CH& CAIRNCROSS&HEMPELMANN
ATTORNEYS AT LAW

524 2nd Ave., Suite 500
Seattle, WA 98104
www.cairncross.com

office 206.587.0700
fax 206.587.2308

May 16, 2016

VIA U.S. MAIL AND ELECTRONIC MAIL

Mr. Phil Mocek
2141 S M Street
Tacoma, WA 98405
10378-42034147@requests.muckrock.com

Mr. Michael Morisy
MuckRock.com
105 Westbourne Lane
Ithaca, NY 14850
morisy@gmail.com

GoDaddy.com
Corporation Service Company
300 Deschutes Way SW, Ste 304
Tumwater, WA 98501
abuse@godaddy.com

Re: *Improper Posting of Protected Materials Related to Seattle Advanced Metering Infrastructure Initiative on MuckRock.com*

Dear Sir or Madam:

I am writing on behalf of Landis+Gyr Technology, Inc. ("Landis+Gyr") with respect to two documents that were recently posted on MuckRock.com that contain trade secrets and sensitive network security information. These documents are related to a recent request under the Washington Public Records Act ("PRA") submitted by Mr. Phil Mocek through the MuckRock.com website. Landis+Gyr will be taking legal action in the very near future to prevent release of its trade secrets, proprietary information, network security information, and other categories of information that are protected from public disclosure under the PRA and Washington's Uniform Trade Secrets Act ("UTSA"), RCW Chapter 19.108. In the meantime, recognizing that the documents were apparently made public through inadvertence or error on the part of the City of Seattle, we respectfully request your cooperation in removing these two documents from public view. To be clear, we do not object to the continued posting of any other documents related to Mr. Mocek's Public Records request on the MuckRock.com website, which includes, for example, documents related to the contract (from which trade secret information has been redacted) and the correspondence between Mr. Mocek and Seattle City Light's Public Records Officer. We are also willing to provide redacted versions of the two documents, with sensitive electronic security information removed, to repost on the website until conclusion of soon-to-be-filed legal proceedings.

The two documents in question apparently were released prematurely by the City of Seattle, before Landis+Gyr was allowed to redact trade secret and sensitive network security information, and before Landis+Gyr could exercise its rights to prevent release of protected information through the court system. We respectfully request that you immediately remove the two documents from the MuckRock.com website until such time as their protected status under the PRA and the UTSA can be resolved by the Washington courts. Please be aware that trade secret information of the kind contained in the documents is protected under the UTSA, and misappropriation of trade secret information may expose you to claims for legal damages and attorney's fees under RCW 19.108.030-.040.

The documents are attached to an email from Stacy Irwin, Seattle City Light's Public Records Officer, dated April 19, 2016, which is posted on MuckRock.com along with other correspondence related to Mr. Mocek's Public Records request. The documents are identified as "Req 9_Security Overview" and "Lands+Gyr Managed Services Report 2015 Final." Each is available in complete and unredacted form through links allowing a MuckRock.com user to "download," "view," or "embed" the documents.

Significant portions of the documents are protected from public disclosure under the PRA because they contain detailed discussions and descriptions of the Landis+Gyr's proprietary electronic security protocols and operations. These portions of the documents are protected from public disclosure under RCW 42.56.420(4), which provides that "[i]nformation regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of agency security, information technology infrastructure, or assets" is exempt from disclosure under the PRA.

The documents are also protected under the UTSA because Landis+Gyr's electronic security protocols and procedures were developed through an investment of millions of dollars and thousands of hours of research and development time. Making the documents public may allow Landis+Gyr's competitors to copy and duplicate its proprietary methods, thus destroying the value of this investment. Similarly, if a hacker or cyber-criminal used the information posted on MuckRock.com to penetrate Landis+Gyr's security systems, Landis+Gyr's investment in those systems would be destroyed, and the reliability of Seattle's electric grid could be put at risk.

For these reasons, the public availability of these two documents presents an immediate threat to Landis+Gyr that can only be relieved by removing those documents from MuckRock.com and from any other public forum where they may appear. We therefore request that you immediately remove the two documents from MuckRock.com, destroy any hard copies of the documents you have made, and remove the documents from any other public forum where they may be posted. We also request that you provide assistance to Landis+Gyr to identify any entities that may have downloaded these documents from MuckRock.com, so that we may take appropriate measures to assure these documents are not further disseminated.

