BROWN SMITH WALLACE

THE FIRM FOR GROWTH.™

STLCOM.COM

Technology made easy.

STL COMMUNICATIONS, INC.

System and Organization Controls (SOC 2) Report on the Suitability of the Design of Controls (Type 1) at a Service Organization Relevant to Security and Availability

November 30, 2018

STL COMMUNICATIONS, INC.

Report on the Suitability of the Design of Controls (Type 1)
at a Service Organization Relevant to Security and Availability

Table of Contents

SECTION I

Independent Service Auditor's Report
Provided by Brown Smith Wallace, LLP

BROWN SMITH WALLACE
6 CITYPLACE DRIVE SUITE 900 ST. LOUIS, MO 63141 PH 314.983.1200 FX 314.983.1300 BROWNSMITHWALLACE.COM
THE FIRM FOR GROWTH.™

Independent Service Auditor's Report

Management of STL Communications, Inc.
Chesterfield, MO 63005

Scope

We have examined the description in Section III titled "Description of Total Voice Managed Hosting System Provided by STL Communications, Inc." (description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2® July 2015) (description criteria) and the suitability of the design of the controls described therein to meet the criteria for the security and availability principle(s) set forth in TSP Section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016) (applicable trust services criteria), as of November 30, 2018. The controls included in the description are those that management of STL Communications, Inc. believes are likely to be relevant to meeting the applicable trust services criteria, and the description does not include those aspects of the Total Voice Managed Hosting system that are not likely to be relevant to meeting the applicable trust services criteria.

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

As indicated in the description, STL Communications, Inc. uses a subservice organization to perform data center hosting and off-site data storage. The description indicates that certain applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of STL Communications, Inc.'s controls are suitably designed and operating effectively, along with the related controls at STL Communications, Inc. The description presents STL Communications, Inc.'s system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented and suitably designed at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organization. Our examination did not extend to the controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibility

In Section II, STL Communications, Inc. has provided its assertion titled "Assertion of Management of STL Communications, Inc." (assertion) about the fairness of the presentation of the description based on the description criteria and suitability of the design of the controls described therein to meet the applicable trust services criteria. STL Communications, Inc. is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls that are suitably designed and operating effectively to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

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 and on the suitability of the design of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed to meet the applicable trust services criteria if the controls operated effectively as of November 30, 2018. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design of controls involves—

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed to meet the applicable trust services criteria as of November 30, 2018.
- assessing the risks that the description is not fairly presented based on the description criteria and that the controls were not suitably designed to meet the applicable trust services criteria.
- evaluating the overall presentation of the description, the suitability of the applicable trust services criteria stated therein, and the suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important in its own particular environment. Because of their nature and inherent limitations, controls at a service organization may not always be suitably designed to meet the applicable trust services criteria, even if the controls operated effectively. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability

of the design of the controls to meet the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Other Matter
We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion
In our opinion, in all material respects, based on the description criteria identified in STL Communications, Inc.'s assertion and the applicable trust services criteria—

a. the description fairly presents the system that was designed and implemented as of November 30, 2018.

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 as of November 30, 2018, and the subservice organization and user entities applied the complementary controls assumed in the design of STL Communications, Inc.'s controls as of November 30, 2018.

Restricted Use
This report is intended solely for the information and use of STL Communications, Inc.; user entities of STL Communications, Inc.'s Total Voice Managed Hosting System as of November 30, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- The nature of user entity controls and responsibilities, and their role in the user entities internal control as they relate to, 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 prevent meeting 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 the specified parties.

Brown Smith Wallace, LLP

St. Louis, MO
November 30, 2018

SECTION II

Assertion of the Management of STL Communications, Inc.

Assertion of the Management of STL Communications, Inc.

We have prepared the description titled Total Voice Managed Hosting System (description) based on the criteria for a description of a service organization's system identified in *paragraph 1.26 of the AICPA Guide, Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2® July 2015)* (description criteria). The description is intended to provide users with information about the Total Voice Managed Hosting System, particularly system controls intended to meet the criteria for the security and availability principle(s) set forth in *TSP 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services principles), as of November 30, 2018.

