls. Authorized customer personnel may request monthly or ad-hoc reports of the individuals that accessed their cages and/or cabinets at the following sites: Toronto-100, Toronto-110, Toronto-104, Brampton-895, Brampton-900, Calgary-530, Calgary-800, Calgary-930, and Kamloops-146. The reports detail the personnel name, date and time the area was accessed.

Authorized customer contacts with access to Control Panel and NHS Portal have the ability to view service-specific information such as open tickets for system changes to core equipment, access requests, or reported incidents.

On a weekly and monthly basis, NHS management review information pertaining to SLA achievement, related performance measures, and available capacity. The reviews include power, availability, and bandwidth SLA metrics, as well as incident resolution, and capacity with respect to power, bandwidth, floor space and computing resources.

## Principal Service Commitments and System Requirements

Bell Canada designs its processes and procedures to meet its objectives for the NHS co-location services relevant to Security and Availability. Those objectives are based on the service commitments that Bell Canada makes to user entities, the laws and regulations that govern the provision of NHS co-location services, and the financial, operational, and compliance requirements that Bell Canada has established for the services.

Security and Availability commitments to user entities are documented and communicated in master services agreement and customer-specific service level schedules and customer guides, as well as in the description of the service offering provided online.

Bell Canada establishes operational requirements that support the achievement of Security and Availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Bell Canada's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific processes required in the operation of the NHS co-location services.

## 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

<u>Integrity and ethical values</u>

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.

<u>Commitment to competence</u>

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.

<u>Board of Directors, Audit Committee and Corporate Governance Committee oversight</u>

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 assesses whether 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 support the 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. IA did not conduct audits at NHS during the current year.

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 activities (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:

<u>Customers</u>

- 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

<u>Employees</u>

- 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 their processes and monitoring the operating effectiveness throughout the period. This function is accomplished as part of the risk assessment process.

Achievement of service commitments, system requirements and related performance measures, e.g., incident resolution times, are monitored by various tools and information from these is consolidated into reports that are reviewed weekly and monthly by NHS management. Required changes from the review are documented in minutes and change tickets following the meetings. A Change Advisory Board (CAB) is in place to review and approve the implementation of changes to core- or customer systems and provide input as required. CAB personnel have knowledge of system design, service commitments and the impacts to these from the implementation of the change. On a periodic basis, designated system owners and security personnel conduct reviews of personnel with logical access to core environments and key systems, e.g., Control Panel, as well as physical access to customer hosting areas. Changes arising from the review are documented and actioned by NOC personnel or the reviewers. Systems are in place to execute scheduled scans of network devices to identify variance from entity hardening standards, anomalous devices, and open ports. Results of the scans are used to initiate patching or device re-configuration activities.

As part of the corporate governance and Sarbanes-Oxley (SOX) and National Instrument 52-109 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

Access controls are implemented to prevent and detect unauthorized access to information resources used to manage the co-location services. Access controls exist across several areas:

- User access management verifies that only authorized users can access information systems
- Network access controls prevent unauthorized access to networked services
- Security monitoring controls prevent the deployment of malicious software and identify security-related events for purposes of assessment and response

### Granting customer access

Customer employees are provided access to pre-defined resources in accordance with customer requests and the rights entitled in the contracted service. Access to NHS information systems and customer environments is controlled through a formal user registration process. Customer requests for access or changes to access are requested to the NHS service desk. The NHS service desk verifies whether the request came from an authorized customer contact. Once a request for access or change to access, has been verified, the NHS service desk analyst provisions or changes the access to customer environments as entitled in the contracted service, and closes the service ticket.

### Access administration for NHS employees

NHS employees are granted access to administrative functions to NHS-managed systems following approval from NHS management. Requests for access are submitted by NHS management to the Security Services Manager for access to Control Panel or Security Panel. Requests are made to the Network Operations Centre for access to the NHS Portal, and tools used to authenticate to the core data centre network. Any requests must be made by NHS management as a pre-approval for access. Personnel with responsibility for provisioning access, will assess the appropriateness of access based on their knowledge of departments, job roles, and required accesses. Requests to the Security Services Manager, if approved, are tracked through the MACD system, and requests managed by the NOC are tracked through the JIRA ticketing system. Access approved by the Security Services Manager is provisioned by Manager, a delegate, or a system owner. Access approved by the NOC is provided by NOC personnel. The process to request, approve and provision access is the same across NHS systems and locations, the personnel charged with approving and provisioning access, and the systems used to document the requests vary depending on the customers and systems which support them.

On a monthly basis, NHS Operations management reviews the accounts of NHS employees who are able to authenticate to the core network to validate that the access remains appropriate. On a quarterly basis, NHS Operations management and the Security Services Manager review employee access to Control Panel, and Security Panel. A service ticket is created to revoke inappropriate access identified from the review and removals are executed by the NOC or the Security Services Manager.

### User authentication

NHS employees connecting to the NHS-managed systems are authenticated using user ID and password. Network devices follow a defined process for configuration where NHS has defined procedures to securely configure these devices in accordance with vendor- and industry suggested practices. Changes to configurations are subject to a change management process. Procedures are also in place to securely remove these devices from service when required.

External access to NHS networks is secured by the use of encrypted VPN services and device- and user based authentication services.

Network security

NHS management network environments are isolated from other network environments through restricted access to network segments. Authentication controls are in place to restrict access to these network segments to authorized NHS personnel

Core data centre network environments are segregated from internal Bell NHS networks. Personnel utilize jumpboxes and authenticate via unique user IDs and passwords to access the core data centre network.

Firewalls on the core network have been configured to prevent and detect unauthorized traffic. Access rules have been configured on firewalls to restrict traffic and access to systems and services. Access to the configuration of network devices (e.g., routers, switches, firewalls, network appliances) is restricted through user IDs and passwords. Knowledge of the user IDs and passwords that allow access to the network devices is restricted to authorized NHS networking personnel.

Ongoing review of critical vendor updates is in place to verify that new vulnerabilities are recognized and addressed. Changes to firewall access are documented in the change ticketing system and follow the change management process.

Network and vulnerability scans are carried out weekly to identify vulnerabilities in operating systems, unauthorized services, and open ports. Based on the severity of identified vulnerabilities, mitigating actions are identified and assigned for resolution.

Network monitoring tools are configured to automatically send alerts to the NHS network operations centre. The network operations centre then follows a formal escalation process. The process covers different types of threats, the priority level for each threat and the investigative action to be followed. In addition, periodic scans of the network are carried out to identify unauthorized devices, services, anomalous operation, and deviations from standard configurations.

## Physical Security

Physical security controls are implemented over areas where computer equipment and storage media used to provide customer services are located. These controls are provided in order to prevent unauthorized physical access, damage, and interference to this equipment.

Access to the NHS data centres is restricted to authorized individuals. NHS staff members and contractors are provided with permanent badges to the data centres. At the following sites, customer personnel who are pre-authorized are required to confirm their identity and re-enroll their accesses at each visit: Toronto-100, Toronto-110, Toronto-104, Brampton-895, Brampton-900, Calgary-530, Calgary-800, Calgary-930, and Kamloops-146. Requests to grant these individuals physical access to the data centre are approved by appropriate management within NHS and customer representatives. At the other data centres, authorized customer personnel are enrolled for access in a manner similar to employees.

Access to the data centres is granted on the basis of an individual's need to perform specific job functions. For the Maynard, Vancouver, Canniff, Markham, St-Laurent and Ottawa data centres, access is provisioned by Bell Corporate Security, whereas physical access to the Rene Levesque data centre building is provisioned by the third-party building management, and to Bell-managed rooms, cages, and cabinets by the Network Operations Centre (NOC) personnel. Access to the other data centres is provisioned by the Security Services Manager. Access to the data centres in Montreal, Ottawa, and the Canniff, Warden, and Maynard data centres is controlled primarily by electronic card system and vascular scans. Access to the data centre in Vancouver is controlled by electronic card system and PIN entry. Access to the other Toronto and Calgary data centres, and those in Brampton and Kamloops is via an electronic card and a fingerprint and weight scan. Closed circuit television monitoring covers sensitive areas at the Ottawa, Canniff, Warden, Maynard, St-Laurent, and Still Creek data centres and the footage is retained by Bell Corporate Security for review as required. Video feeds from the Rene Levesque site are monitored and retained by NOC personnel and feeds from the other sites are monitored by Security Coordination Centre (SCC) personnel.

