ROGERS
SOFTWARE DEVELOPMENT

GENERAL CONTROLS SUPPORTING THE FULL-SERVICE SALON MANAGEMENT SOFTWARE

SOC 2 - Type II Audit Report

Independent Service Auditor's Report on Controls Placed in Operation Relevant to the Trust Principles of Security, Availability, and Processing Integrity

For the Period March 1, 2015 to August 31, 2015

INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

The Moore Group, CPA
SOC Audit Specialists

Independent Service Auditor's Report

To: Rogers Software Development:

Scope
We have examined the description of Rogers Software Development's (ROGERS) full-service salon management software and systems for the period March 1, 2015 to August 31, 2015 and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability and processing integrity principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations *for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA*, Technical Practice Aids*) (applicable trust services criteria), throughout the period March 1, 2015 to August 31, 2015. The description indicates that certain applicable trust service criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Rogers' controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Service organization's responsibilities
In Section 2, ROGERS has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. ROGERS is responsible for (1) preparing the description and for the assertion; (2) the completeness, accuracy, and method of presentation of the description and the assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities
Our responsibility is to express an opinion on the

- fairness of the presentation of the description based on the description criteria set forth in Rogers' assertion and on the
- suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period March 1, 2015 to August 31, 2015.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations
Because of their nature and inherent limitations, 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 risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion
In our opinion, in all material respects, based on the description criteria identified in Rogers' assertion and the applicable trust services criteria,

a. the description fairly presents the system that was designed and implemented throughout the period March 1, 2015 to August 31, 2015.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period March 1, 2015 to August 31, 2015, and user entities applied the complementary user-entity controls contemplated in the design of Rogers' controls throughout the period March 1, 2015 to August 31, 2015.

c. the controls that were tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period March 1, 2015 to August 31, 2015.

Description of tests of controls
The specific controls we tested, the tests we performed, and the results of our tests are presented in Section 4, the ~~T~~esting Matrices”.

This report and the description of tests of controls and results thereof are intended solely for the information and use of ROGERS; user entities of ROGERS' described services during some or all of the period March 1, 2015 to August 31, 2015; 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 the service organization
- How the service organization’s system interacts with user entities, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- 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.

The Moore Group CPA, LLC

September 30, 2015
Nashua, NH

SECTION 2

ASSERTIONS BY THE SERVICE ORGANIZATION’S MANAGEMENT

ROGERS MANAGEMENT'S ASSERTION

We have prepared the attached description of Rogers' full-service salon management software and systems for the period March 1, 2015 to August 31, 2015 (the description), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.33–.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the full-service salon management software and system controls intended to meet the criteria for the security, availability and processing integrity principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the full-service salon management software and systems throughout the period March 1, 2015 to August 31, 2015, based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

(2) The components of the system used to provide the services, which are the following:

- *Infrastructure.* The physical and hardware components of a system (e.g., facilities, equipment, and networks).
- *Software*. The programs and operating software of a system (e.g., systems, applications, and utilities).
- *People*. The personnel involved in the operation and use of a system (e.g., developers, operators, users, and managers).
- *Procedures*. The automated and manual procedures involved in the operation of a system.
- *Data.* The information used and supported by a system (e.g., transaction streams, files, database, and tables).

(3) The boundaries or aspects of the system covered by the description

(4) How the system captures and addresses significant events and conditions

(5) The process used to prepare and deliver reports and other information to user entities and other parties.

(6) If information is provided to, or received from, subservice organizations or other parties, (a) how such information is provided or received and the role of the subservice organization or other parties and (b) the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the system and, when the inclusive method is used to present a subservice organization, controls at the subservice organization.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with our privacy commitments.

(9) Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons therefore.

(10) Other aspects of our control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria

(11) Relevant details of changes to the described services and systems during the period covered by the description

ii. The description does not omit or distort information relevant to the system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in the description were suitably designed throughout the period March 1, 2015 to August 31, 2015 to meet the applicable trust services criteria.

c. the controls stated in the description operated effectively throughout the period March 1, 2015 to August 31, 2015 to meet the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE SERVICE ORGANIZATION’S SYSTEM PROVIDED BY MANAGEMENT

DESCRIPTION OF CONTROLS PLACED IN OPERATION

OVERVIEW OF OPERATIONS

Company Background

Since 1999, Rogers Software Development (ROGERS) has devoted its energy to addressing the unique needs of business owners who provide personal services.

Founded by Matt Rogers, a former multi-location salon owner, ROGERS' mission has been to help retail and service companies grow their businesses through innovative and intuitive point of sale, online booking, customer engagement, and business management software.

Description of Services Provided

ROGERS' flagship software, SuperSalon, is an intuitive point of sale and salon management solution that is used by over 12,000 businesses worldwide. SuperSalon software offers everything needed to manage a growing salon, spa, wellness center, or health club. With Power Tool product add-ons and partner integrations, SuperSalon is a complete front and back office solution for independent, multi-location, and national chain salons.

SuperSalon features iOffice, a powerful back office tool that helps manage the entire business – from scheduling and payroll to inventory management and reporting. iOffice delivers a complete suite of useful features that can help grow the business and reduce expenses:

- Point of Sale – Quick and convenient check in and check out, customer look up, service and stylist menu, wait time, product look up, credit and debit card processing, and more.

- Card processing – SuperSalon provides secure credit and debit card processing and supports EMV and PCI requirements for point of sale transactions.

- Appointment Book – Book appointments, schedule staff hours, split commissions, and see the entire day, week, or month at a glance.

- Cloud Storage – Secure, reliable storage of data, customer information, shop information, and more. Backed up nightly and managed automatically.

- iOffice – Serious reporting tools, inventory, and time management, accounting, payroll, staff management, and more.

- Touch Screen Ready – SuperSalon operates beautifully on traditional PCs or a touch screen kiosk – giving unparalleled convenience and ease of use at the point of sale.

- Power Tools – Choose powerful add-ons to help expand the business, retain customers, and promote the salon’s services in effective and cost-efficient ways. Sample add-ons include:
    - Self Check-In Kiosk – Fast, convenient self-service check-in for regular customers and walk-ins
    - Video Menu Board – Show wait times, special offers, available salon services, and more
    - Mobile App – Smartphone appointment setting and check-ins for customers
    - SalonCheckIn.com – Online appointment setting and check-ins for customers
    - iOffice2go – Dashboard reporting and remote management from a smartphone or mobile device
    - Time Clock Kiosk – The all-in-one touch screen terminal for busy salons and schools
    - Centralized Database – Quickly and easily share customer information between multiple locations
    - SMS Notifications – Automatically send SMS notifications of confirmations and appointment reminders
    - Tablet Power Tool – Extend SuperSalon by creating additional terminals using a tablet
    - RateMyVisit.com – Fully integrated customer feedback and ranking system for salon locations
    - SmartReceipt – Graphically printed receipts to promote the business and brand
    - Gift Cards – Redeemable gift cards and gift certificates for salon services.

Facilities and Data Flow

ROGERS’ main corporate office is in Chandler, Arizona. For co-location of critical production servers and systems, ROGERS utilizes a secure third party data center, IO Data Center in Phoenix, Arizona. IO had a SOC 1-SSAE 16 Type II audit covering the period October 1, 2013 to September 30, 2014, which includes descriptions of various security controls that exist at the data center for the period.

The applications run on Linux Ubuntu and Debian OS platforms, with MySQL databases to support the applications. ROGERS uses a LAMP stack (Linux, Apache HTTP Server, MySQL database software, and PHP) for its web services. The systems are monitored by several enterprise monitoring applications, configured with preset thresholds and logging of critical events. Incidents are tracked with a Redmine ticketing system through to resolution, and ROGERS performs a root cause analysis (RCA). Redmine is accessed by ROGERS' employees via individually assigned user IDs and passwords, over securely encrypted SSL connections. The authorized users only have access to company specific data.

Linux operating system patches for critical production systems are updated via SALT, an open source configuration management and SSH authentication utility and terminal emulator. An RCA is performed to determine necessity, and patches are rolled to dev servers first for testing as needed.