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

1) The description fairly presents the Total Voice Managed Hosting System as of November 30, 2018 based on the following description criteria:
   a) The description contains the following information:
      i) The types of services provided.
      ii) The components of the system used to provide the services, which are as follows:
         (1) *Infrastructure.* The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
         (2) *Software.* The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
         (3) *People.* The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
         (4) *Processes.* The automated and manual procedures.
         (5) *Data.* Transaction streams, files, databases, tables, and output used or processed by a system.
      iii) The boundaries or aspects of the system covered by the description.
      iv) For information provided to, or received from, subservice organizations, and other parties—
         (1) how the information is provided or received and the role of the subservice organizations and other parties.
         (2) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

v) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

(1) Complementary user entity controls contemplated in the design of the service organization's system.

vi) If the service organization presents the subservice organization using the carve-out method—

(1) the nature of the services provided by the subservice organization.

(2) each of the applicable trust services criteria that are 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.

vii) Any applicable trust services criteria that are not addressed by a control and the reasons.

b) The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.

2) The controls stated in the description were suitably designed as of November 30, 2018 to meet the applicable trust services criteria.

Steve Leidholdt
STL Communications, Inc.
President/CEO

SECTION III

Description of Total Voice Managed Hosting System
Provided by STL Communications, Inc.

Overview of Operations

Company Background

Located and headquartered in St. Louis, Missouri, STL Communications blends that can-do spirit and desire to help clients with the latest communications products and services. We take pride in knowing that we helped solve a business problem or that our technology provided improvements. We believe in old-fashioned values like hard work, integrity, honesty, dedication, and personal responsibility. We drive creativity, generate ideas and accelerate smarter decisions providing our customers with better productivity, greater profitability and a stronger competitive advantage.

With over 600 years of combined employee experience and manufacturer best-in-class and world-class ratings, STL Communications has the knowledge, strength, ability, and support to meet all of your collaboration and communication challenges. Our customers tell us we are always professional, flexible and easy to work with – "you make things happen for us", "you provide clear and understandable ideas and we can count on STL Communications to solve our communication problems."

Along with our top-notch Customer Care Center and complete communication system management and monitoring services, we have a staff of fully certified technicians who will keep your technology running strong. In addition, our sales people and engineers will keep bringing new ideas and innovation to help your business increase employee productivity and information, drive better customer satisfaction, while striving to bring more profit to your bottom line.

Description of the Information Technology Operations for User Entities

The concept of STLCOM's Total Voice managed service is really quite simple. Consider how your organization currently purchases utility services in a consumption model: paying only for what you use on a monthly basis. Gas, electric, and water utility companies make large investments in production facilities and deliver infrastructure to reliably provide these services to their customers.

STL Communications, Inc. has invested in the production and delivery infrastructure required to provide reliable, quality hosted telephony and cloud services. Why not simply purchase the telephone services you need as you consume them and never again purchase another phone system?

Types of Services Provided

STL Communications offers two managed solution models in order to suit your business needs best: Total Voice Cloud and Total Voice Hybrid. Both feature the option to scale and customize the solution to fit your specific needs, as well as the following:

- All the latest unified communications features, Powered by Avaya
- Use the device of your choice – VoIP, digital, analog, softphone or mobile app
- Voicemail with integration to email
- Smart phone integration with both iPhone and Android devices
- Multi-party audio conferencing bridge
- E911 services

Components of the System

Infrastructure

STL Communications infrastructure components are separated into the following groupings:

- The development environments are used by the development and QA teams to test changes to the applications prior to implementation into production.
- Service production is hosted at a third-party data center.
- Customer production data is also housed at the third-party data center.

Software

STL Communications utilizes a variety of software products to support the Total Voice Hosting system.

People

STL Communications personnel provide the following core support services over Total Voice Hosting environment:

- Systems and Network Monitoring
- Security
- Backup Operations
- Network Management
- Application Change Management
- Infrastructure Change Management

Policies and procedures require segregation of duties between all teams. Procedures, with respect to personnel, encourage annual vacations and require delegation of duties when staff is absent.

Personnel are experienced, qualified information systems professionals that are technically competent. Detailed descriptions of job requirements are utilized to fulfill the needs of open positions. For existing staff, management provides close supervision to determine that skills are continually advancing. STL Communications performs employee background checks to screen prospective employees as part of the applicant process.