At the following sites, customer access to their cages and cabinets is via electronic access card and fingerprint authentication: Toronto-100, Toronto-110, Toronto-104, Brampton-895, Brampton-900, Calgary-530, Calgary-800, Calgary-930, and Kamloops-146. Customers are provided access to only their cages and cabinets and upon request, may receive reports of which customer- and NHS personnel have accessed their area. At the Lepine, St-Laurent, Warden, and Rene-Levesque sites, cage access is controlled via access card, and access to cabinets is via keys which are managed using a KeyWatcher system. At the Canniff site, both cages and cabinets are accessed via KeyWatcher. At the Maynard site, cabinets are secured via a key and tumbler system. Site staff maintain control of the keys and these are retained in a secured, staff-only area. Customers have access via tumbler codes. The Vancouver sites utilizes standalone pods which are accessed by keys handled by site staff and stored in a secured staff-only area. Customers are responsible for verifying that only authorized personnel are aware of KeyWatcher or tumbler codes used to access cabinets, and that requests to remove accesses at sites which use electronic access cards and fingerprints are made timely.

Entrance points to each facility are identified and each door is assigned a door owner within NHS. For the Ottawa, Canniff, Warden, Maynard, St-Laurent, and Still Creek sites, Bell Corporate Security provides to the door owner, on a quarterly basis, a system-generated door access list. NHS door owners review the door access list to validate that access remains current and notify Bell Corporate Security to remove any inappropriate access identified. For the Rene Levesque site, door access lists are generated by NOC personnel, reviewed by a designated door owner, and the reviewed reports are returned to the NOC to execute any requested access changes. For the other sites, reports are generated by the Security Services Manager, reviewed by local data centre team leads or managers, and required access changes are executed by the Security Services Manager or a delegate. At each site, other personnel, such as the customers who require temporary access (not issued with permanent badges), customer's auditors, and customer's third-party equipment maintenance providers could be granted access to the data centres in the capacity of a guest. With the exception of the Vancouver data centre, security guards are stationed at the entrance of each data centre for guest sign-in and inspection of government-issued photo ID. Once the guest identity has been verified, the guest logs on the visitor sign-in sheet and wears a visitor ID. At the Vancouver data centre, the visitor sign-in process is conducted by data centre staff. Guests are escorted at all times when inside the building premises.

Bell Canada NHS co-locates its Rene Levesque site in a data centre owned and operated by Cologix, Inc (Cologix). On an annual basis, Bell Canada NHS management reviews the scope, control objectives, and control descriptions of the service organization controls (SOC 1) report provided by Cologix. The scope of the report is over Cologix's co-location services and the objective of the review is to determine whether the report includes the physical security controls and environmental safeguards which are relevant to Bell Canada NHS. Management reviews the audit opinion, and deviations identified in the report, if any, and follows up with Cologix management to identify compensating controls, if necessary, to mitigate associated risks.

## Environmental Protection

The NHS-managed data centres have in place environmental safeguards such as smoke detectors, fire suppression systems and building heating, ventilation and air conditioning. Climate control systems regulate air temperature within the computer rooms. Separate climate control systems are in place to protect against failure of individual HVAC units.

Temperature monitoring equipment continuously monitors environmental conditions. Alarm panels and alerts monitor and detect facility environmental settings such as moisture and temperature fluctuations. Alerts are automatically sent to the NHS operations team as well as Bell Canada's NOC, who investigates the incident, in the event of a failure of the environmental control equipment in the computer room.

Production systems are protected from power failures and other electrical anomalies. Multiple uninterruptible power supply and diesel generators exist to provide back-up power to essential operations and systems including the computer room.

An equipment and data centre maintenance program that includes at least annual maintenance or testing is in place to keep data centres and equipment in working order. The fire suppression system is tested annually. The electrical power controls are inspected and tested regularly.

As noted above, NHS management also reviews the Cologix SOC report to determine whether it includes appropriate environmental protection controls and follows-up with Cologix management as necessary.

System Operation, Service Monitoring and Reporting Programs

Bell Canada's business is organized around the consistent delivery of services to customers. As this is the foundation of Bell Canada's business, adherence is maintained to the internal policies and procedures and monitoring of the systems is performed on a continuous basis. The NOC is 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 NOC are not directed to these groups but are sent to a corporate Bell security team and/or directly to appropriate senior management members. As such, 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 Coordination 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 DCPOs 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 and NHS Portal have change logs 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 at the following sites Toronto-100, Toronto-110, Toronto-104, Brampton-895, Brampton-900, Calgary-530, Calgary-800, Calgary-930, and Kamloops-146. 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 Coordination Centre for the following sites: Toronto-100, Toronto-110, Toronto-104, Brampton-895, Brampton-900, Calgary-530, Calgary-800, Calgary-930, and Kamloops-146. 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.

The NOC monitors co-location services. Bell Canada has an established security incident response process whereby a consistent and effective approach to the management of information security incidents, communications, weakness associated with client support systems and network devices and infrastructure are reported, corrected and resolved in a timely manner.

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 Coordination Centre and the Network Operations Centre. This report is presented to Senior Management on a periodic basis to validate the prioritization and resolution of 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.

## Incident Management

NHS has established an incident management process for dealing with incidents arising from a failure or issue arising in the overall operation of the NHS environments.

NHS operations manuals document and describe the underlying processes and procedures used by NHS to fulfill its operational obligations in delivering quality service to their customers through effective and efficient standards.

Incidents include failures and questions from customers concerning the operation and usage of their individual environments, as well as those detected by NHS' internal environmental and network monitoring tools. Two core objectives underlie NHS incident management: (1) restore normal service as quickly as possible thereby minimizing the adverse impacts on customer business operations, and (2) actively communicate with customers so that that they remain abreast of the incident resolution

Incident identification occurs either when (1) an event is detected by automated monitoring tools operating in the Data Centre, (2) there is a notification to the NHS service desk originated by a customer calling or reporting an incident in Control Panel or NHS Portal, or (3) a technician logs an incident to formally respond to an event in the infrastructure.

The NHS service desk performs triage and initial incident resolution. They are the single points of contact for supporting each NHS customer for incident notification, status, and resolution information. NHS customers are assigned a service desk by the sales team. Supplied with issue segmentation knowledge and tools, the service desk identifies the nature of the issue and logs the issue in an incident ticket. The service desk either resolves the issue with the caller on the phone, providing them with information to resolve the issue themselves, if required, or escalates the ticket to the operations team.

Incident resolution times are defined and operations personnel work in accordance with operations manuals and guides to investigate and resolve issues within the defined based on the incident's category or severity. Incident tickets are resolved in accordance with the response procedures defined within Bell Canada NHS operations manuals.

For high severity incidents, a root cause analysis is prepared and reviewed by management and is then communicated to the customer. Based on the root cause analysis, additional change or incident requests are created as necessary.

On a weekly basis, NHS management reviews incidents that have not been closed. Statistics on meeting internal service level agreements are maintained and documented.

Bell Canada has a Corporate Incident Response Team (CIRT) and a National Incident Centre to respond to serious computer and network incidents or attempted incidents such as distributed denial of service attacks, denial of service attacks, or viruses. Immediate remedial measures to address any attack are made based on recommendations from the network and security staff addressing the incident. CIRT staff work with the NHS Operations team to assess and recommend what corrective measures should be made.

There have been no significant system incidents during the period of 1 January 2018 through 31 December 2018, that would impact Bell Canada's service commitments and system requirements on Security and Availability.

## Change Management

The NHS Operations Manual documents and describes the underlying processes and procedures used by NHS to facilitate the change management process through the various stages of the creation, review, approval, implementation, verification and closing of a change.

Change requests may come from the customer or may be initiated by NHS on behalf of customers to support their computing environments. Customers call or email the NHS service desk and details of the customer request are entered into Bell's ticketing system by service desk analysts. Alternately, customers with access to Control Panel and NHS Portal have the ability to request changes. Requests are directed to service desk agents who may either accept the request and add to the ticketing system, or reject it based on the nature of the request. NHS uses JIRA as the change ticketing system for changes impacting legacy NHS systems and Control Panel as the change ticketing system for changes impacting former Q9 systems. Internal change requests initiated by NHS personnel are also entered into the ticketing system.

There are two types of changes described within the change management process: (1) scheduled changes; and (2) emergency changes.