Please feel free to contact me at any time if you have questions about anything discussed in this letter. We look forward to cooperation in this matter and, given the urgency of the situation, request a reply at your earliest convenience.

Very truly yours,

Eric L. Christensen

ELC:aea
cc: Jessica Nadelman, Assistant City Attorney, City of Seattle

Tab: Communications Network

Requirement 9 – Security Overview

The Landis+Gyr Gridstream security suite is built to US government and international standards. The Landis+Gyr cyber security system is built to Federal Information Processing Standard government computer security standard (FIPS 140) and includes National Security Agency suite B compliant cryptography. It is also built on the Common Criteria for Information Technology Security Evaluation which is an international standard (ISO/IEC 15408) for computer security certification.

Working with partners such as EMC/RSA Laboratories and SafeNet, the Gridstream security solution is based on open, non-proprietary mechanisms that provide compliance with industry standards and best practices including the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, NSA Suite B, AMI-SEC, NERC CIP, DOE and others.

Landis+Gyr also address dynamic risk management through ongoing penetration testing of the Gridstream AMI system. Landis+Gyr engaged Lockheed Martin to perform an objective NERC CIP and NIST focused risk assessment of the Gridstream AMI system in an effort to identify risk areas. This is in addition to internal and external risk assessments to identify, classify, and mitigate vulnerabilities that an attacker could exploit.

Compliance with standards such as NERC CIP 002-009 requires a consolidation of utility policies and procedures and vendor technology. Landis+Gyr is committed to continually enhancing product features with future development guided by industry standards.

Compliance with the industry, government and international standards for security, along with periodic penetration testing will assure utilities that the Landis+Gyr security systems are the best available in the industry. Landis+Gyr in cooperation with AEP deployed the first end-to-end secure AMI system utilizing these standards.

NISTIR 7628 Compliance

NISTIR 7628 is a set of guidelines for implementing Smart Grid security. The information and requirements within NISTIR 7628 provide valuable direction for developing effective cyber security strategies. Landis+Gyr has taken a standards based approach toward the development of the Gridstream AMI security solution that leverages much of the relevant information provided by NIST. Landis+Gyr has implemented security controls in all phases of the development cycle, from the design phase through implementation, maintenance, and device/product decommissioning. Landis+Gyr has developed and performed ongoing risk assessments and penetration tests in order to identify assets, vulnerabilities, threats, and impacts that can be used to prioritize and implement necessary mitigating security features. Landis+Gyr has maintained ongoing participation with existing Smart Grid security bodies, including the NIST Cyber Security Working Group (CSWG), the AMI-SEC task force within the UCAIug, and the ZigBee Alliance.

NERC CIP

The applicability of the NERC CIP standards as they relate to AMI is still being debated. However, it is commonly believed that compliance with these standards may become a future requirement. Landis+Gyr has taken a proactive approach by retaining Lockheed Martin to perform NERC CIP assessments of the Gridstream AMI system.

The assessment covered all CIP standards, including the following:

- NERC CIP-002 – Critical Cyber Security Asset Identification
- NERC CIP-003 – Security Management Controls
- NERC CIP-004 – Personnel & Training
- NERC CIP-005 – Electronic Security Perimeters
- NERC CIP-006 – Physical Security of Critical Cyber Assets
- NERC CIP-007 – Systems Security Management
- NERC CIP-008 – Cyber Security – Incident Reporting and Response Planning
- NERC CIP-009 – Recovery Plans for Critical Cyber Assets

Although many of the requirements listed in the NERC CIP-002 through CIP-009 are considered policy and procedural in nature, Landis+Gyr was able to take the results of the assessment, identify the technology based requirements, and then used this information to architect a solution that allows clear integration within utilities' NERC CIP compliance program.

Systemic Security Controls

Landis+Gyr takes an end-to-end approach to security. While some security approaches focus on protecting the transportation of data messages, the Gridstream AMI system has the capability to go beyond message transportation. The Gridstream security approach offer protocols to validate the origin of a data message and prevent the spread of unauthorized or malicious code.

The Gridstream AMI system provides extensive key management capabilities, including Key Manager from RSA Laboratories and SafeNet's Hardware Security Module (HSM). The Command Center head-end system includes the interfaces needed to connect to these applications, reducing the complexity of the installation and setup process.