Procedures

STL Communications requires a high standard of performance to meet the service requirements of each customer. Policies and procedures have been established to effectively meet the control objectives of STL Communications and its customers. This section provides a brief description of the control policies and procedures. Management has developed and communicated procedures to restrict access to its STL Communications system. Changes to these procedures are performed as needed and are authorized by management.

Data
Data, as defined by STL Communications, constitutes application data and user generated data.

Relevant Aspects of Internal Control Environment

Control Environment
The information in this section is intended to provide an understanding of STL Communications' culture of controls at a high level. The organizational structure of STL Communications is designed to allow for information and communication flexibility and responsiveness to client needs, while at the same time ensuring that management is aware of important issues. The departmental structure divides operations into task areas with responsible managers and staff for implementation. Initiative to develop and implement controls comes from both the staff and management. Management initiates controls development when required to adhere to best practices, meet a regulatory requirement, or improve a process. Staff are encouraged to identify the need for controls in their areas to improve all aspects of the products.

Management Philosophy
Security Management
A formal management structure supporting the security and controls for the organization is in place. By policy, the President is ultimately responsible for the oversight of the STL Communications security system. This is achieved by controls assigning appropriate governance oversight and authority to the operational groups of the Company.

Security Policies
STL Communications has based its policies and procedures upon the standards laid out by various frameworks including the NIST (www.nist.gov) family of special publications. The base STL Communications customer population are small to mid-size companies.

Personnel Security
Within the daily infrastructure and network interaction, personnel are secured using several processes around their workstations, the network, and training. Workstations are controlled and protected within an Active Directory (AD) environment, with required anti-malware installed and running. In addition, workstations are required to use encryption. The network is protected by firewalls and other industry standard methodologies.

Security policies covering controls for most issues are available to the general STL Communications employee population on the Company's Intranet and are covered in mandatory security training. These policies cover all aspects of the individual's responsibility for maintaining corporate security including:

- Individual security responsibility
- Best practices
- Data management and safekeeping
- Data ownership
- Physical security

Physical Security and Environmental Controls

The production system deployed by STL Communications exists within the third-party data center platform, so they enjoy all of the physical protection and environmental redundancies deployed by that service. The STL Communications physical facility employs safeguards such as a secure server room facility.

Access to sensitive locations is restricted to current employees with demonstrated need using multiple factor authentication. Access is reviewed as needed.

Change Management

STL Communications employs a structured system and application development and maintenance process which include controls in place to ensure changes are tested thoroughly before being migrated to production. The concept of separation of duties is followed throughout the development/deployment process.

Change requests are documented formally in a controlled change management system, with major changes requiring management approval. There is separation of duties; developers may not approve, test, or migrate their own changes.

System Monitoring

Tools are used for monitoring the performance of the production instances of STL Communications services. Alerts are set up to be delivered to on call and support personnel in the event of a detected anomaly.

Processing capacity is monitored on an ongoing basis in accordance with SLAs, key performance indicators (KPIs), and other performance related parameters. Processes are monitored through service level management procedures that monitor compliance with commitments and requirements. Results are shared according to policies. Finally, intrusion detection systems are in place.

Problem Management

STL Communications services pages contain information on how to contact customer support in the event of an issue, or simply a question. Customer support operates in a tiered fashion, with calls and e-mails coming in to the main center. Should the first tier be unable to resolve the issue, it is escalated. Customer support uses tools to manage and track issues.

Internally, problems requiring development intervention, including code changes, are tracked in the tools.

System Account Management

System accounts are user based – that is – no generic or shared accounts are permitted. Accounts must be assigned to an individual. Accounts not in use or assigned incorrectly are disabled or reassigned.

Client accounts for STL Communications are setup by privileged administrators and are limited to their organizational unit.

Risk Assessment Process
Risk assessment is governed by policy. Risk management software is used to help document, manage, and resolve identified risks; a review of the risk position is performed annually.

External and internal scans of the STL Communications network are performed by the IT Department. For IT security risk scan results, any problem areas are identified; and a remediation plan is created and executed to fix the issue.

Information and Communication Systems
Duties and responsibilities of the IT and Operations staff are depicted in organizational charts that are up-to-date and maintained accordingly. Appropriate levels of supervision are defined and exist within each functional area. Additionally, job responsibilities and descriptions are documented for IT and Operations functions within the organization. Throughout STL Communications, each functional area is generally responsible for the development and implementation of procedures and controls within its respective area. The information system components relevant to services provided to user organizations are described in various sections of this report.