Scheduled Requests for Change (RFCs) are planned changes, which follow the standard change management process. RFCs are submitted at least one week in advance of the change implementation to allow appropriate time for technical assessments and reviews. Approvals are received prior to the scheduling and implementation of the change. In certain instances, changes that are assessed as low risk are considered pre-approved.

Emergency RFCs are unplanned changes, which follow an accelerated and escalated process resulting in a more immediate implementation into a production environment. Emergency changes require the same approvals as scheduled RFCs. They are created in response to a security breach, perceived security breach or incident resolution that has an impact on the service level agreement with the customer.

Patching activities for core network devices are within the scope of the change management process to keep them up-to-date with security requirements.

The RFC is the starting point of the change management process. When a system change is required to meet a business need, an RFC is created within the ticketing system. The RFC identifies the technical description of the change, justification for the change (the business need driving the change), details about the service to which the change applies, deadline for the change, the impact to the customer and/or environment of not implementing the change, implementation plan and a back-out plan, where applicable.

The RFC is entered into the ticketing system by a predetermined deadline in order to be validated, approved and scheduled within the earliest scheduled Maintenance window. A calendar integrated with the ticketing systems is used to track the date and time at which approved changes are to be implemented in production, this calendar is available to users with ticketing system access.

Once the RFC is submitted, technical validation commences. The Change Manager assigns the RFC to relevant subject matter experts. This review is based upon classification, scope, and potential impact. Changes that have an architectural impact are reviewed by the architecture team. assessments include considerations for the security and availability impacts of changes. Any modifications to the RFC recommended during these steps are captured in the change management system. Any changes to key device configurations (e.g., host names) are also reflected in a configuration management database (CMDB). A functionality of JIRA operates as the CMDB for devices at NHS sites and a tool called BARN is in use for devices at former Q9 sites.

Once all technical approvals are in place, the RFC is submitted by the Change Manager to the Change Advisory Board (CAB) for approval. The CAB participants are familiar with the business objectives of a customer and/or are intimate with the technical infrastructure through which the customer's service is delivered. For proposed changes which may impact on one or more shared services, and are deemed to be of higher risk, the NHS NOC Manager approves the RFC.

During the scheduled maintenance window, the change owner implements and tests the change as it was described, resourced, and approved in the RFC. The RFC ticket is changed from "Implementation in Progress" to "Verification in Progress."

The change is further tested as described in the Verification test plan. If successful, the RFC Ticket status is changed to "Successful". Otherwise, the Change Owner executes the contingency back-out plan, restoring service to its original specification.

## 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 an 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. This section describes some of the controls that should be in operation at user entities to complement the controls at Bell Canada NHS.

| 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 MSAs, Service Schedules, and customer guides. | CC2.1, CC2.2, CC2.3, CC6.1, CC6.2, CC6.4, CC6.6, CC7.1, CC7.4, CC8.1, |
| User entities are responsible for implementing appropriate logical access security measures over the system components for which they are responsible, per the user entity MSAs, Service Schedules, and customer guides. | CC6.1, CC6.2, CC6.3, CC6.6 |
| 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. | CC6.7 |
| 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. | CC6.8 |
| User entities are responsible for identifying appropriate authorized personnel, to request NHS Portal, Control Panel and physical access for other user entity personnel. | CC6.2, CC6.3, CC6.4 |
| User entities are responsible for providing timely notification to Bell Canada NHS when user entity NHS Portal and/or Control Panel users no longer require access | C6.2, CC6.3 |
| User entities are responsible for implementing controls to restrict NHS Portal and Control Panel access to authorized personnel only. | CC6.2, CC6.3, CC6.4 |
| User entities are responsible for carrying out periodic reviews of user entity NHS Portal and Control Panel users and communicating any required access changes to Bell Canada NHS timely. | CC6.2, CC6.3, CC6.4 |
| 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. | CC6.4 |
| User entities are responsible for identifying user entity personnel who will have unescorted access to their cages/cabinets. | CC6.4 |
| User entities are responsible for submitting requests for physical access via Control Panel, for personnel who do not have unescorted access privileges. | CC6.4 |
| User entities are responsible for providing timely notification to Bell Canada NHS when user entity personnel no longer require physical access. | CC6.4 |
| 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. | CC7.1, CC7.2, CC7.3 |
| User entities are responsible for implementing controls such that changes to system components are authorized, tested and approved by the user entity, if required. | CC8.1 |
| 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 back-up and system availability and recovery requirements | A1.2 |

| | |
|---|---|
| User entities that do not subscribe to back-up services are responsible for implementing and administering back-up utilities in their environments. | A1.2 |

## Complementary Subservice Organization Controls

In designing its system, Bell Canada NHS has contemplated that certain controls would be placed in operation by its subservice organization, Cologix, Inc. (Cologix). This section describes some of the controls that should be in operation at the subservice organization to complement the controls at Bell Canada NHS.

| Complementary Subservice Organization Controls | Criteria |
|---|---|
| Cologix is expected to have implemented an electronic card access system to control access to data centre rooms. | CC6.4 |
| Cologix is expected to have implemented controls to manage access to the data centre building and doors to areas controlled by Cologix, e.g., main doors, common areas. | CC6.4 |
| Cologix is expected to have implemented controls for the timely notification to NHS of changes to key contacts in their organization, and changes to the access of their employees to the NHS data centre rooms. | CC6.4 |
| Cologix is expected to have implemented controls for maintaining adequate environmental safeguards such that computing hardware is operating under manufacturer's recommended conditions (e.g., heat, humidity, air conditioning, fire suppression), reported equipment alarms are assessed and resolved in a timely manner, and that the equipment will be adequately protected against fire and other unforeseen events that can damage the equipment and prevent it from operating properly. | A1.2 |

# Applicable Trust Services Principles and Criteria, Bell's Related Controls and Ernst & Young LLP's Tests of Controls and Results

## Testing of Entity-Level Controls

In planning the nature, timing and extent of our testing of the controls specified by Bell Canada, Ernst & Young LLP (Service Auditors, we) considered the aspects of Bell Canada's control environment, risk assessment processes, information and communications, and monitoring procedures and performed such procedures that we considered necessary in the circumstances.

## Procedures for Assessing Completeness and Accuracy of Information Produced by the Entity (IPE)

For tests of controls requiring the use of Information Produced by the Entity (IPE), procedures were performed to assess the reliability of the information, including completeness and accuracy of the data or reports, to determine whether the information can be relied upon in the examination procedures. This includes IPE produced by Bell Canada and provided to user entities (if relevant and defined as part of the trust criteria), IPE used by Bell Canada management in performance of controls (i.e., periodic review of user listings), and IPE used in the performance of our examination procedures.

Based on the nature of the IPE, a combination of the following procedures were performed to address the completeness and accuracy of the data or reports used: (1) inspect source documentation relating to the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) agree data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing.