For backups of critical company data, RSync open source backup scripts are used for file-based backups to a local physical backup server. For database backups, Percona MySQL backup functionality performs daily backups, which are retained for 30 days.

Encryption is utilized to protect data in transit, including SSL encryption over HTTPS connections utilized for secure communications between ROGERS and customer end users. Certain IT engineers access production network equipment and data stored at the third party data center remotely, via secure VPN tunnels protected by IPsec or SSL encryption.

PFSense firewalls are utilized, which reside on redundant physical servers configured in an active-active cluster. FW modifications must be approved by ROGERS' Change Advisory Board, which also performs an annual audit of firewall rule sets

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Rogers' control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of Rogers' ethical and behavioral standards, how they are communicated, and how they are reinforced in daily practice.

These standards include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, and by personal example.

Specific control activities that ROGERS has implemented in this area are described below.

- The **employee handbook** contains organizational policy statements, and codes of conduct and benefits and practices to which all employees are required to adhere.
- **Codes of conduct**, organizational policy statements, and disciplinary policies are documented and communicate entity values and behavioral standards to personnel.
- Policies and procedures require that new employees sign an **employee handbook acknowledgment form** indicating that they have been given access to it, and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook. The signed form is kept in the employee personnel file.
- Employees must sign a **confidentiality and non-disclosure agreement** to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Comprehensive **background checks** are performed by an independent third party for certain positions as a component of the hiring process.
- Management personnel perform **reference checks** on all candidates being considered for positions within ROGERS.
- Management maintains **insurance coverage** to protect against dishonest acts that may be committed by personnel.
- Periodic **meetings with staff** are conducted whereby the core values and mission of ROGERS are discussed as well as ways to reinforce and improve the components of Rogers' related core functions.

Commitment to Competence

Rogers' management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Rogers' commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

Specific control activities that ROGERS has implemented in this area are described below.

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into **written position requirements**.
- Management utilizes **skills assessment testing** for certain positions during the hiring process.
- Management has developed a **training and development program** for employees. This includes:
  - **Initial training** with peers and supervisors in the period immediately after hire.
  - **Ongoing training** to maintain and enhance the skill level of personnel on an as-needed basis.
- Each new employee undergoes an **initial 90 day review** to evaluate performance.
- ROGERS utilizes an **independent CPA firm** to audit/compile its financial statements and/or prepare tax returns.

Management's Philosophy and Operating Style

Rogers' management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward the full-service salon management software, information processing, accounting functions and personnel. Management is periodically briefed on regulatory and industry changes affecting services provided. Management meetings are held on a periodic basis to discuss and monitor operational issues.

Specific control activities that ROGERS has implemented in this area are described below.

- Management is guided by Rogers' corporate **mission statement** in determining the implementation of corporate goals and operational activities to meet them.
- Management regularly attends **conferences, trade shows, and webinars** to stay current on any regulatory compliance or operational trends affecting the services provided.
- **Management meetings** are held on a regular basis to discuss operational planning and budgeting, human resource planning and hiring, and customer related issues. Meeting agendas and meeting minutes are recorded and communicated to relevant personnel.
- ROGERS utilizes an **independent CPA firm** to audit/compile its financial statements and/or prepare tax returns.

Organization Structure and Assignment of Authority and Responsibility

Rogers' organization structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Rogers' management believes that establishing a relevant organization structure includes considering key areas of authority and responsibility and appropriate lines of reporting. ROGERS has developed an organization structure suited to its needs. This organization structure is based, in part, on its size and the nature of its activities.

Rogers' assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that all personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that ROGERS has implemented in this area are described below.

- **Organizational charts** are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and updated as needed.
- Rogers' **organization structure** is traditional, with clear lines of authority and responsibility. Autonomy within departments is allowed to a reasonable extent to provide for innovative approaches to managing the company, with close oversight maintained by the CEO.
- Rogers' **operating goals and objectives are communicated** to the entire organization during regular staff meetings, employee performance reviews, newsletters and other written communications.
- ROGERS provides an informal **employee orientation program** that communicates organization structure and responsibility, company and departmental objectives, and relationships between departments and personnel.

Human Resource Policies and Practices

Rogers' human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that ROGERS has implemented in this area are described below.

- Comprehensive **background checks** are performed by an independent third party for certain positions as a component of the hiring process.
- Management personnel perform **reference checks** on all candidates being considered for positions within INLINE.
- Management has developed a detailed **employee handbook** that communicates human resource policies and practices.
- Management has developed a **training and development program** for employees. This includes:
    - **Initial training** with peers and supervisors in the period immediately after hire.
    - **Ongoing training** to maintain and enhance the skill level of personnel on an as-needed basis.
- Each new employee undergoes an **initial 90 day probationary period and performance review** to evaluate performance. A formal evaluation form is prepared, and is maintained in employee's HR file.
- Human Resources management utilizes a **termination checklist** to ensure that specific elements of the termination process are consistently executed. The checklist is retained in the employee files.

RISK ASSESSMENT

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the management's description of the services and systems. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. However, because control objectives relate to risk that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting their system.

Objective Setting

ROGERS establishes objectives in order for management to identify potential events affecting their achievement. ROGERS has placed into operation a risk management process to help ensure that the chosen control objectives support and align with the organization's mission and are consistent with its risk framework. Objective setting enables management to identify measurement criteria for performance, with focus on success factors.

ROGERS has established certain broad categories including:

- **Strategic Objectives** — these pertain to the high level organizational goals and the alignment of those goals to support the overall mission
- **Operations Objectives** — these pertain to effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding of resources against loss
- **Reporting Objectives** — these pertain to the preparation of reliable reporting
- **Compliance Objectives** — these pertain to adherence to laws and regulations to which the entity is subject

Risks Identification

Regardless of whether an objective is stated or implied, an entity's risk-assessment process should consider risks that may occur. It is important that risk identification be comprehensive. ROGERS has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user organizations.

Management considers risks that can arise from both external and internal factors including:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities

The ROGERS risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. ROGERS senior management oversees risk management ownership, accountability, and is involved in risk identification process. Management identifies elements of business risk including threats, vulnerabilities, safeguards and the likelihood of a threat, to determine the actions to be taken.

Risks Analysis

Rogers' methodology for analyzing risks varies, largely because many risks are difficult to quantify. Nonetheless, the process includes:

- Estimating the significance of a risk
- Assessing the likelihood (or frequency) of the risk occurring
- Considering how the risk should be managed, including an assessment of what actions need to be taken

Risk analysis is an essential process to the entity’s success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities

Control activities are a part of the process by which ROGERS strives to achieve its business objectives. ROGERS has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization.

The applicable trust criteria and related control activities are included in Section 4 (the –Testing Matrices”) of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in the Testing Matrices. Although the applicable trust criteria and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of Rogers' description of controls and systems.

The description of the service auditor’s tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization’s description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

Rogers' management performs monitoring activities in order to continuously assess the quality of internal control over time. Monitoring activities are used to initiate corrective action through department meetings, client conference calls, and informal notifications. Management performs monitoring activities on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Ongoing and Separate Evaluations of the Control Environment

Monitoring can be done in two ways: through ongoing activities or separate evaluations. The greater the degree and effectiveness of ongoing monitoring, the less the need is for separate evaluations. Management determines the need for separate evaluations by consideration given to the following: the nature and degree of changes occurring and their associated risks, the competence and experience of the people implementing the controls, as well as the results of the ongoing monitoring. Management has implemented a combination of ongoing monitoring and separate evaluations, as deemed necessary; to help ensure that the internal control system maintains its effectiveness over time.

Ongoing Monitoring

Examples of Rogers' ongoing monitoring activities include the following:

- In carrying out its regular management activities, operating management obtains evidence that the system of internal control continues to function.
- Communications from external parties and customers corroborate internally generated information or indicate problems.
- Organization structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Training, planning sessions, and other meetings provide important feedback to management on whether controls are effective.
- Personnel are briefed on organizational policy statements and codes of conduct to communicate entity values.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to ensure follow-up actions are taken and subsequent evaluations are modified as necessary.