Service agreements are maintained between STL Communications and their customers. The agreements include a service description and availability commitments.

Monitoring Controls
Controls are ultimately monitored by management of STL Communications. Frequency of monitoring is defined by policy; where possible, monitoring items are placed in a table where they are tracked. Frequency varies by control, some are annual, while other many be weekly.

Trust Services Criteria, Related Controls, and Tests of Controls

Relevant trust services criteria and STL Communications, Inc.'s related controls are included in Section IV of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section IV. Although the controls are presented in Section IV, they are, nevertheless, an integral part of STL Communications' description of its system.

Expected Subservice Organization Controls

STL Communications uses the service organization to perform data center housing and off-site data storage. The description above does NOT include controls implemented at the subservice organization. The chart below illustrates controls STL Communications "expects" to be implemented, suitably designed, and operating effectively at the subservice organization to meet the trust services criteria listed below:

Trust Services Criteria	Expected Control
Common Criteria Related to Logical and Physical Access 5.5: Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.	Physical access to facilities that house IT resources, servers, and related hardware such as firewalls and routers is restricted to authorized individuals by access systems and monitored by video surveillance. Physical access cards are managed by building staff. Access card usage is logged and reviewed by staff. Cabinets are locked with keys and keys are controlled. Requests for physical access privileges to the computer facilities require the approval of management.
Additional Criteria for Availability 1.1: 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.	Operational monitoring system includes weekly reports of aggregate data from calls, alarms, and problems from all facilities and includes data for capacity and usage.
Additional Criteria for Availability 1.2: Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	Environmental protections have been installed including the following: • Power distribution • Cooling systems • Battery and generator backup in the event of power failure • Redundant communication lines • Fire detection and suppression Operations personnel monitor the status of environmental protections during each shift. Environmental protections receive maintenance on at least an annual basis.

Complementary User Entity Controls

STL Communications' controls are designed with the assumption that certain controls would be placed in operation by user entities. This section describes some of the controls that should be in operation at user entities to complement the controls at STL Communications. User auditors determine whether user entities have established controls to provide reasonable assurance that:

- Customers have retained responsibility for administering security on machines used to access the STL Communications software.
- Customers should implement policies and procedures to ensure only authorized and properly trained personnel are granted logical access to the STL Communications software and that access levels are appropriate based on job functions.
- Customers are responsible for communicating problems related to the STL Communications software to the appropriate STL Communications personnel in a timely manner. The customer should maintain contact with STL Communications to ensure the problem is appropriately resolved.
- Customers should ensure the application is configured to meet their specific compliance needs.
- Customers should ensure the application is configured to be consistent with data retention needs.
- Customers are responsible for validating the completeness and accuracy of data input into the application.
- Customers should ensure that the implementation of the application meets their requirements.
- Customers are responsible for reviewing and validating the completeness and accuracy of outputs and reports from the application.

The list of user control considerations presented here does not represent a comprehensive set of all the controls that should be employed by user entities. Customers and their auditors should recognize that specific responsibilities of clients and STL Communications are described in contracts as negotiated between the two parties. Other controls may be required at user entities.

SECTION IV

Trust Services Principles, Criteria, and Related Controls
Provided by Brown Smith Wallace, LLP