## Security Criteria

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC 1.0 | Control Environment | | | |
| CC1.1 | COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | NHS.10: Personnel are required to read and accept the Code of Conduct upon hire and annually thereafter within the HR performance management tool. | Inquired of management to determine whether personnel are required to read and accept the Code of Conduct upon hire and annually thereafter within the HR performance management tool.<br>For a selection of current employees, contractors and new hires from reports from the human resources performance management tool, inspected training reports to determine whether they complete the required acknowledgement of the Code of Conduct, annually, or upon hiring. | No deviations noted. |
| | | NHS.09: Management monitors employees' and contractors' 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. | Inquired of management to determine whether they monitor employees' and contractors' 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.<br>For a selection of quarters, inspected reports from external customer surveys and the Business Conduct Helpline to determine whether they are suitably designed to collect information around employee and contractor adherence to the Code of Conduct and whether management action is required based on reports and responses to surveys. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.53: Bell Canada policies include probation, suspension, and termination as potential sanctions for employee misconduct. | Inquired of management to determine whether Bell Canada policies include probation, suspension, and termination as potential sanctions for employee misconduct.<br>Inspected corporate policies to determine whether they include probation, suspension, and termination as potential sanctions for employee misconduct. | No deviations noted. |
| | | NHS.65: The expectations of the Board of Directors and senior management concerning integrity and ethical values are defined in the Code of Business Conduct. | Inquired of management to determine whether the expectations of the Board of Directors and senior management concerning integrity and ethical values are defined in the Code of Business Conduct.<br>Inspected the Code of Business Conduct to determine whether it describes the expectations of the Board of Directors and senior management concerning integrity and ethical values. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC1.2 | COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | NHS.66: The Board of Directors is independent from management and has established the Audit Committee and Governance Committee to provide oversight and monitoring of the organizational and governance reporting structures, and requirements for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis in accordance with the needs of each operational business unit. | Inquired of management to determine whether the Board of Directors is independent from management and has established the Audit Committee and Governance Committee to provide oversight and monitoring of the organizational and governance reporting structures, and requirements for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis in accordance with the needs of each operational business unit.<br>Inspected the BCE Annual Report to identify the members of the Board and key executives.<br>Inspected the Audit Committee Charter and Governance Committee Charter to determine whether these Committees are in place, and whether they describe the Committees' membership, and their duties and responsibilities. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC1.3 | COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | 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. | Inquired of management to determine whether Bell Canada has an up-to-date organizational chart to define reporting lines, authorities and responsibilities and whether this is revised when necessary to meet changing commitments and requirements.<br>Inspected the organizational chart on the internal human resources performance management tool to determine whether it defines reporting lines and authorities and whether it defines responsibilities via job titles.<br>Inquired with Bell Canada personnel around their reporting lines, authorities and responsibilities to determine whether the organization chart was current. | No deviations noted. |
| | | NHS.02: Job roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors. Job descriptions are updated accordingly when a job is open for hiring. | Inquired of management to determine whether job roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors. Inquired of management to determine whether job descriptions are reviewed for needed changes and updated accordingly when a job is open for hiring.<br>For a selection of roles identified from the organization chart on the human resources performance management tool, inspected a selection of job descriptions, to determine whether they define job roles and responsibilities, and whether job descriptions are updated as needed. | No deviations noted. |
| | | NHS.66: Refer to CC1.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC1.4 | COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | NHS.03: Employee and contractor 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. | Inquired of management to determine whether employee and contractor performance, personal and career goals are reviewed by management on an annual basis. inquired of management to determine whether during the review, job duties may be identified for changes and required training is established.<br>For a selection of current employees and contractors from the organization chart, inspected performance review documentation to determine whether performance, personal and career goals are reviewed by management annually, whether job duties are identified for changes, and whether training is assigned as necessary. | No deviations noted. |
| | | NHS.06: Bell Canada administers and monitors skills training commensurate with its commitments and requirements for employees and contractors through the corporate HR performance management tool. | Inquired of management to determine whether Bell Canada administers and monitors training commensurate with its commitments and requirements for employees and contractors through the corporate HR performance management tool.<br>For a selection of current employees and contractors from the human resources performance management tool, inspected training reports and dashboards, to determine whether training is assigned, completion is monitored by management, and whether training is commensurate with Bell Canada's commitments and requirements for employees and contractors. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.07: Personnel are required to attend annual security training. Management monitors compliance with training requirements through the corporate HR performance management tool. | Inquired of management to determine whether personnel are required to attend annual security training, and whether management monitors compliance with training requirements through the corporate HR performance management tool.<br>For a selection of current employees and contractors from a report from the human resources performance management tool, inspected training reports and dashboards, to determine whether the employees and contractors complete annual security training, and whether management monitors compliance with training requirements. | No deviations noted. |
| | | NHS.11: Personnel must pass a criminal background check before they may be hired by the entity. | Inquired of management to determine whether personnel must pass a criminal background check before they may be hired by the entity.<br>For a selection of new hires, including contractors from a report from the human resources performance management tool, inspected their CPIC reports to determine whether personnel pass a criminal background check with no significant issues, prior to their start date. | No deviations noted |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.05: Candidates' abilities to meet job requirements are evaluated as part of the hiring or transfer evaluation process. | Inquired of management to determine whether candidates' abilities to meet job requirements are evaluated as part of the hiring or transfer evaluation process.<br>For a selection of new hires or transfers going into technical roles, including contractors, from a report from the human resources performance management tool, inspected knowledge assessment questionnaires, to determine whether their ability to meet job requirements are evaluated as part of the hiring process. | No deviations noted. |
| | | NHS.02: Refer to CC1.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.09: Refer to CC1.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.10: Refer to CC1.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC1.5 | COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | NHS.67: An internal audit group has been established to assist the Audit Committee in assessing and reporting on the effectiveness of internal controls. | Inquired of management to determine whether an internal audit group has been established to assist the Audit Committee in assessing and reporting on the effectiveness of internal controls.<br>Inspected the Audit Committee Charter, internal audit policies and internal audit plans to determine whether an internal audit group has been established to assist the Audit Committee in assessing and reporting on the effectiveness of internal controls. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.68: The President and Chief Executive Officer, Executive Vice-President and Chief Financial Officer, and Senior Vice-President and Controller sign-off on their management responsibility over the effectiveness of internal controls. | Inquired of management to determine whether the President and Chief Executive Officer, Executive Vice-President and Chief Financial Officer, and Senior Vice-President and Controller sign-off on their management responsibility over the effectiveness of internal controls.<br>Inspected the BCE Annual Report to determine whether the President and Chief Executive Officer, Executive Vice-President and Chief Financial Officer, and Senior Vice-President and Controller sign-off on their management responsibility over the effectiveness of internal controls. | No deviations noted. |
| | | NHS.69: Requirements for ongoing confidentiality and non-disclosure survive employment. As per the Personnel Security Policy, management reviews with the employee or contractor involved his/her continuing obligations under the Bell Code of Business Conduct and other relevant policies (including Human Resources policies). | Inquired of management to determine whether requirements for ongoing confidentiality and non-disclosure survive employment and whether, management reviews with the employee or contractor involved his/her continuing obligations under the Bell Code of Business Conduct and other relevant policies (including Human Resources policies).<br>Inspected the Personnel Security Policy to determine whether confidentiality and non-disclosure survive employment and whether it requires that upon the end of employment, management reviews with the employee or contractor involved his/her continuing obligations under the Bell Code of Business Conduct and other relevant policies. | No deviations noted. |
| | | NHS.02: Refer to CC1.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.03: Refer to CC1.4 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

<table>
<tr><th>Ref.</th><th>Criteria Description</th><th>Controls Specified by Bell Canada</th><th>Ernst & Young LLP's Testing Procedures</th><th>Results of Tests</th></tr>
<tr><td rowspan="4"></td><td rowspan="4"></td><td colspan="3">NHS.09: Refer to CC1.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests.</td></tr>
<tr><td colspan="3">NHS.10: Refer to CC1.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests.</td></tr>
<tr><td colspan="3">NHS.53: Refer to CC1.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests.</td></tr>
<tr><td colspan="3">NHS.66: Refer to CC1.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests.</td></tr>
</table>