Reporting Deficiencies

Deficiencies in management’s internal control system surface from many sources, including Rogers' ongoing monitoring procedures, separate evaluations of the internal control system and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision for addressing deficiencies based on whether the incident was isolated or requires a change in Rogers' procedures or personnel.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

A combination of custom developed and commercial applications are utilized to support the full-service salon management software and services provided to user organizations. The applications run on Linux Ubuntu and Debian operating system platforms, with MySQL databases to support the applications.

Redundancy is maintained for components of the data infrastructure, including firewalls, routers, servers and switches. Systems are developed and deployed to enable the addition of bandwidth and server capacity quickly to support customer requirements. External services and internal applications constantly monitor communications, job logs, system performance, and security and send alerts to the operations staff before customers are affected.

Communication Systems

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within ROGERS. Management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organizational charts, employee handbooks, training classes and job descriptions are in place at ROGERS. Management's communication activities are made electronically, verbally, and through the actions of management.

COMPLEMENTARY CONTROLS AT USER ORGANIZATIONS

Rogers' services are designed with the assumption that certain controls will be implemented by user organizations. Such controls are called complementary user organization controls. It is not feasible for all of the control objectives related to Rogers' full-service salon management software to be solely achieved by Rogers' control procedures. Accordingly, user organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of ROGERS.

The following complementary user organization controls should be implemented by user organizations to provide additional assurance that the control objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user organizations' locations, user organizations' auditors should exercise judgment in selecting and reviewing these complementary user organization controls, which may include:

- User organizations are responsible for understanding and complying with their contractual obligations to ROGERS.
- User organizations are responsible for developing their own disaster recovery and business continuity plans that address their ability to access or utilize ROGERS services.
- User organizations are responsible for ensuring that user IDs and passwords used to access ROGERS applications are kept in a secure manner and only used by authorized employees.
- User organizations are responsible for requesting an authorized user ID and password for user organization employees. User organizations are responsible for defining the level of access given to employees and customers.
- User organizations are responsible for requesting the revocation of application access privileges assigned to terminated employees as a component of the employee termination process.
- User organizations are responsible for restricting administrative privileges within the application or systems to authorized personnel and for designating internal personnel who are authorized to request user additions, deletions, and security level changes.
- User organizations are responsible for notifying ROGERS of changes made to technical or administrative contact information in a timely manner.
- User organizations are responsible for understanding and defining data storage requirements.
- User organizations are responsible for understanding and implementing encryption protocols to protect data during transfer to ROGERS.
- User organizations are responsible for immediately notifying ROGERS of any actual or suspected information security breaches, including compromised user accounts and passwords.
- User organizations are responsible for notifying ROGERS of any regulatory issues that may affect the services provided by ROGERS.

SECTION 4

TESTING MATRICES

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1	The entity has defined organization structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements related to security and availability.	Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements that delineate employee responsibilities and authority.	Inspected a judgmental sample of written job descriptions to determine that management had considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.	No exceptions noted.
		Management has authorized specific personnel to administer information security within the production and internal network environments.	Inspected access rights of personnel authorized by management to administer information security.	No exceptions noted.
		Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and are updated as needed.	Inquired of management regarding communication of organizational charts to determine that the charts are communicated to employees and updated as needed.	No exceptions noted.
			Inspected organizational charts to determine that organizational charts are in place to communicate key areas of authority and responsibility and are updated as needed.	No exceptions noted.
		Rogers' organization structure is traditional, with clear lines of authority and responsibility. Autonomy within departments is allowed to a reasonable extent to provide for innovative approaches to managing the company, with close oversight maintained by the CEO.	Inquired of management to determine that Rogers' organization structure is traditional, with clear lines of authority and responsibility, and that autonomy within departments is allowed to a reasonable extent to provide for	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			innovative approaches to managing the company, with close oversight maintained by the CEO.	
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and placed in operation.	A policy is in place to assign responsibility and accountability for developing and maintaining the entity's system availability and related security policies, and changes and updates to those policies, to appropriate personnel.	Inspected the policies and procedures to determine that responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, were assigned to appropriate personnel.	No exceptions noted.
		Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements that delineate employee responsibilities and authority.	Inspected a judgmental sample of written job descriptions to determine that management had considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.	No exceptions noted.
CC1.3	Personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting security and availability have the qualifications and resources to fulfill their responsibilities.	Policies and procedures are in place to guide personnel regarding providing for training and other resources to support its system security policies.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding training and other resources to support its system security policies.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Policies and procedures are in place to ensure that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	Inspected policies and procedures and human resource hiring guidelines to determine that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	No exceptions noted.
		Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements that delineate employee responsibilities and authority.	Inspected a judgmental sample of written job descriptions to determine that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	No exceptions noted.
		Management has authorized specific personnel to administer information security within the production and internal network environments.	Inspected the access rights listing to determine that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	No exceptions noted.
		Management utilizes skills assessment testing for certain positions during the hiring process.	Inquired of management to determine that management utilizes skills assessment testing for certain positions during the hiring process.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management has developed a training and development program for employees. This includes: • Initial training with peers and supervisors in the period immediately after hire. • Ongoing training to maintain and enhance the skill level of personnel on an as-needed basis.	Inquired of management into initial and ongoing training and development for employees, to determine that a program is in place.	No exceptions noted.
			Inspected a judgmental sample of company documentation (meeting agendas, assignments) of initial training and development for new employees.	No exceptions noted.
			Inspected a judgmental sample of documented training programs (meeting agendas, assignments) for tenured employees to determine that ongoing training is utilized for each employee on an as-needed basis beyond the initial hiring training period.	No exceptions noted.
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security and availability.	ROGERS maintains an employee handbook, which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.	Inspected the employee handbook to determine that it contains organizational policy statements, benefits and practices to which all employees are required to adhere.	No exceptions noted.

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have been given access to it, and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook. The signed form is kept in the employee personnel file.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee handbook and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook.	No exceptions noted.
		Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
		Management utilizes skills assessment testing for certain positions during the hiring process.	Inquired of management to determine that management utilizes skills assessment testing for certain positions during the hiring process.	No exceptions noted.
		Comprehensive background checks are performed by an independent third party for certain positions as a component of the hiring process.	Inspected completed background checks for a judgmental sample of employees subject to background checks hired during the review period to determine that	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC1.0 - COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT

The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			background checks are performed by an independent third party.	
		Management personnel perform reference checks on all candidates being considered for positions within ROGERS.	Inquired of management to determine that management personnel perform reference checks on all candidates being considered for positions within ROGERS.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	Security policies are in place to guide personnel regarding physical and information security practices.	Inspected the policies and procedures manual to determine that security policies were in place to guide personnel regarding physical and information security practices.	No exceptions noted.
		New client contracts are approved by ROGERS management prior to initiating service. A Service Level Agreement (SLA) is signed by the client and ROGERS management.	Inspected a judgmental sample of new client contracts and SLAs formalized during the review period to determine that they are signed off by the client and ROGERS management.	No exceptions noted.
		Network diagrams are in place and communicated to appropriate personnel.	Inspected network diagrams to determine that network diagrams are in place and communicated to appropriate personnel.	No exceptions noted.
		An objective description of the full-service salon management software and systems and its boundaries is communicated within printed materials provided to authorized users and on the ROGERS website.	Inspected printed materials and the ROGERS website description of the full-service salon management software and systems to determine that the description of the system and its boundaries is communicated to authorized users.	No exceptions noted.
CC2.2	The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal	Policies and procedures are in place for identifying and documenting the system availability and related security requirements of authorized users.	Inspected the policies and procedures to determine that the entity’s system availability and related security policies were established.	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	system users to enable them to carry out their responsibilities.			
		Security policies are in place to guide personnel regarding physical and information security practices.	Inspected the policies and procedures manual to determine that security policies were in place to guide personnel regarding physical and information security practices.	No exceptions noted.
		New client contracts are approved by ROGERS management prior to initiating service. A Service Level Agreement (SLA) is signed by the client and ROGERS management.	Inspected a judgmental sample of new client contracts and SLAs formalized during the review period to determine that they are signed off by the client and ROGERS management.	No exceptions noted.
		ROGERS maintains an employee handbook, which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.	Inspected the employee handbook to determine that it contains organizational policy statements, benefits and practices to which all employees are required to adhere.	No exceptions noted.
		Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have been given access to it, and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook. The signed form is kept in the employee personnel file.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee handbook and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
		The security obligations of users and Rogers' commitments to users are communicated verbally and in writing. Any issues with the system are communicated either verbally or through the ticketing system or email between ROGERS, the client and any other affected party.	Inquired of management to determine that the availability and related security obligations of users and the entity's availability and related security commitments to users were communicated to authorized users.	No exceptions noted.
		An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner, and properly document them.	Inspected the incident response plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.	No exceptions noted.
CC2.3	The entity communicates the responsibilities of internal and external users and others whose roles affect system operation.	Policies and procedures are in place to assign responsibility and accountability for system availability and security.	Inspected the security policies and procedures to determine that monitoring policies and procedures were in place to assign responsibility and accountability for system availability and security.	No exceptions noted.
		Documented backup procedures are in place for company systems deemed critical by management, to guide personnel in performing backup system tasks.	Inspected documented backup procedures to determine that documented backup procedures are in place for critical ROGERS systems.	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		ROGERS maintains an employee handbook, which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.	Inspected the employee handbook to determine that it contains organizational policy statements, benefits and practices to which all employees are required to adhere.	No exceptions noted.
		Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have been given access to it, and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook. The signed form is kept in the employee personnel file.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee handbook and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook.	No exceptions noted.
		Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC2.4	Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls relevant to the	Policies and procedures are in place to guide personnel regarding providing for training and other resources to support its system security policies.	Inspected the security policies and procedures to determine that the entity's policies included training and other resources to support its system security policies.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	security and availability of the system have the information necessary to carry out those responsibilities.			
		Policies and procedures are in place to guide personnel regarding the handling of exceptions and situations not specifically addressed in its system security policies.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding the handling of exceptions and situations not specifically addressed in its system security policies.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	Inspected the policies and procedures and the service level agreements to determine that the entity's policies included procedures regarding the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	No exceptions noted.
		Policies and procedures are in place to assign responsibility and accountability for system availability and security.	Inspected the security policies and procedures to determine that monitoring policies and procedures were in place to assign responsibility and accountability for system availability and security.	No exceptions noted.
		Third party enterprise monitoring applications are used to monitor and record performance criteria for critical ROGERS server and network equipment.	Inspected the Op Manager enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			critical ROGERS server and network equipment.	
		The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via email to IT support personnel.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
		System downtime and operations issues are monitored to help ensure that system downtime does not exceed predefined levels.	Inspected the metrics tracking reports to determine that system downtime and operations issues were monitored.	No exceptions noted.
		An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner, and properly document them.	Inspected the incident response plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.	No exceptions noted.
		Management has documented information security policies and procedures to communicate corporate security standards to employees.	Inspected the information security policies to determine that management documented information security policies to communicate corporate security standards to employees.	No exceptions noted.
		Policies and procedures are in place to govern critical computer operations activities.	Inspected the policies and procedures to determine that policies and procedures are in place to govern critical computer operations activities.	No exceptions noted.
		Documented backup procedures are in place for company systems deemed critical by management, to guide personnel in performing	Inspected documented backup procedures to determine that documented backup procedures are	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		backup system tasks.	in place for critical ROGERS systems.	
CC2.5	Internal and external system users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding resolution of complaints and requests relating to system security and related issues.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding the handling of exceptions and situations not specifically addressed in its system security policies.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding the handling of exceptions and situations not specifically addressed in its system security policies.	No exceptions noted.
		The customer agreement documents the process for informing the entity about breaches of the system security and for submitting complaints.	Inspected an example customer agreement to determine that the process for informing the entity about system security issues and breaches of system security and for submitting complaints was communicated to authorized users.	No exceptions noted.
CC2.6	System changes that affect internal and external system user responsibilities or the entity's commitments and requirements relevant to security and availability are communicated to those users in a timely manner.	Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding assigning responsibility and accountability for system changes and maintenance.	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATIONS

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Customers are notified verbally or via e-mail notification regarding changes that may affect system security and availability.	Inquired of management to determine that changes that may affect system security and availability were communicated to management and users who were affected.	No exceptions noted.
		Leadership Team approval is obtained before changes are migrated to the production environment.	Inspected a judgmental sample of code releases from the review period for management signoff to determine that Leadership Team approval was obtained before changes were migrated to the production environment.	No exceptions noted.
		Changes to the application are rolled to production either during or after hours on a case-by-case basis depending on customer preference. Emergency changes take place immediately.	Inspected rollout logs to determine that changes are rolled to production either during or after hours on a case-by-case basis depending on customer preference, while emergency changes take place immediately.	No exceptions noted.
		Documented change requests are completed for bug fixes, enhancements and new development. Requests are reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	Inspected a judgmental sample of product changes from the review period for entries in the tracking system to determine that requests were reviewed and prioritized by management based on business needs and resource availability.	No exceptions noted.

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1	The entity (1) identifies potential threats that would impair system security and availability commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).	Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.	Inquired of management regarding risk assessment to determine that procedures were in place to assess risks on a periodic basis.	No exceptions noted.
			Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.	No exceptions noted.
		Redundant architecture is built into network infrastructure, including, but not limited to the: • Network interface cards (NICs) • High availability networks • Firewalls and switches • Web servers • DB cluster • PBX.	Observed the redundant network infrastructure components to determine that redundant architecture was built into certain aspects of the network infrastructure.	No exceptions noted.
CC3.2	The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.	Policies and processes are in place to protect against unauthorized access to system resources. Firewall systems are in place to handle data flow between external parties and the ROGERS network. Firewall ports are configured to allow only specific types of traffic between certain destinations.	Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and ROGERS network.	No exceptions noted.

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the firewall system configuration to determine that firewalls are configured to allow only specific types of traffic between certain destinations.	No exceptions noted.
		Management maintains insurance coverage to protect against dishonest acts that may be committed by personnel.	Inspected insurance coverage policy declarations page to determine that management maintained insurance coverage to protect against dishonest acts by personnel.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.	No exceptions noted.
			Inspected a judgmental sample of server configurations to determine that all servers have this functionality turned on.	No exceptions noted.
		Multiple firewalls are utilized for redundancy. The firewalls are set up in an active/passive configuration with automatic failover in the event of failure of the primary.	Inspected the firewall rule sets and failover configurations to determine that they are set up in a failover configuration.	No exceptions noted.
			Observed the network firewalls to determine that multiple firewalls are utilized for redundancy.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Firewall configurations filter internet traffic based on content and destination site address. The configurations include: • Network Address Translation (NAT) services are enabled on all network firewalls to hide internal servers. • Firewall ports are configured to allow only specific types of traffic between certain destinations. All unused ports on the firewall are blocked. • The firewall is configured to deny all traffic that is not specifically authorized in the rule set.	Inspected firewall configurations to determine that firewall configurations filter internet traffic based on content and destination site address.	No exceptions noted.
			Inspected the firewall configuration to determine that the NAT services are enabled on all network firewalls.	No exceptions noted.
			Inspected the firewall system configuration to determine that firewalls are configured to allow only specific types of traffic between certain destinations, and that unused ports are disabled.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall was configured to deny traffic that was not specifically authorized in the rule set.	No exceptions noted.
		Firewall access control lists (ACLs) are set up to limit access. These include: • IP address filtering (IP white listing) is used in limited circumstances in the	Inspected the firewall access lists to determine that firewall access lists (IP white lists) are utilized in limited circumstances for filtering traffic into	No exceptions noted.