Common Criteria

Criteria		Control Ref.	STL Communications, Inc. Controls
CC1.0	***Common Criteria Related to Organization and Management***		
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability.	**CC1.1a**	The company evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.
		CC1.1b	Job requirements are documented in job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.
		CC1.1c	Job descriptions are reviewed and updated by management as needed.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.	**CC1.1a**	The company evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.
		CC1.1b	Job requirements are documented in job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.
		CC1.1c	Job descriptions are reviewed and updated by management as needed.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and	**CC1.3a**	Policies and procedures for significant processes that address system requirements are available on the intranet.
		CC1.1b	Job requirements are documented in job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC1.0	***Common Criteria Related to Organization and Management***		
	availability and provides resources necessary for personnel to fulfill their responsibilities.	**CC1.3c**	The experience and training of candidates for employment or transfer are evaluated before they assume the responsibilities of their position.
		CC1.3d	Management establishes skills and continued training with its commitments and requirements for employees.
		CC1.3e	Management monitors compliance with training requirements.
		CC1.3f	Management evaluates the need for additional tools and resources in order to achieve business objectives, during its ongoing and periodic business planning and as part of its ongoing risk assessment and management process.
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 system requirements as they relate to security and availability.	**CC1.4a**	Management monitors employees' compliance with the code of conduct through customer and employee complaints.
		CC1.4b	Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and to formally re-affirm them annually thereafter.
		CC1.4c	Management uses a list of characteristics to evaluate candidates based on sensitivity or skill requirements for the given position.
		CC1.4d	New employees must pass a criminal and financial trust background check.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC2.0	***Common Criteria Related to Communications***		
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	**CC2.1a**	System descriptions are available to authorized external users that delineate the boundaries of the system and describe relevant system components as well as the purpose and design of the system.
		CC2.1b	Documentation of the system description is available to authorized users via the entity's customer-facing website.
		CC2.1c	System user guides are provided if requested by the customer and are also available at AVAYA.com/user guides.
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 users to enable them to carry out their responsibilities.	**CC2.1a**	System descriptions are available to authorized external users that delineate the boundaries of the system and describe relevant system components as well as the purpose and design of the system.
		CC2.1b	Documentation of the system description is available to authorized users via the entity's customer-facing website.
		CC2.2c	A description of the organizational structure, system support functions, processes, and organizational roles and responsibilities is posted on the entity's intranet and available to entity internal users. The description delineates the parties responsible, accountable, consented, and informed of changes in design and operation of key system components.
		CC2.2d	Commitments regarding the system are included in the master services agreement and customer-specific service level agreements. In addition, a summary of these commitments is available on the entity's customer facing website.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC2.0	***Common Criteria Related to Communications***		
		CC2.2e	Personnel are required to read and accept the entity's code of conduct and the statement of security, confidentiality, and privacy practices upon hire.
		CC2.2f	Processes are monitored through service level management procedures that monitor compliance with service level commitments and agreements. Results are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties, including customers, when such commitments and agreements are not met.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	**CC1.3a**	Policies and procedures for significant processes that address system requirements are available on the intranet.
		CC2.3b	Policies and procedures for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and available on the intranet.
		CC2.3c	Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on the customer website and in system documentation.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.	**CC1.3a**	Policies and procedures for significant processes that address system requirements are available on the intranet.
		CC2.2f	Processes are monitored through service level management procedures that monitor compliance with service level commitments and agreements. Results are shared with applicable personnel and customers, and actions are taken and communicated to relevant parties, including customers, when such commitments and agreements are not met.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC2.0	***Common Criteria Related to Communications***		
		CC2.3b	Policies and procedures for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and available on the intranet.
		CC2.3c	Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on the customer website and in system documentation.
CC2.5	Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	**CC2.3b**	Policies and procedures for significant processes, which include responsibility for reporting operational failures, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and available on the intranet.
		CC2.3c	Customer responsibilities, which include responsibility for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on the customer website and in system documentation.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.	**CC2.6a**	Proposed system changes affecting customers are published on the customer website before their implementation. Users are given the chance to participate in user acceptance testing for major changes prior to implementation. Changes made to systems are communicated and confirmed with customers through ongoing communications mechanisms such as customer care meetings and via the customer website.