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC 2.0 | Communication and Information | | | |
| CC2.1 | COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control | NHS.13: 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 describes key aspects of processing. | Inquired of management to determine whether internal procedure documents and operating manuals are posted on the intranet and are available to the internal users, and whether they delineate the boundaries of the system and services, and describe key aspects of processing.<br>Inspected Control Panel, NHS Portal, and internal NHS websites to determine whether procedure documents and operating manuals are available to the internal users, whether they delineate the boundaries of the system and services, and describe key aspects of processing. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.14: 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 Canada identifies responsible personnel and communication channels with customers, e.g., a generic NOC email address, customer account managers. | Inquired of management to determine whether 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. Inquired of management to determine whether Bell Canada identifies responsible personnel and communication channels with customers, e.g., a generic NOC email address, customer account managers.<br>For a selection of customers from a listing of co-location services customers, inspected the MSA, Acceptable Use Policies, Service Schedules, and customer guides to determine whether they delineated the parties responsible, accountable, consented, and informed of changes in design and operation of key system components. Inspected these to determined whether they identify responsible personnel and communication channels with customers. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.16: Availability, and incident resolution for system components, are monitored at weekly 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. | Inquired of management to determine whether availability and incident resolution for system components, are monitored at weekly meetings, whether results are shared with applicable personnel, and whether actions are taken and communicated to relevant parties as required. Inquired of management to determine whether customer responsibilities are listed in the SLA and in system documentation.<br>For a selection of weekly meetings, inspected reports and meeting minutes to determine whether availability and incident resolution for system components, are monitored, whether attendees at the meetings are appropriate to assess results and assign activities to resolve issues, and whether actions are taken and communicated to relevant parties as required.<br>For a selection of customers from a listing of co-location services customers, inspected Service Schedules and customer guides to determine whether customer responsibilities are listed. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.20: A master list of Bell Canada's system components is maintained on Bell's Canada'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. | Inquired of management to determine whether a master list of Bell Canada's system components is maintained on Bell Canada's asset management tool, accounting for additions and removals, and whether the tool captures key system components, technical and installation specific implementation details, and supports ongoing asset and service management commitments and requirements.<br>Inspected Bell's Canada's asset management tools, Configuration Management Database (CMDB) and BARN, to determine whether they host master lists of Bell Canada's system components, i.e., servers and network devices.<br>For a selection of system components from CMDB and BARN, inspected the relevant entries to determine customer and installation-specific information is retained, whether changes in components and components configurations are captured, and whether they are used to support ongoing asset and service management commitments and requirements. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.04: 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. | Inquired of management to determine whether Bell Canada has defined a formal risk management process that specifies risk tolerances, roles and responsibilities in the risk management process, and the process for evaluating  risks based on identified threats and the specified tolerances.<br>Inspected the risk management process documentation to determine whether it specifies risk tolerances, roles, responsibilities and the process for evaluating and mitigating risks based on threats, impacts and tolerances. | No deviations noted. |
| | | NHS.27: Vulnerability scans are performed weekly. Issues are remediated based on severity. | Inquired of management to determine whether vulnerability scans are performed weekly and whether issues are remediated based on severity.<br>For a selection of weeks, inspected vulnerability scan results to determine whether scans are performed weekly, and inspected whether vulnerabilities if any, are assigned for resolution and are resolved based on severity. | No deviations noted. |
| | | NHS.28: Network scans are performed weekly. Issues are remediated based on severity. | Inquired of management to determine whether network scans are performed weekly and whether issues are remediated based on severity.<br>For a selection of weeks, inspected network scan results to determine whether scans are performed weekly, and inspected whether vulnerabilities if any, are assigned for resolution and are resolved based on severity. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.57: The nature and extent of the protections in place for critical infrastructure components, e.g., back-up power, at NHS-managed data centres are assessed to be appropriate for the level of risk faced by the components, e.g., sufficient redundancy. The assessment is annual. | Inquired of management to determine whether the nature and extent of the protections in place for critical infrastructure components at NHS-managed data centres, are assessed to be appropriate for the level of risk faced by the components, and whether the assessment is annual.<br>Inspected the Data Centre Risk Assessment to determine whether it assesses the nature and extent of the protections in place for critical infrastructure components at NHS-managed data centres to be appropriate for the level of risk faced by the components. | No deviations noted. |
| CC2.2 | COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | NHS.70: Documented escalation procedures are available to internal users to guide users in identifying and reporting security incidents, availability issues, concerns, and other complaints. | Inquired of management to determine whether documented escalation procedures are available to internal users to guide users in identifying and reporting security incidents, availability issues, concerns, and other complaints.<br>Inspected corporate security policies and their location on the Bell Canada intranet to determine whether escalation procedures are available to internal users to guide them in identifying and reporting security incidents, availability issues, concerns, and other complaints. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.50: 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. | Inquired of management to determine whether operations personnel follow documented procedures for evaluating, classifying, escalating, and resolving reported events as required.<br>Inspected operations manuals and guides, to determine whether procedures are in place for evaluating, classifying, escalating, and resolving reported events.<br>For a selection of incidents, from JIRA and Control Panel queues, inspected tickets to determine whether operations personnel follow procedures from the operations manuals and guides when evaluating, classifying, escalating, and resolving reported events. | No deviations noted. |
| | | NHS.75: Bell Canada promotes familiarity of security policies, practices and standards to employees and, where relevant, contractors who use Bell Canada data centres and information systems through the use of messages included as part of the weekly corporate-wide correspondence. | Inquired of management to determine whether Bell Canada promotes familiarity of security policies, practices and standards to employees and, where relevant, contractors who use Bell Canada data centres and information systems through the use of messages included as part of the weekly corporate-wide correspondence.<br>Inspected a selection of weekly corporate-wide correspondences (Bell-in-Brief) to determine whether the communication has been published on Bell Canada's intranet and that the communication includes updates to security policies, practices and standards. | No deviations noted. |
| | | NHS.13: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.02: Refer to CC1.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.06: Refer to CC1.4 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.07: Refer to CC1.4 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.66: Refer to CC1.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC2.3 | COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | NHS.12: 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. | Inquired of management to determine whether 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.<br>For a selection of customers, from a listing of co-location services customers, inspected the MSA, Acceptable Use Policies, Service Schedule, and customer guides to determine whether they delineate the boundaries of the service, and describe relevant services components as well as the purpose and design of the services.<br>Inspected Control Panel and NHS Portal to determine whether customer guides are made available to authorized external users and they contain relevant service-related information. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.15: Bell Canada's security and availability commitments regarding the services are included in the master services agreement and customer-specific service level schedules. | Inquired of management to determine whether Bell Canada's security and availability commitments regarding the services are included in the master services agreement and customer-specific service schedules.<br>For a selection of customers from a listing of co-location services customers, inspected the MSA, related Service Schedules, and SLAs to determine whether Bell Canada's security and availability commitments regarding the services are included. | No deviations noted. |
| | | NHS.71: Bell Canada issues an annual report to all external parties that includes matters affecting the functioning of internal control and specific reports on internal control performance for specific business units. | Inquired of management to determine whether Bell Canada issues an annual report to all external parties that includes matters affecting the functioning of internal control and specific reports on internal control performance for specific business units.<br>Inspected the BCE Annual Report to determine whether it includes a report on matters affecting the functioning of internal control.<br>Inspected third-party assurance reports on internal control performance for specific business units or services. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.17: Proposed system shutdowns associated with changes that affect external parties are communicated before their implementation. | Inquired of management to determine whether proposed system shutdowns associated with changes that affect external parties are communicated before their implementation.<br>For a selection of change requests from JIRA and Control Panel, inspected change tickets and emails to determine whether proposed system shutdowns associated with changes that affect external parties are communicated before their implementation. | No deviations noted. |
| | | NHS.19: For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, additional change or incident requests are created as necessary. | Inquired of management to determine whether for high severity incidents, a root cause analysis is prepared and reviewed by operations management and whether based on the root cause analysis, additional change or incident requests are created as necessary.<br>For a selection of high severity incident tickets from JIRA and Control Panel, inspected tickets to determine whether a root cause analysis is prepared, if necessary, and reviewed, and whether additional change or incident requests are created. | No deviations noted. |
| | | NHS.14: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.09: Refer to CC1.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC 3.0 | Risk Assessment | | | |
| CC3.1 | COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | NHS.72: Management establishes objectives consistent with standards and frameworks of recognized external organizations. | Inquired of management to determine whether management establishes objectives consistent with standards and frameworks of recognized external organizations.<br>Inspected internal audit policies and manuals to determine whether control frameworks are consistent with recognized external organizations. | No deviations noted. |
| | | NHS.14: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.15: Refer to CC2.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.04: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.13: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC3.2 | COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. | NHS.21: 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. | Inquired of management to determine whether 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.<br>For a selection of quarters, inspected the quarterly risk assessments to determine whether 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. | No deviations noted. |
| | | NHS.22: Identified risks are rated using a risk evaluation process and ratings are reviewed by management. | Inquired of management to determine whether identified risks are rated using a risk evaluation process and ratings are reviewed by management.<br>For a selection of quarters, inspected quarterly risk assessments to determine whether identified risks are rated using a risk evaluation process and ratings are reviewed by management. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.23: 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 Sr. Manager, Network Operations. | Inquired of management to determine whether the Security team executes or assigns risk mitigating activities, evaluates the effectiveness of controls and mitigation strategies in meeting identified risks, recommends changes based on its evaluation, and whether recommendations are reviewed and approved by the Sr. Manager, Network Operations<br>For a selection of quarters, inspected quarterly risk assessments to determine whether the Security team executes or assigns risk mitigating activities, evaluates the effectiveness of controls and mitigation strategies in meeting identified risks, recommends changes based on its evaluation, and whether recommendations are reviewed and approved by the Sr. Manager, Network Operations. | No deviations noted. |
| | | NHS.04: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.28: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.27: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC3.3 | COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | NHS.24: Control self-assessments are performed by operating units on an annual basis. | Inquired of management to determine whether control self-assessments are performed by operating units on an annual basis.<br>Inspected the annual self-assessment for Bell Canada NHS controls to determine whether information around the execution of the control is documented. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.21: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.22: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.23: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.71: Refer to CC2.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.09: Refer to CC1.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC3.4 | COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | NHS.04: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.21: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC 4.0 | Monitoring Activities | | | |
| CC4.1 | COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | NHS.25: Internal audits are performed based on the annual risk-based internal audit plan. As required, corrective actions from past audit findings are assessed. | Inquired of management to determine whether internal audits are performed based on the annual risk-based internal audit plan, and whether, corrective actions from past audit findings are assessed as required.<br>Inspected the annual internal audit plan and inspected documentation from a selection of internal audits to determine whether these are executed, findings are addressed, and corrective actions from past audit findings are assessed. | No deviations noted. |
| | | NHS.26: IT DR plans and data centre BC plans are tested annually. | Inquired of management to determine whether IT DR plans and data centre BC plans are tested annually.<br>Inspected the annual IT DR and data centre BC plan test documentation, including any incident tickets, change tickets, or related documentation to determine whether plans are tested. | No deviations noted. |