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		firewall to restrict network access from outside of the network to only known personal computers.	the network.	
		Management utilizes vulnerability assessment tools (VAT) to help determine vulnerability risks and evaluates and takes action on issues identified in the report.	Inspected vulnerability assessment tools, configurations and test reports generated to determine that management utilizes vulnerability assessment tools to help determine vulnerability risks.	No exceptions noted.
			Inspected a judgmental sample of closed tickets remediating issues in the most recent report to determine that management evaluates and takes action on issues identified in the report.	No exceptions noted.
		Policies and procedures are in place to govern critical computer operations activities.	Inspected the policies and procedures to determine that policies and procedures are in place to govern critical computer operations activities.	No exceptions noted.
CC3.3	The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for security and availability and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and	Policies and procedures are in place to guide personnel regarding the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	Inspected the policies and procedures and the service level agreements to determine that the entity's policies included procedures regarding the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	No exceptions noted.

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	monitoring of those activities, and updates them as necessary.			
		Security policies and procedures are in place and periodically reviewed by a designated individual or group.	Inquired of management regarding availability and related security policies to determine that the entity's system security policies were established and periodically reviewed and approved by the director.	No exceptions noted.
			Inspected the policies and procedures manual to determine that the entity's system security policies were established.	No exceptions noted.
		Management regularly attends conferences, trade shows, and webinars to stay current on any regulatory compliance or operational trends affecting the services provided.	Inspected a judgmental sample of conference, trade show and webinar agendas to determine that management is periodically briefed on regulatory and industry changes affecting services provided.	No exceptions noted.
		Third party enterprise monitoring applications are used to monitor and record performance criteria for critical ROGERS server and network equipment.	Inspected the Op Manager enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical ROGERS server and network equipment.	No exceptions noted.
		The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via email to IT support personnel.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.

CC3.0 - COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		IT personnel subscribe to informational services and are notified of recent attacks and vulnerabilities.	Inspected a sample of informational services communications to determine that personnel subscribe to informational services and are notified of attacks and vulnerabilities.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC4.0 - COMMON CRITERIA RELATED TO MONITORING OF CONTROLS

The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1	The design and operating effectiveness of controls are periodically evaluated against security and availability commitments, and requirements, corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Security policies and procedures are in place and periodically reviewed by a designated individual or group.	Inquired of management regarding availability and related security policies to determine that the entity's system security policies were established and periodically reviewed and approved by the director.	No exceptions noted.
			Inspected the policies and procedures manual to determine that the entity's system security policies were established.	No exceptions noted.
		Third party enterprise monitoring applications are used to monitor and record performance criteria for critical ROGERS server and network equipment.	Inspected the Op Manager enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical ROGERS server and network equipment.	No exceptions noted.
		The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via email to IT support personnel.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
		IT personnel subscribe to informational services and are notified of recent attacks and vulnerabilities.	Inspected a sample of informational services communications to determine that IT personnel subscribe to informational services and are notified of recent attacks and vulnerabilities.	No exceptions noted.

CC4.0 - COMMON CRITERIA RELATED TO MONITORING OF CONTROLS

The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Certain network events are logged and maintained for management review. Critical servers have auditing enabled, and for security, system management and network functions.	Inspected the network account and local event monitoring configurations, and event logs to determine that certain network events were logged and maintained for management review.	No exceptions noted.
			Inspected a judgmental sample of server configurations to determine that critical servers have auditing enabled, and for security, system management and network functions.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inquired of management to determine that management periodically performs internal security assessments.	No exceptions noted.
			Inspected a judgmental sample of server configurations to determine that all servers have this functionality turned on.	No exceptions noted.
		Management has developed Rogers' definition of system downtime and determined severity level criteria	Inspected policies and procedures to determine management has developed Rogers' definition of system downtime and severity level criteria.	No exceptions noted.
		System downtime and operations issues are monitored to help ensure that system downtime does not exceed predefined levels.	Inspected the metrics tracking reports to determine that system downtime and operations issues were monitored.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC4.0 - COMMON CRITERIA RELATED TO MONITORING OF CONTROLS