		CC2.6b	IT/Engineering must obtain approval from the V.P. of Technical Services before notification is sent out to Total Voice Customers notifying them of the coming changes.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC2.0	***Common Criteria Related to Communications***		
		CC2.6c	The system change calendar that describes changes to be implemented is posted on the entity intranet.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC3.0	***Common Criteria Related to Risk Management and Design and Implementation of Controls***		
CC3.1	The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system); (2) analyzes the significance of risks associated with the identified threats; (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies); (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control; and (5) reassesses, and revises as necessary, risk assessments and mitigation strategies based on the identified changes.	**CC3.1a**	A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.
		CC3.1b	The company uses a configuration management database and related processes to capture key system components, technical and installation specific implementation details, and to support ongoing asset and service management commitments and requirements.
		CC3.3a	During the risk assessment and management process, management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.
		CC3.2a	Management identified risks are rated using a risk evaluation process and ratings are reviewed by management.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and	**CC3.2a**	Management identified risks are rated using a risk evaluation process and ratings are reviewed by management.
		CC3.2b	Internal and external vulnerability scans are performed annually, and the frequency is adjusted as required to meet ongoing and changing commitments and requirements.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC3.0	***Common Criteria Related to Risk Management and Design and Implementation of Controls***		
	monitoring of those activities, and updates the controls, as necessary.		
CC3.3	The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological) 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 monitoring of those activities, and updates them as necessary.	**CC3.3a**	During the risk assessment and management process, management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives.
		CC3.2a	Management identified risks are rated using a risk evaluation process and ratings are reviewed by management.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC4.0	***Common Criteria Related to Monitoring of Controls***		
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	**CC4.1a**	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software sends a message to the operations center and automatically opens an incident, problem, or change management "ticket" record when specific predefined thresholds are met.
		CC3.2b	Internal and external vulnerability scans are performed annually, and the frequency is adjusted as required to meet ongoing and changing commitments and requirements.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***		
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.	**CC5.1a**	Standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.
		CC3.2b	Internal and external vulnerability scans are performed annually, and the frequency is adjusted as required to meet ongoing and changing commitments and requirements.
		CC5.1c	Users are provided access to resources to meet their job responsibilities.
		CC5.1d	External access by employees is permitted only through an encrypted virtual private network (VPN) connection.
		CC5.1e	A role-based security process has been defined with an access control system that is required to use roles.
		CC5.1f	An employee termination checklist is completed by the dismissing manager before termination takes place.
		CC5.1g	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by management.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is	**CC5.1a**	Standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.
		CC5.1c	Users are provided access to resources to meet their job responsibilities.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***		
	administered by the entity, user system credentials are removed when user access is no longer authorized.	**CC5.1d**	External access by employees is permitted only through an encrypted virtual private network (VPN) connection.
		CC5.1e	A role-based security process has been defined with an access control system that is required to use roles.
		CC5.1f	An employee termination checklist is completed by the dismissing manager before termination takes place.
		CC5.1g	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by management.
		CC5.2g	System security is configured to require users to change their password upon initial sign-on and periodically thereafter.
		CC5.2h	Individuals are provided a unique user account.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.	**CC5.1a**	Standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.
		CC5.1c	Users are provided access to resources to meet their job responsibilities.
		CC5.1d	External access by employees is permitted only through an encrypted virtual private network (VPN) connection.
		CC5.1e	A role-based security process has been defined with an access control system that is required to use roles.
		CC5.1f	An employee termination checklist is completed by the dismissing manager before termination takes place.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***		
		CC5.1g	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by management.
		CC5.2g	System security is configured to require users to change their password upon initial sign-on and periodically thereafter.
		CC5.2h	Individuals are provided a unique user account.
CC5.4	Access to data, software, functions, and other IT resources is authorized and modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.	**CC5.4a**	Formal role-based access controls restrict access to system and infrastructure components.
		CC5.4b	User access requests for a specific role are approved by the user manager and are submitted to the security group via the change management record system.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.	**CC5.5a**	An access fob based physical access control system is in place within the perimeter of facilities.
		CC5.5b	Visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.
		CC5.5c	Keys are issued to key personnel to gain access to sensitive areas.
		CC5.1c	Users are provided access to resources to meet their job responsibilities.
		CC5.1f	An employee termination checklist is completed by the dismissing manager before termination takes place.
CC5.6	Logical access security measures have been implemented to protect against security and availability threats from sources outside the	**CC5.1a**	Standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity

Criteria		Control Ref.	STL Communications, Inc. Controls
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***		
	boundaries of the system to meet the entity's commitments and system requirements.		configuration standards, and standardized access control lists.
		CC5.6b	External points of connectivity are protected by a firewall.
		CC5.6c	Firewall hardening standards are based on relevant applicable technical specifications and are updated periodically.
		CC5.1d	External access by employees is permitted only through an encrypted virtual private network (VPN) connection.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.	**CC5.7a**	VPN, SSL, secure file transfer program (SFTP), and other encryption technologies are used for defined points of connectivity and to protect communications between the processing center and users connecting to the processing center from within or external to customer networks.
		CC5.7b	Policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.
		CC5.7c	Data loss prevention software is used to scan for sensitive information in outgoing transmissions over public communication paths.
		CC5.7d	Backup media are encrypted during creation.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.	**CC5.8a**	The ability to install software on workstations and laptops is restricted to IT support personnel.
		CC5.8b	Antivirus software is installed on workstations, laptops, and servers supporting such software.
		CC5.8c	Antivirus software is configured to receive an updated virus signature at least daily. A network operation receives a

Criteria		Control Ref.	STL Communications, Inc. Controls
CC5.0	*Common Criteria Related to Logical and Physical Access Controls*		
			report of devices that have not been updated in 30 days and follows up on the devices.
		CC5.8d	The ability to install applications on systems is restricted to change implementation and system administration personnel.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC6.0	***Common Criteria Related to System Operations***		
CC6.1	Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.	**CC4.1a**	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software sends a message to the operations center and automatically opens an incident, problem, or change management "ticket" record when specific predefined thresholds are met.
		CC6.1b	IT administrator personnel receive telephone and e-mail requests for support, which may include requests to reset user passwords or notify entity personnel of potential breaches and incidents. IT administration personnel follow defined protocols for recording, resolving, and escalating received requests.
		CC6.1c	Weekly full-system and daily incremental backups are performed using an automated system.
CC6.2	Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	**CC6.2a**	IT Administrator personnel follow defined protocols for evaluating reported events. Security related events are assigned to the Senior Managing Group for evaluation.
		CC6.2b	IT Admin and management follow defined protocols for resolving and escalating reported events.
		CC6.2c	Resolution of security events (incidents or problems) is reviewed at the weekly management.
		CC6.2d	Internal and external users are informed of incidents in a timely manner and advised of corrective measure to be taken on their part.
		CC6.2e	Policies include probation, suspension, and termination as potential sanctions for employee misconduct.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC6.0	***Common Criteria Related to System Operations***		
		CC6.2f	Change management requests are opened for events that require permanent fixes.

Criteria		Control Ref.	STL Communications, Inc. Controls
CC7.0	***Common Criteria Related to Change Management***		
CC7.1	The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	**CC7.1a**	System change requests are evaluated to determine the potential effect of the change on security and availability commitments and requirements throughout the change management process.
		CC7.1b	System changes other than those classified as minor require the approval of the management and the Operations Manager prior to implementation.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.	**CC7.1a**	System change requests are evaluated to determine the potential effect of the change on security and availability commitments and requirements throughout the change management process.
		CC7.2b	During the ongoing risk assessment process and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are created based on the identified needs.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.	**CC7.1a**	System change requests are evaluated to determine the potential effect of the change on security and availability commitments and requirements throughout the change management process.
		CC7.3b	System change requests must be reviewed and approved by the owner of the infrastructure or software and management prior to work commencing on the requested change.
CC7.4	Changes to system components are authorized, designed, developed, configured,	**CC7.4a**	System change requests must be reviewed and approved by the owner of the infrastructure or software and the change

Criteria		Control Ref.	STL Communications, Inc. Controls
CC7.0	***Common Criteria Related to Change Management***		
	documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.		Senior Manager prior to work commencing on the requested change.
		CC7.4b	System and regression testing are prepared by the testing department using approved test plans and test data.
		CC7.4c	Standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists.
		CC7.4d	Changes to hardening standards are reviewed and approved by infrastructure management.
		CC7.4e	Separate environments are used for testing and production.

Additional Criteria for Availability

Criteria		Control Ref.	STL Communications, Inc. Controls
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	**A1.1a**	Processing capacity is monitored on an ongoing basis.
		A1.1b	Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.
		CC4.1a	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. This software sends a message to the operations center and automatically opens an incident, problem, or change management "ticket" record when specific predefined thresholds are met.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	**A1.2a**	Environmental protections have been installed including a sprinkler system and fire detectors.
		CC6.1c	Weekly full-system and daily incremental backups are performed using an automated system.
		A1.2c	Business continuity and disaster recovery plans have been developed and updated annually.
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	**CC6.1c**	Weekly full-system and daily incremental backups are performed using an automated system.
		A1.2c	Business continuity and disaster recovery plans have been developed and updated annually.