| | | NHS.51: DR test results are reviewed and the contingency plan is adjusted. | Inquired of management to determine whether DR test results are reviewed and the contingency plan is adjusted.<br>Inspected DR test results to determine whether DR test results are reviewed by senior operations management, and the contingency plan is adjusted, if required. | No deviations noted. |
| | | NHS.04: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.24: Refer to CC3.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.27: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.28: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC4.2 | COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.23: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.25: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.51: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC 5.0 | Control Activities | | | |
| CC5.1 | COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | NHS.22: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.23: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.04: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.50: Refer to CC2.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.25: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.13: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.72: Refer to CC3.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC5.2 | COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | NHS.08: Management evaluates the need for additional tools and resources in order to achieve business objectives, as part of weekly KPI meetings. | Inquired of management to determine whether they evaluate the need for additional tools and resources in order to achieve business objectives, as part of weekly KPI meetings.<br>For a selection of weeks, inspected Omnia KPI reports and KPI meeting minutes to determine whether management monitors service level metrics, and evaluates the need for additional tools and resources in order to achieve business objectives, in accordance with service level reporting. | No deviations noted. |
| | | NHS.04: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.50: Refer to CC2.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.70: Refer to CC2.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.72: Refer to CC3.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.13: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC5.3 | COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | NHS.73: Bell Canada has developed policies and procedures that outline the control activities that support security and availability requirements.  Policies include the Information Security policy, Acceptable Use of Information Technology Resources policy, Privacy Policy and guidance, Information Management policy, Encryption Directive, Mobile Security Directive and the Telework Policy. Policies and directives are updated on an annual basis. | Inquired of management to determine whether Bell Canada has developed policies and procedures that outline the control activities that support security and availability requirements, and whether policies and directives are updated on an annual basis<br>Inspected a selection of policies, directives, and procedure documents including the Information Security policy, Operations Manual, Information Management Policy, and Personnel Security Policy and determined that they outline the control activities that support security and availability requirements.<br>Inspected the policies and directives to determine whether they are updated on an annual basis. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.62: Mobile Device Management (MDM) tools are installed on corporate mobile devices to enforce administrator-defined policies, e.g., encryption, remote wiping. | Inquired of management to determine whether MDM tools are installed on corporate mobile devices to enforce administrator-defined policies, e.g., encryption, remote wiping.<br>Inspected corporate policies to determine security requirements for mobile devices with access to Bell Canada NHS internal networks.<br>Inspected the MDM and its configuration on a corporate mobile device to determine that it in place and set up in accordance with corporate policies. | No deviations noted. |
| | | NHS.13: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.02: Refer to CC1.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.23: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.01: Refer to CC1.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC 6.0 | Logical and Physical Access Controls | | | |
| CC6.1 | The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. | NHS.30: Customer environments and core network environments are accessed via jumpboxes which require a unique user ID and password. Access to management applications(Control Panel, Security Panel, NHS Portal) require separate, unique, credentials. | Inquired of management to determine whether customer environments and core network environments are accessed via jumpboxes which require a unique user ID and password and whether access to management applications, e.g., Control Panel require separate, unique, credentials<br>Observed that a unique user ID and password are required to access jumpboxes.<br>Observed that a separate, unique user ID and password are required for access to Control Panel, Security Panel, and NHS Portal.<br>Inspected password configurations for jumpboxes, Control Panel, Security Panel, and NHS Portal to determine whether passwords are enforced by separate systems and are in accordance with NHS standards. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.29: Access to the management network and customer environments is reviewed periodically to confirm that access privileges remain authorized and appropriate. Any required changes of access privilege are modified in a timely manner. | Inquired of management to determine whether access to the management network and customer environments is reviewed periodically to confirm that access privileges remain authorized and appropriate, and whether any required changes of access privilege are modified in a timely manner.<br>For a selection of quarters, inspected reviews of access to the management network (Control Panel, Security Panel), and for a selection of months inspected reviews of access to the customer environment, to determine whether management confirm that access privileges remain authorized and appropriate, and whether any required changes of access privilege are modified in a timely manner. | No deviations noted. |
| | | NHS.34: External access to the Management Network by employees and contractors is permitted only through an encrypted virtual private network (VPN) connection and multi-factor authentication. | Inquired of management to determine whether external access to the Management Network is permitted only through an encrypted virtual private network (VPN) connection and multi-factor authentication.<br>Inspected the configuration of the VPN client to determine whether VPN connections are encrypted and require multi-factor authentication. | No deviations noted. |
| | | NHS.35: Password complexity standards are established to restrict access to management tools. | Inquired of management to determine whether password complexity standards are established to restrict access to management tools.<br>Inspected corporate policies and standards to determine whether password complexity standards are established to restrict access to management tools. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.36: Role-based access controls limit access to Control Panel and Security Panel. | Inquired of management to determine whether role-based access controls limit access to Control Panel and Security Panel.<br>Inspected configurations in Control Panel and Security Panel to determine whether role-based access controls are in place. | No deviations noted. |
| | | NHS.45: External points of connectivity are protected by a firewall complex. | Inquired of management to determine whether external points of connectivity are protected by a firewall complex.<br>Inspected a network diagram to determine whether external points of connectivity are protected by a firewall complex. | No deviations noted. |
| | | NHS.46: Firewall hardening standards are used to configure new firewalls and are based on relevant applicable technical specifications, and product and industry recommended practices. | Inquired of management to determine whether firewall hardening standards are used to configure new firewalls and are based on relevant applicable technical specifications, and product and industry recommended practices.<br>Inspected the checklist used during the deployment of firewalls to determine whether it includes considerations for vendor updates and configurations, and data centre industry-specific configurations.<br>For a selection of firewalls from the configuration management database and BARN, inspected deployment tickets, firewall policies and firewall configurations to determine whether they are configured in accordance with the firewall deployment checklist. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.37: Access control devices have been installed that limit access to the NHS-managed data centre facilities. | Inquired of management to determine whether access control devices have been installed that limit access to the NHS-managed data centre facilities.<br>Observed that at each of the NHS data centres, access control devices have been installed at entry points to sensitive areas in the data centre. | No deviations noted |
| | | NHS.76: Firewall access rules are defined and configured to prevent and detect unauthorized traffic. Firewalls has been set-up in a redundant failover configuration. | Inquired of management to determine whether firewall access rules were defined and configured to prevent and detect unauthorized traffic.<br>Inquired of management to determine whether, firewalls have been set-up in a redundant failover configuration.<br>Inspected a selection of firewalls from the configuration management database to determine whether access rules were configured to restrict traffic and are deployed in a redundant configuration. | No deviations noted |
| | | NHS.77: Access to administrative functions on NHS-managed systems is restricted to appropriate individuals based on job function | Inquired of management to determine whether access to administrative functions on NHS-managed systems is restricted to appropriate individuals based on job functions.<br>For a selection of NHS-managed servers from the configuration management database and BARN, inspected the list of accounts with access to administrative functions to determine whether such access is restricted to appropriate individuals based on job function. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.74: A policy governing access to information and uses of removable media has been established, approved by management and communicated to employees and contractors through the corporate intranet. | Inquired of management to determine whether a policy governing access to information and uses of removable media has been established, approved by management and communicated to employees and contractors through the corporate intranet.<br>Inspected corporate policies governing access to information and uses of removable media to determine that they are approved by management.<br>Inspected the Bell Canada intranet to determine whether these policies are communicated to employees and contractors through the corporate intranet. | No deviations noted. |
| | | NHS.81: For NHS employees and contractors, access requests to set up a new user account in NHS systems and customer environments, if applicable, or to modify the access privileges of an existing account are approved by appropriate management. | Inquired of management to determine whether for NHS employees and contractors, access requests to set up a new user account in NHS systems and customer environments, modify the access privileges of an existing account, or remove the access of a user are approved by NHS management.<br>For a selection of new and modified user accounts in NHS systems and customer environments for employees and contractors, inspected access requests to determine whether they were approved by NHS management and whether accesses granted are in accordance with those approved. | No deviations noted. |
| | | NHS.20: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC6.2 | Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. | NHS.33: Customer accounts are created based on authorization of the designated customer point of contact through the Control Panel and NHS Portal. | Inquired of management to determine whether customer accounts are created based on authorization of the designated customer point of contact through the Control Panel and NHS Portal.<br>For a selection of customer access creation requests from Control Panel and NHS Portal queues, inspected access creation requests and system accesses to determine whether customer accounts are created based on authorization of the designated customer point of contact and accesses created correspond to the accesses that are approved. | No deviations noted |
| | | NHS.32: Customer accounts are removed for users that no longer require access from the Control Panel and NHS Portal in a timely manner. | Inquired of management to determine whether customer accounts are removed for users that no longer require access from the Control Panel and NHS Portal in a timely manner.<br>For a selection of customer access removal requests from Control Panel and NHS Portal queues, inspected access removal requests and system accesses to determine whether customer accounts are removed timely. | No deviations noted |
| | | NHS.31: For Bell Canada employees and contractors, access to systems is removed within a timely manner. | Inquired of management to determine whether for Bell Canada employees and contractors, access to systems is removed within a timely manner.<br>For a selection of terminations from the a report from the human resources performance management tool, inspected access removal requests for employees and contractors, and system accesses to determine whether access is removed timely. | No deviations noted |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.29: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.81: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC6.3 | The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. | NHS.36: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.33: Refer to CC6.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.32: Refer to CC6.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.31: Refer to CC6.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC6.4 | The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. | NHS.38: Bell Canada's employee, contractors and customer access to data centre facilities is restricted and is appropriately authorized based on access required. | Inquired of management to determine whether employee, contractor, and customer access to data centre facilities is restricted and is appropriately authorized based on access required.<br>For a selection of new employee and contractor access granted to the data centre facilities, inspected access request tickets and system access granted to determine whether temporary or permanent access is approved by appropriate management and is provisioned in accordance with the request.<br>For a selection of customer access requests from the Control Panel acccess provisioning queue, and access granted to individuals from reports generated by the door access systems, inspected the access request tickets and access granted to determine whether temporary or permanent access is approved by appropriate management and is provisioned in accordance with the request. | No deviations noted |
| | | NHS.39: Valid identification and sign-in is required for visitors and contractors requesting access to the data centre facilities. Access cards. if issued, are required to be returned to Bell Canada at the end of the visit. | Inquired of management to determine whether valid identification and sign-in is required for visitors and contractors requesting access to the data centre facilities, and whether an access card, if issued, is required to be returned to Bell Canada at the end of the visit.<br>Observed at each of the NHS data centres, that valid identification and sign-in is required for visitors and contractors requesting access to the data centre facilities, that visits are logged in a log-book, and that access cards, if issued are is required to be returned to at the end of the visit. | No deviations noted |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.40: Visitor accesses are recorded and visitor cards do not permit access to any secured areas of the facility. | Inquired of management to determine whether visitor accesses are recorded and visitor cards do not permit access to any secured areas of the facility.<br>Observed the log-book and sign-in forms at each data centre to determine whether visits are recorded, including information about each visitor, Bell Canada contact, and the date and time of the visit.<br>Observed during visits to data centres, that visitor cards do not permit access to any secured areas of the facility. | No deviations noted |