The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		ROGERS utilizes internal vulnerability assessment tools (VAT) to periodically review system security and potential impairments to defined system security policies.	Inspected the VAT utilized to determine that these tools are used to periodically review system security and potential impairments to defined system security policies.	No exceptions noted.
		A ticketing system is utilized to manage systems infrastructure issues such as system security breaches and other incidents. Tickets are assigned to support personnel based on the nature of the ticket.	Inspected a judgmental sample of logs from the ticketing system showing closed tickets to determine a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on nature.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	A secure VPN (Virtual Private Network) connection is used for remote external access to the internal network by authorized ROGERS employees. The use of VPN connection is restricted to authorized employees through user names and passwords, and is controlled via Active Directory.	Inquired of management to determine that a secure VPN is used for remote connection to the network by authorized ROGERS employees.	No exceptions noted.
		Management has segregated specific duties within the production environment for administering critical areas such as network administration and database management. Management restricts network domain administration privileges to approved positions only.	Inspected the administrative access rights listing to confirm that management has authorized specific personnel to administer information security within the production environment, and has segregated specific duties for administering critical areas such as network administration, and database management.	No exceptions noted.
		Users are assigned to pre-defined roles and access rights within all ROGERS systems: • Access to sensitive production server directories and files is restricted based on job responsibilities. • Users are granted variable access rights according to a rights authorization methodology. • Access to systems is granted on a ―least privilege” basis, with employees acquiring access only to	Inquired of management to determine that users are assigned to pre-defined roles and access rights within all ROGERS production systems, and that variable rights are assigned based on job responsibilities and least privilege.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		those systems necessary to perform their job functions.		
			Inspected the access rights listing to determine that users are assigned to variable, pre-defined roles and access rights within all ROGERS production systems.	No exceptions noted.
		Processes and procedures are in place to restrict access to backup data and systems. Management restricts the ability to access backup electronic data from the backup servers to authorized personnel only.	Inspected policies and procedures related to restricting access to offline storage, backup data, systems, and media.	No exceptions noted.
			Inspected the backup access/ recall listing to determine that management restricts the ability to recall backup electronic data from the third party provider to authorized personnel.	No exceptions noted.
		Policies and processes are in place to protect against unauthorized access to system resources. Firewall systems are in place to handle data flow between external parties and the ROGERS network. Firewall ports are configured to allow only specific types of traffic between certain destinations.	Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and ROGERS network.	No exceptions noted.
			Inspected the firewall system configuration to determine that firewalls are configured to allow only specific types of traffic between certain destinations.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Server-based firewalls and routers are placed at all network perimeter and third-party entry points to ROGERS networks.	Inspected the network diagram, router security policy, and firewall system rule sets to determine that server-based firewalls and routers are placed at all network perimeter and third party entry points to ROGERS networks.	No exceptions noted.
CC5.2	New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.	Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.	Inspected the policies and procedures to determine that new user access, modification, and removal policies are in place.	No exceptions noted.
		Management revokes network and production server connection privileges assigned to terminated employees as a component of the employee termination process.	Inspected the default domain user listing and a judgmental sample of production server user listings to determine that management revoked network access privileges assigned to terminated employees as a component of the employee termination process.	No exceptions noted.
		The request to create or modify user access to the hosted user application must be provided by an authorized customer end user.	Inquired of management to determine that a request to create or modify user access to the hosted user application must be provided by an authorized customer end user.	No exceptions noted.
CC5.3	Internal and external system users are identified and authenticated when accessing the system	A secure VPN (Virtual Private Network) connection is used for remote external access to the internal network by authorized ROGERS	Inquired of management to determine that a secure VPN is used for remote connection to the	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	components (for example, infrastructure, software, and data).	employees. The use of VPN connection is restricted to authorized employees through user names and passwords, and is controlled via Active Directory.	network by authorized ROGERS employees.	
		All production Linux system level users are required to authenticate at the shell level via a unique network ID and password. Further root level administrative access can only be gained by root level authentication for root authorized users. • No shared accounts are currently in use. • Passwords are masked upon entry (not displayed in clear text).	Observed the critical Linux server authentication process to determine that users are required to authenticate via a network ID and password before being granted shell access to critical ROGERS Linux servers, and that passwords are masked upon entry.	No exceptions noted.
			Observed the root level authentication process to determine that further administrative access can only be gained by root level authentication for root authorized users.	No exceptions noted.
			Inspected the listing of root authorized users for a judgmental sample of servers to determine that only authorized users can gain root level access.	No exceptions noted.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.	Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.	Inspected the policies and procedures to determine that new user access, modification, and removal policies are in place.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management has segregated specific duties within the production environment for administering critical areas such as network administration and database management. Management restricts network domain administration privileges to approved positions only.	Inspected the administrative access rights listing to confirm that management has authorized specific personnel to administer information security within the production environment, and has segregated specific duties for administering critical areas such as network administration, and database management.	No exceptions noted.
		Users are assigned to pre-defined roles and access rights within all ROGERS systems: • Access to sensitive production server directories and files is restricted based on job responsibilities. • Users are granted variable access rights according to a rights authorization methodology.	Inquired of management to determine that users are assigned to pre-defined roles and access rights within all ROGERS production systems, and that variable rights are assigned based on job responsibilities and least privilege.	No exceptions noted.
			Inspected the access rights listing to determine that users are assigned to variable, pre-defined roles and access rights within all ROGERS production systems.	No exceptions noted.
		Management revokes network and production server connection privileges assigned to terminated employees as a component of the employee termination process.	Inspected the default domain user listing and a judgmental sample of production server user listings to determine that management revoked network access privileges assigned to terminated employees as a component of the employee termination process.	No exceptions noted.
CC5.5	Physical access to facilities housing the system (for example,	Physical security policies and procedures are in place to guide personnel regarding	Inspected the policies and procedures manual to determine	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.	restricting access to the facility.	that physical security policies and procedures were in place to guide personnel regarding restricting access to the facility.	
		ROGERS utilizes a third party data center for hosting critical production servers and networking equipment. The third party data center has physical access controls in place to restrict access to authorized personnel only.	Inspected the third party data center SOC 1-SSAE 16 audit report for the review period October 1, 2013 to September 30, 2014 to determine that physical access controls are present at the facility utilized by ROGERS.	No exceptions noted.
		The employee termination process includes the removal of the terminated personnel's ability to gain access to the facility, including deactivation and retrieval of all electronic access means. This process is documented in the termination checklist.	Inquired of management to determine that electronic access is deactivated and physical keys are retrieved where possible.	No exceptions noted.
			Inspected a judgmental sample of termination checklists for any employees terminated during the review period to determine that this process is documented in the checklist.	No exceptions noted.
CC5.6	Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system.	Firewall systems are in place to handle data flow between external parties and the ROGERS network. All external traffic intended for the ROGERS production environment must pass through a firewall system to communicate with the ROGERS servers.	Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and ROGERS network.	No exceptions noted.
		Server-based firewalls are in place, utilizing	Inspected the Windows Server	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		third party firewall applications. The firewall applications are set up locally on each server.	firewall configurations for a judgmental sample of servers to determine that server-based firewall applications are in use, and that they are set up locally on each server.	
		Multiple firewalls are utilized for redundancy. The firewalls are set up in an active/passive configuration with automatic failover in the event of failure of the primary.	Inspected the firewall rule sets and failover configurations to determine that they are set up in a failover configuration.	No exceptions noted.
			Observed the network firewalls to determine that multiple firewalls are utilized for redundancy.	No exceptions noted.
		The ability to modify the firewall system software, configurations or rule sets is restricted based on job responsibility, and is limited to approved positions only.	Inspected firewall system access documentation to determine that the ability to modify the firewall system software, configuration or rule sets is restricted based on job responsibility and is limited to approved positions only.	No exceptions noted.
		All firewall system modifications are required to be submitted and approved by the company Change Advisory Board (CAB). In addition, an annual audit of the firewall rulesets is performed to ensure that all modifications have been authorized, and that rule sets remain current and locked down.	Inspected a judgmental sample of tickets for firewall and other network security changes to determine that changes are submitted and approved by the CAB.	No exceptions noted.
			Inquired of management to determine that all changes are submitted and approved by the CAB, and that an annual audit of rulesets is conducted.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Firewall configurations filter internet traffic based on content and destination site address. The configurations include: • Network Address Translation (NAT) services are enabled on all network firewalls to hide internal servers. • Firewall ports are configured to allow only specific types of traffic between certain destinations. All unused ports on the firewall are blocked. • The firewall is configured to deny all traffic that is not specifically authorized in the rule set.	Inspected firewall configurations to determine that firewall configurations filter internet traffic based on content and destination site address.	No exceptions noted.
			Inspected the firewall configuration to determine that the NAT services are enabled on all network firewalls.	No exceptions noted.
			Inspected the firewall system configuration to determine that firewalls are configured to allow only specific types of traffic between certain destinations, and that unused ports are disabled.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall was configured to deny traffic that was not specifically authorized in the rule set.	No exceptions noted.
		Network administrators harden servers by disabling unnecessary operating system services.	Inquired of Management to determine that network administrators disable unnecessary operating system services.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A secure VPN (Virtual Private Network) connection is used for remote external access to the internal network by authorized ROGERS employees. The use of VPN connection is restricted to authorized employees through user names and passwords, and is controlled via Active Directory.	Inquired of management to determine that a secure VPN is used for remote connection to the network by authorized ROGERS employees.	No exceptions noted.
CC5.7	The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security and availability.	Policies and procedures are in place to guide personnel regarding sharing information with third parties.	Inspected the security policies and procedures and the service level agreements to determine that the entity's policies included procedures to guide personnel regarding sharing information with third parties.	No exceptions noted.
		Documented policies and procedures are in place, which govern critical data communication activities.	Inspected policies and procedures which govern critical data communication activities to determine that documented policies and procedures are in place, which govern critical data communication activities.	No exceptions noted.
		Communication sessions between Rogers' servers/applications and external parties are secured using various encryption methods when applicable.	Inspected the encryption documentation to determine that communication sessions between ROGERS servers and applications and certain external parties are secured using various encryption methods when applicable.	No exceptions noted.
		External and internal servers and network devices that need access to internal resources	Inspected a judgmental sample of server configurations to determine	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		are configured with industry standard SSL-encrypted tunnels to protect their connection.	that external servers that need access to internal resources are configured with SSH-encrypted tunnels to protect their connection.	
		Transaction processing performed on web-based applications is secured through the use of the Secure Socket Layer (SSL) encryption protocol over HTTPS connections.	Inspected the web application SSL certificates to determine that transaction processing performed on web-based applications is secured through the use of the Secure Socket Layer (SSL) protocol over HTTPS connections.	No exceptions noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.	Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the security policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.	No exceptions noted.
		Policies and processes are in place to protect against infection by computer viruses, malicious code, and unauthorized software.	Inspected policies and processes to determine that management has policies and processes in place to protect against infection by computer viruses, malicious code, and unauthorized software.	No exceptions noted.
		IT personnel subscribe to informational services and are notified of recent attacks and vulnerabilities.	Inspected a sample of informational services communications to determine that IT personnel subscribe to informational services and are notified of recent attacks and vulnerabilities.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC6.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1	Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated, and countermeasures are implemented to compensate for known and new vulnerabilities.	Third party enterprise monitoring applications are used to monitor and record performance criteria for critical ROGERS server and network equipment.	Inspected the Op Manager enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical ROGERS server and network equipment.	No exceptions noted.
		The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via email to IT support personnel.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inquired of management to determine that management periodically performs internal security assessments.	No exceptions noted.
			Inspected a judgmental sample of server configurations to determine that all servers have this functionality turned on.	No exceptions noted.
		IT personnel subscribe to informational services and are notified of recent attacks and vulnerabilities.	Inspected a sample of informational services communications to determine that IT personnel subscribe to informational services and are notified of recent attacks and vulnerabilities.	No exceptions noted.
		Third party automated backup applications are utilized to perform scheduled system backups.	Inspected the third party automated backup system to determine that automated backup systems are	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			utilized to perform scheduled system backups.	
		ROGERS utilizes internal vulnerability assessment tools (VAT) to periodically review system security and potential impairments to defined system security policies.	Inspected the VAT utilized to determine that these tools are used to periodically review system security and potential impairments to defined system security policies.	No exceptions noted.
		A ticketing system is utilized to manage systems infrastructure issues such as system security breaches and other incidents. Tickets are assigned to support personnel based on the nature of the ticket.	Inspected a judgmental sample of logs from the ticketing system showing closed tickets to determine a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on nature.	No exceptions noted.
		A Data Breach Response Plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner, and properly document them.	Inspected the Data Breach Response Plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.	No exceptions noted.
CC6.2	Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.	Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the security policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding resolution of	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC6.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			complaints and requests relating to system security and related issues.	
		A Data Breach Response Plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner, and properly document them.	Inspected the Data Breach Response Plan to determine that a plan is in place to ensure appropriate response to outages or security incidents.	No exceptions noted.
		A written change management form is completed and properly approved before core changes are made to production application code.	Inspected a sample change management form to determine that a change management form is completed and properly approved before core changes are made to production application code.	No exceptions noted.
		A ticketing system is utilized to manage systems infrastructure issues such as system security breaches and other incidents. Tickets are assigned to support personnel based on the nature of the ticket.	Inspected a judgmental sample of logs from the ticketing system showing closed tickets to determine a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on nature.	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1	Security and availability commitments and requirements, are addressed, during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.	Policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	Observed and inspected relevant policies and procedures to determine that policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	No exceptions noted.
			Inspected authentication policies and configurations for the production servers and administrative rights.	No exceptions noted.
		Leadership Team approval is obtained before changes are migrated to the production environment.	Inspected a judgmental sample of code releases from the review period for management signoff to determine that Leadership Team approval was obtained before changes were migrated to the production environment.	No exceptions noted.
CC7.2	Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to security and availability.	Policies and procedures are in place for classifying data based on its criticality and sensitivity and that classification is one of many factors used to define protection requirements, access rights and restrictions, and retention and destruction requirements.	Inspected the policies and procedures to determine that data classification, protection requirements, access rights, access restrictions, and retention and destruction policies were established.	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding assigning responsibility and accountability for system changes and maintenance.	No exceptions noted.
		Management has a data classification policy and methodology to identify and classify sensitive data in the production environment.	Inspected data classification methodology and policy to determine that management has a data classification policy and methodology to identify and classify sensitive data in the production environment.	No exceptions noted.
		Critical production equipment is maintained under warranty and maintenance or Service Level Agreements (SLAs) with 3rd party vendors.	Inquired of management to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.	No exceptions noted.
		A management-approved methodology is utilized to monitor patch releases, distribute patches to relevant devices and apply the patches to the device.	Inquired of management to determine that a methodology is utilized to monitor patch releases, distribute patches to relevant devices and apply the patches to the device.	No exceptions noted.
		Documented change requests are completed for bug fixes, enhancements and new development. Requests are reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	Inspected a judgmental sample of product changes from the review period for entries in the tracking system to determine that requests were reviewed and prioritized by management based on business needs and resource availability.	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		All planned critical infrastructure changes follow a structured change methodology, including testing of hardware changes where necessary.	Inspected the infrastructure change management policies and procedures to determine that all critical infrastructure changes follow a structured change methodology.	No exceptions noted.
		A ticketing system is utilized to manage systems infrastructure issues and changes. Tickets are assigned to support personnel based on the nature of the ticket.	Inspected a judgmental sample of logs from the ticketing system showing closed tickets to determine that a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on the nature of the ticket.	No exceptions noted.
		Redundant architecture is built into network infrastructure, including, but not limited to the: • Network interface cards (NICs) • High availability networks • Firewalls • Switches • Web servers • DB cluster • PBX.	Observed the redundant network infrastructure components to determine that redundant architecture was built into certain aspects of the network infrastructure.	No exceptions noted.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Observed and inspected relevant policies and procedures to determine that policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security and availability commitments and requirements.	Documented change requests are completed for bug fixes, enhancements and new development. Requests are reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	Inspected a judgmental sample of product changes from the review period for entries in the tracking system to determine that requests were reviewed and prioritized by management based on business needs and resource availability.	No exceptions noted.
		Documented policies and procedures are in place to centrally maintain, manage and monitor application development, maintenance and documentation activities.	Inspected the documentation to determine that a documented process is utilized to centrally maintain, manage and monitor application development and maintenance activities.	No exceptions noted.
		Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.	Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assigning responsibility and accountability for system changes and maintenance.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding testing, evaluating, and authorizing system components before implementation.	Inspected the policies and procedures related to testing, evaluating, and authorizing before implementation of components.	No exceptions noted.
		Procedures are in place to provide that emergency changes are documented and authorized on a timely basis.	Inspected policies and procedures to determine that procedures exist to provide that emergency changes are documented and timely authorized.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A management-approved methodology is utilized to monitor patch releases, distribute patches to relevant devices and apply the patches to the device.	Inquired of management to determine that a methodology is utilized to monitor patch releases, distribute patches to relevant devices and apply the patches to the device.	No exceptions noted.
		A small server test environment is utilized to ensure that patches and upgrades to critical services can be tested before being introduced to the production environment.	Observed test servers to determine that a server test environment is utilized.	No exceptions noted.
		The Leadership Team must approve all changes made to the system software, hardware or infrastructure.	Inspected policies and procedures to determine that the Leadership Team must approve all changes made to the software, hardware and infrastructure.	No exceptions noted.
		Documented change requests are completed for bug fixes, enhancements and new development. Requests are reviewed and prioritized by management based on business needs and resource availability, and assigned to personnel for action.	Inspected a judgmental sample of product changes from the review period for entries in the tracking system to determine that requests were reviewed and prioritized by management based on business needs and resource availability.	No exceptions noted.
		A written change management form is completed and properly approved before core changes are made to production application code.	Inspected a sample change management form to determine that a change management form is completed and properly approved before core changes are made to production application code.	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Quality assurance personnel perform quality assurance testing for application changes and update the change request ticket history to indicate approval of the test results prior to migration to the production environment.	Inspected a judgmental sample of emails for changes promoted to production during the review period to determine that quality assurance personnel perform quality assurance testing for application changes.	No exceptions noted.
		User acceptance testing is performed and signed off on by stakeholders before migration to the production environment.	Inspected a judgmental sample of code releases from the review period to determine that user and stakeholder approvals were obtained before changes were migrated to the production environment.	No exceptions noted.
		Program development is performed in a distinct development environment that is logically separated from the production environment.	Observed the location of the servers for each environment to determine that development environment is logically separated from the production environment.	No exceptions noted.
			Inspected network configurations to determine that development and test environments are logically separated from the production environment.	No exceptions noted.
			Inspected the checkout process from the version control software and a judgmental sample of local development machines to determine that development takes place on developers' local machines.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO SECURITY AND AVAILABILITY PRINCIPLES

CC7.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The quality assurance and testing efforts are performed in a distinct test environment that is physically and logically separated from the production environment.	Observed the location of the servers for each environment to determine that quality assurance and test environments are physically separated from the production environment.	No exceptions noted.
		All planned critical infrastructure changes follow a structured change methodology, including testing of hardware changes where necessary.	Inspected the infrastructure change management policies and procedures to determine that all critical infrastructure changes follow a structured change methodology.	No exceptions noted.
		Change management software is utilized to manage application changes, and the associated reporting and logging functions.	Inspected and observed the application to determine that change management software is utilized to manage application changes, and the associated reporting and logging functions.	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR AVAILABILITY

Availability Principle and Criteria Table
The availability principle refers to the system's availability for operations and use as committed or agreed.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.	Policies and procedures are in place to guide personnel regarding monitoring system capacity to achieve customer commitments or other agreements regarding availability.	Inspected the policies and procedures to determine that policies and procedures were in place to guide personnel regarding monitoring system capacity to achieve customer commitments or other agreements regarding availability.	No exceptions noted.
		Policies and procedures are in place for identifying and documenting the system availability and related security requirements of authorized users.	Inspected the policies and procedures to determine that the entity's system availability and related security policies were established.	No exceptions noted.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	Policies and procedures are in place to guide personnel regarding the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	Inspected the security policies and procedures and the service level agreement to determine that the entity's policies included procedures regarding the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	No exceptions noted.
		ROGERS utilizes a third party data center for hosting critical production servers and networking equipment. The environmental controls at the third party data center are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	Inspected the third party data center SOC 1-SSAE 16 audit report for the review period October 1, 2013 to September 30, 2014 to determine that environmental protections are present at the facility utilized by ROGERS.	No exceptions noted.
		Third party automated backup applications are utilized to perform scheduled system backups.	Inspected the third party automated backup system to determine that automated backup systems are utilized to perform scheduled system backups.	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR AVAILABILITY