| | | NHS.41: All visitors must be escorted by a Bell Canada employee or contractor when visiting facilities where sensitive system and system components are maintained and operated. | Inquired of management to determine whether visitors must be escorted by a Bell Canada employee or contractor when visiting facilities where sensitive system and system components are maintained and operated.<br>Observed at each data centre, that visitors must be escorted by a Bell Canada employee or contractor when visiting facilities where sensitive system and system components are maintained and operated. | No deviations noted |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.42: Access for terminated Bell Canada customers, employees and contractors who no longer require access is removed in a timely manner. | Inquired of management to determine whether access for terminated Bell Canada customers, employees and contractors who no longer require access is removed in a timely manner.<br>For a selection of terminations from reports provided by human resources, inspected the access removal tickets and the status of authentication access credentials to determine whether these are revoked timely.<br>For a selection of customer requests from the Control Panel acccess removal queue, and access removed for individuals from reports generated by the door access systems, inspected the access removal tickets and the status of authentication access credentials to determine whether these are revoked timely. | No deviations noted |
| | | NHS.43: Owners of sensitive areas of the facilities review the list of names and roles of those granted physical access to their areas on a periodic basis to check for continued business need. Requests for changes are made through the change management record system. | Inquired of management to determine whether owners of sensitive areas of the facilities review the list of names and roles of those granted physical access to their areas on a periodic basis to check for continued business need. Requests for changes are made through the change management record system.<br>For a selection of quarters, inspected the reviews of access to sensitive areas of the facilities to determine whether owners review the list of names and roles of those granted physical access to their areas to check for continued business need. Inspected requests for changes to determine whether these are made through the change management record system and whether access removals, if required, were completed timely. | No deviations noted |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.44: The sharing of access badges and tailgating are prohibited by policy. | Inquired of management to determine whether the sharing of access badges and tailgating are prohibited by policy.<br>Inspected corporate policies to determine whether the sharing of access badges and tailgating are prohibited by policy. | No deviations noted |
| | | NHS.63: Closed circuit television monitoring equipment exists and covers sensitive areas of the data centres. | Inquired of management to determine whether closed circuit television monitoring equipment exists and that it covers sensitive areas of the NHS data centres.<br>Observed at each of the NHS data centres, that closed circuit television monitoring equipment exists to cover server rooms at each of the NHS data centres.<br>Inspected a selection of closed circuit television recordings to determine whether recordings are retrievable for review as necessary. | No deviations noted |
| | | NHS.37: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC6.5 | The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | NHS.47: Corporate policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted. | Inquired of management to determine whether corporate policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted.<br>Inspected the Code of Conduct and corporate policies and standards to determine whether entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths (for example, e-mail) unless it is encrypted. | No deviations noted |
| | | NHS.82: Decommissioning of physical and virtual devices follow documented procedures and are part of the change management process. | Inquired of management to determine whether decommissioning of physical and virtual devices follow documented procedures and are part of the change management process.<br>For a selection of device decommissions from the Control Panel and JIRA queues, inspected change tickets to determine whether decommissioning procedures are followed, and the decommissioning was subject to the change management process. | No deviations noted. |
| | | NHS.83: Removal of production physical devices from the data centre requires data centre protection officer supervision. | Inquired of management to determine whether removal of production physical devices from the data centre requires data centre protection officer supervision.<br>For each of the NHS data centres, observed that points through which equipment can be brought in, or removed from the data centre require manual input from a data centre protection officer to allow ingress/egress. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC6.6 | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | NHS.47: Refer to CC6.5 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.34: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.35: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.30: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.45: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.46: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC6.7 | The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | NHS.35: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.34: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.30: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.74: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.62: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC6.8 | The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.28: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.27: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.45: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.76: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC7.0 | System Operations | | | |
| CC7.1 | To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. | NHS.16: Refer to C2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.27: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.28: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.50: Refer to CC2.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC7.2 | The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. | NHS.78: NHS management review the scope, control objectives, and control descriptions of any relevant service organization report, on an annual basis, to verify the report identifies all internal controls relevant to physical access management. | Inquired of management to determine whether they review the scope, control objectives, and control descriptions of any relevant service organization report, on an annual basis, to verify the report identifies all internal controls relevant to physical access management.<br>Inspected the Service Organization Control (SOC) report assessment prepared by management for the subservice organization which executes physical access management controls at a data centre, and determined that the assessment includes a review of the scope, control objectives, control descriptions, testing procedures and testing results. | No deviations noted |
| | | NHS.80: NHS management review the audit opinion and any deviations included in the service organization report, on an annual basis, and follow up with subservice organization management to identify compensating controls, if necessary, to mitigate associated risks. | Inquired to management to determine whether NHS management reviewed the audit opinion and any deviations included in the service organization report, on an annual basis, and followed up with subservice organization management to identify compensating controls, if necessary, to mitigate associated risks.<br>Inspected the Service Organization Control (SOC) report and SOC report assessment prepared by management to determine whether their assessment and follow-up over the audit opinion and deviations, if any, is appropriate. | No deviations noted |
| | | NHS.16: Refer to C2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.27: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.28: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.63: Refer to CC6.4 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.50: Refer to CC2.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.45: Refer to CC6.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC7.3 | The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. | NHS.52: Internal and external users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part. | Inquired of management to determine whether internal and external users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.<br>For a selection of incidents from the JIRA and Control Panel queues, inspected tickets and related correspondence, e.g., emails, to determine whether Bell Canada personnel, and if necessary, customers and third-parties, are informed of incidents timely and advised of corrective measures to be performed by them. | No deviations noted |
| | | NHS.50: Refer to CC2.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.24: Refer to CC3.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.25: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.19: Refer to CC2.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC7.4 | The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. | NHS.50: Refer to CC2.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.19: Refer to CC2.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| CC7.5 | The entity identifies, develops, and implements activities to recover from identified security incidents. | NHS.61: The entity uses its multi-location facilities to permit the resumption of IT operations in the event of a disaster at its data centres, for clients that subscribe to such services. | Inquired of management to determine whether Bell Canada uses its multi-location facilities to permit the resumption of IT operations in the event of a disaster at its data centres, for clients that subscribe to such services.<br>Inspected a network diagram, failover configurations and system information from devices, to determine whether devices are configured to failover to a secondary data centre, in the event of a disaster at the primary location, for a client that subscribes to multi-location services. | No deviations noted |
| | | NHS.26: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.51: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.19: Refer to CC2.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC8.0 | Change Management | | | |
| CC8.1 | The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. | NHS.54: Production change requests are evaluated at key points to determine the potential effect of the change on security and availability commitments and requirements. | Inquired of management to determine whether production change requests are evaluated at key points to determine the potential effect of the change on security and availability commitments and requirements.<br>For a selection of change requests from the JIRA and Control Panel change queues, inspected the change tickets to determine whether they include assessments of the impact of the change to Bell Canada's security and availability commitments and requirements. | No deviations noted |
| | | NHS.55: Changes that are not pre-approved, are reviewed and approved by the Change Advisory Board (CAB) prior to implementation. The CAB is comprised of Change Managers and Subject Matter Experts. | Inquired of management to determine whether changes that are not pre-approved, are reviewed and approved by the Change Advisory Board (CAB) prior to implementation, and whether the CAB is comprised of Change Managers and Subject Matter Experts.<br>For a selection of change requests from the JIRA and Control Panel change queues, inspected change tickets to determine whether changes that are not pre-approved, are reviewed and approved by the CAB prior to implementation.<br>For a selection of change requests from JIRA and Control Panel, inspected CAB meeting minutes to determine whether the CAB is comprised of Change Managers and Subject Matter Experts. | No deviations noted |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.56: Changes are tested prior to implementation, or validated post-implementation if pre-implementation testing is not feasible. | Inquired of management to determine whether changes are tested prior to implementation, or validated post-implementation if pre-implementation testing is not feasible.<br>For a selection of change requests from the JIRA and Control Panel change queues, inspected change tickets to determine whether changes are tested prior to implementation, or validated post-implementation if pre-implementation testing is not feasible. | No deviations noted |
| | | NHS.18: The system change calendar that indicates CAB approved changes to be implemented is posted on the entity's intranet. | Inquired of management to determine whether the system change calendar that indicates CAB approved changes to be implemented is posted on the entity's intranet.<br>Inspected the system change calendar that indicates CAB approved changes to be implemented on the Bell Canada NHS intranet.<br>For a selection of change requests from JIRA and Control Panel, inspected change tickets and the change calendar to determine whether CAB approved changes are identified in the system change calendar. | No deviations noted |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.48: Patching for devices is performed in accordance with client requests. Patching follows the change management process. | Inquired of management to determine whether patching for devices is performed in accordance with client requests, and whether patching follows the change management process.<br>For a selection of patching requests from the JIRA and Control Panel queues, inspected the tickets to determine whether patching is performed in accordance with client requests, and whether patching follows the change management process. | No deviations noted |
| | | NHS.49: The ability to patch devices is restricted to system administration personnel. | Inquired of management to determine whether the ability to patch devices is restricted system administration personnel.<br>For a selection of managed devices from the configuration management database and BARN, inspected access control lists to determine whether administration privileges are restricted to data centre technical administration personnel. | No deviations noted |
| | | NHS.19: Refer to CC2.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.17: Refer to CC2.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC9.0 | Risk Management | | | |
| CC9.1 | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | NHS.59: Operations personnel monitor the status of environmental protections, network connectivity, and device availability in the data centres on a continuous basis. | Inquired of management to determine whether Operations personnel monitor the status of environmental protections, network connectivity, and device availability in the data centres on a continuous basis.<br>Observed that operations personnel monitor the status of environmental protections, network connectivity, and device availability in the data centres on a continuous basis, in accordance with operations manuals and support guides.<br>Inspected the configurations of data centre monitoring tools to determine whether the status of environmental protections, network connectivity, and device availability in the data centres are monitored. | No deviations noted |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.26: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.51: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.61: Refer to CC7.5 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.04: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.21: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| CC9.2 | The entity assesses and manages risks associated with vendors and business partners. | NHS.64: Bell Canada has established procedures and processes to manage vendors and associated vendor risks, including vendor performance management, vendors requirements and commitments, and vendor communication. | Inquired of management to determine whether Bell Canada has established procedures and processes to manage vendors and associated vendor risks, including vendor performance management, vendors requirements and commitments, and vendor communication.<br>Inspected corporate policies to determine whether Bell Canada has established procedures and processes to manage vendor risks, performance, commitments, vendor communication to meet its security and availability commitments and requirements. | No deviations noted |
| | | NHS.04: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.21: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.22: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.23: Refer to CC3.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.11: Refer to CC1.4 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