Availability Principle and Criteria Table
The availability principle refers to the system's availability for operations and use as committed or agreed.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3	Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.	Management performs systematic reviews of the backup applications and logs to detect abnormalities in the backup process.	Inspected a judgmental sample of backup application logs or reports to determine that management performs systematic reviews of the backup applications and logs to detect abnormalities in the backup process.	No exceptions noted.
		Only ROGERS authorized personnel are granted access rights to recall backup data from the RAID array.	Inspected the backup media access rights to determine that only ROGERS authorized personnel are granted rights to recall backup data from the RAID array.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding recovering and continuing service in accordance with documented customer commitments or other agreements.	Inspected the policies and procedures and service level agreement s to determine that policies and procedures were in place to guide personnel regarding recovering and continuing service in accordance with documented customer commitments or other agreements.	No exceptions noted.
		Procedures have been implemented to provide for the integrity of backup data and systems maintained to support the entity's defined system availability policies.	Inspected procedures and related documentation to determine that procedures have been implemented to provide for the integrity of backup data and systems maintained to support the entity's defined system availability policies.	No exceptions noted.
			Observed the backup, storage, and recover process to determine that procedures have been implemented to provide for the integrity of backup data and systems.	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR AVAILABILITY

Availability Principle and Criteria Table
The availability principle refers to the system's availability for operations and use as committed or agreed.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management performs test restorations of backup data on a periodic basis to verify the success of the backup processes and employee readiness.	Inspected a judgmental sample of restore logs to determine that backup data is restored on a periodic basis to verify the success of the backup processes and employee readiness.	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

Processing Integrity Principle and Criteria Table
The processing integrity principle refers to the system's processing being complete, valid, accurate, timely and authorized.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PI1.1	Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements.	Policies and procedures are in place for identifying and documenting the system processing integrity and related security requirements of authorized users.	Inspected the policies and procedures to determine that the entity's system processing integrity and related security policies were established.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding monitoring system capacity to achieve customer commitments or other agreements regarding availability.	Inspected the policies and procedures to determine that policies and procedures were in place to guide personnel regarding monitoring system capacity to achieve customer commitments or other agreements regarding availability.	No exceptions noted.
		ROGERS utilizes the services of IO Data Center to house certain critical production servers and networking systems.	Inspected the services agreement with IO Data Center to determine that ROGERS utilizes its services.	No exceptions noted.
		IO Data Center's SOC 1 Type II report for the period October 1, 2013 to September 30, 2014 describes controls related to physical security including: • Building access • Visitor access • Server room access • Environmental controls • Security Cameras • Confidential destruction	Reviewed the SOC 1 Type II report for IO Data Center to determine that the report included descriptions of physical security controls that exist at the data for the period October 1, 2013 to September 30, 2014.	No exceptions noted.
		Documented backup procedures are in place for company systems deemed critical by management, to guide personnel in performing backup system tasks.	Inspected documented backup procedures to determine that documented backup procedures are in place for critical ROGERS systems.	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

Processing Integrity Principle and Criteria Table
The processing integrity principle refers to the system's processing being complete, valid, accurate, timely and authorized.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Third party automated backup applications are utilized to perform scheduled system backups.	Inspected the third party automated backup system to determine that automated backup systems are utilized to perform scheduled system backups.	No exceptions noted.
		Success and failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.	Inquired of management to determine that notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.	No exceptions noted.
			Inspected a judgmental sample of emailed notifications to determine that notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.	No exceptions noted.
		Only ROGERS authorized personnel are granted access rights to recall backup data from the RAID array.	Inspected the backup media access rights to determine that only ROGERS authorized personnel are granted rights to recall backup data from the RAID array.	No exceptions noted.
PI1.2	System inputs are measured and recorded completely, accurately, and timely in accordance with processing integrity commitments and requirements.	Procedures have been implemented to maintain completeness, accuracy, timeliness, and authorization of inputs and are consistent with the documented system processing integrity policies.	Inspected procedures related to completeness, accuracy, timeliness, and authorization of inputs to determine that measures have been implemented to maintain completeness, accuracy, timeliness, and authorization of inputs and are consistent with the documented system processing integrity policies.	No exceptions noted.

Processing Integrity Principle and Criteria Table
The processing integrity principle refers to the system's processing being complete, valid, accurate, timely and authorized.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Documented policies and procedures are in place, which govern critical data communication activities.	Inspected policies and procedures which govern critical data communication activities to determine that documented policies and procedures are in place, which govern critical data communication activities.	No exceptions noted.
		Transaction processing performed on web-based applications is secured through the use of the Secure Socket Layer (SSL) encryption protocol over HTTPS connections.	Inspected the web application SSL certificates to determine that transaction processing performed on web-based applications is secured through the use of the Secure Socket Layer (SSL) protocol over HTTPS connections.	No exceptions noted.
PI1.3	Data is processed completely, accurately, and timely as authorized in accordance with processing integrity commitments and requirements.	Procedures have been implemented to provide for the completeness, accuracy, and timeliness of backup data and systems.	Inspected policies and procedures to determine that procedures have been implemented to provide for the completeness, accuracy, and timeliness of backup data and systems.	No exceptions noted.
		Procedures have been implemented to enable tracing of information inputs from their source to their final disposition and vice-versa.	Inspected procedures to determine that procedures exist to enable tracing of information inputs from their source to their final disposition and vice-versa.	No exceptions noted.
PI1.4	Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.	Policies and procedures are in place for classifying data based on its criticality and sensitivity and that classification is one of many factors used to define protection requirements, access rights and restrictions, and retention and destruction requirements.	Inspected the policies and procedures to determine that data classification, protection requirements, access rights, access restrictions, and retention and destruction policies were established.	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

Processing Integrity Principle and Criteria Table
The processing integrity principle refers to the system's processing being complete, valid, accurate, timely and authorized.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Third party automated backup applications are utilized to perform scheduled system backups.	Inspected the third party automated backup system to determine that automated backup systems are utilized to perform scheduled system backups.	No exceptions noted.
		Success and failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.	Inquired of management to determine that notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.	No exceptions noted.
			Inspected a judgmental sample of emailed notifications to determine that notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.	No exceptions noted.
		Only ROGERS authorized personnel are granted access rights to recall backup data from the RAID array.	Inspected the backup media access rights to determine that only ROGERS authorized personnel are granted rights to recall backup data from the RAID array.	No exceptions noted.
PI1.5	System output is complete, accurate, distributed, and retained in accordance with processing integrity commitments and requirements.	Procedures have been implemented to maintain completeness, accuracy, timeliness, and authorization of outputs and are consistent with the documented system processing integrity policies.	Inspected procedures related to completeness, accuracy, timeliness, and authorization of inputs to determine that measures have been implemented to maintain completeness, accuracy, timeliness, and authorization of outputs and are consistent with the documented system processing integrity policies.	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

Processing Integrity Principle and Criteria Table
The processing integrity principle refers to the system's processing being complete, valid, accurate, timely and authorized.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PI1.6	Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	Policies and procedures are in place to ensure that modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	Observed and inspected relevant policies and procedures to determine that policies and procedures are in place to ensure that modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	No exceptions noted.
		Procedures have been implemented to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.	Inspected policies and procedures and disaster recovery plan to determine that procedures have been implemented to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.	No exceptions noted.
		Only ROGERS' authorized personnel are granted access rights to recall backup data from the RAID array.	Inspected the backup media access rights to determine that only ROGERS authorized personnel are granted rights to recall backup data from the RAID array.	No exceptions noted.

END OF REPORT