## Availability Criteria

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| Additional Criteria for Availability | | | | |
| A1.1 | The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| A1.2 | The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | NHS.58: Environmental protections have been installed at NHS-managed data centres, including the following:<br>o Cooling systems<br>o Battery and generator back-up in the event of power failure<br>o Fire detectors<br>o Fire suppression. | Inquired of management to determine whether the following environmental protections have been installed at NHS-managed data centres:<br>o Cooling systems<br>o Battery and generator back-up in the event of power failure<br>o Fire detectors<br>o Fire suppression.<br><br>Observed at each of the NHS-managed data centres that the following environmental protections have been installed in a redundant configuration:<br>o Cooling systems<br>o Battery and generator back-up in the event of power failure<br>o Fire detectors<br>o Fire suppression. | No deviations noted |
| | | NHS.79: NHS management review the scope, control objectives, and control descriptions of any relevant service organization report, on an annual basis, to verify the report identifies all internal controls relevant to environmental protections. | Inquired of management to determine whether they review the scope, control objectives, and control descriptions of any relevant service organization report, on an annual basis, to verify the report identifies all internal controls relevant to environmental protections.<br><br>Inspected the Service Organization Control (SOC) report assessment prepared by management for the subservice organization which executes environmental protection controls at a data centre, and determined that the assessment includes a review of the scope, control objectives, control descriptions, testing procedures and testing results. | No deviations noted. |

| Ref. | Criteria Description | Controls Specified by Bell Canada | Ernst & Young LLP's Testing Procedures | Results of Tests |
|---|---|---|---|---|
| | | NHS.60: Environmental protections at NHS-managed data centres receive maintenance on at least an annual basis. | Inquired of management to determine whether environmental protections at NHS-managed data centres receive maintenance on at least an annual basis.<br>Inspected preventative maintenance reports from NHS-managed data centres to determine whether computer environmental protection systems are regularly inspected and tested to ascertain that these are kept in good working condition. | No deviations noted |
| | | NHS.57: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.59: Refer to CC9.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.26: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.61: Refer to CC7.5 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.50: Refer to CC2.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.19: Refer to CC2.3 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.16: Refer to CC2.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.80: Refer to CC7.2 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| A1.3 | The entity tests recovery plan procedures supporting system recovery to meet its objectives. | NHS.26: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |
| | | NHS.51: Refer to CC4.1 for the Control Specified by Bell Canada, Ernst & Young LLP's Testing Procedures, and Results of Tests. | | |