RSA Laboratories' security solution is a non-proprietary and scalable solution with a proven track record of securing network transactions in a variety of industries. The main components of the RSA solution include providing cryptographic functionality at the network communications devices and the AMI meters using the BSAFE crypto-library and at the head-end system using the RSA Key Manager. In this system, network devices have the capability to generate keys during the registration process. These keys are securely passed to the Command Center head-end system and stored in the key manager. Each network communications device or AMI meter generates its own key, eliminating the possibility that the key could be stolen or compromised during manufacturing.

The SafeNet Hardware Security Module (HSM) establishes a strong root of trust by providing a secure storage medium for network keys. This FIPS 140-2 validated solution ensures integrity of encryption throughout the network and provides confidence that network activities and commands are legitimately initiated within the network.

Landis+Gyr manage energy better

Report on Landis+Gyr Technology, Inc.'s Description of its Managed Services Operations System and on the Suitability of the Design and Operating Effectiveness of Its Controls for the Period May 1, 2015 to October 31, 2015

The Report on Landis+Gyr Technology Inc.'s Description of its Managed Services Operations System and on the Suitability of the Design and Operating Effectiveness of Controls is confidential. The report is intended solely for use by the management of Landis+Gyr Technology, Inc., its user entities, and the independent auditors of its user entities.

Table of Contents

I. Report of Independent Service Auditors

Report of Independent Service Auditors

To the Management of Landis+Gyr Technology, Inc.

Scope

We have examined Landis+Gyr Technology, Inc.'s description of its Managed Services Operations system for processing user entities' transactions throughout the period May 1, 2015 to October 31, 2015 (the "description") and the suitability of the design and operating effectiveness of Landis+Gyr Technology, Inc.'s controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Landis+Gyr Technology, Inc.'s 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 II, Landis+Gyr Technology, Inc. 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. Landis+Gyr Technology, Inc. is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, 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, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period May 1, 2015 to October 31, 2015.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. 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 achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in management's assertion in Section II. 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, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. 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 achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Other information provided by the service organization

The information included in Section V, "Other Information Provided by Landis+Gyr Technology, Inc.", is presented by management of Landis+Gyr Technology, Inc. to provide additional information and is not a part of Landis+Gyr Technology, Inc.'s description of its Managed Services Operations system made available to user entities during the period May 1, 2015 to October 31, 2015. Information about Landis+Gyr Technology, Inc. management's response to the exception, environmental controls, physical security notifications, network monitoring, application changes, change management, logical access, data processing, and data recording, has not been subjected to the procedures applied in the examination of the description of the Managed Services Operations system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Managed Services Operations system and accordingly, we express no opinion on it.

Opinion

In our opinion, in all material respects, based on the criteria described in Landis+Gyr Technology, Inc.'s assertion in Section II,

a. the description fairly presents the Managed Services Operations system that was designed and implemented throughout the period May 1, 2015 to October 31, 2015.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period May 1, 2015 to October 31, 2015 and user entities applied the complementary user entity controls contemplated in the design of Landis+Gyr Technology, Inc.'s controls throughout the period May 1, 2015 to October 31, 2015.

c. the controls tested, which together with the complementary user entity controls referred to in the scope section of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period May 1, 2015 to October 31, 2015.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Intended users and purpose

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Landis+Gyr Technology, Inc., user entities of Landis+Gyr Technology, Inc.'s Managed Services Operations system during some or all of the period May 1, 2015 to October 31, 2015, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties. If report recipients are not user entities that have contracted for services with Landis+Gyr Technology, Inc. for the period specified above or their independent auditors (herein referred to as a "non-specified user") and have obtained this report, or have access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against PricewaterhouseCoopers LLP as a result of such access. Further, PricewaterhouseCoopers LLP does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

PricewaterhouseCoopers LLP

Atlanta, GA
December 17, 2015

II. Landis + Gyr Technology, Inc.’s Assertion

Landis+Gyr Technology, Inc.
30000 Mill Creek
Avenue
Suite 100
Alpharetta, GA 30022

Landis + Gyr Technology, Inc.’s Assertion

We have prepared the description of Landis+Gyr Technology, Inc.'s Managed Services Operations system (the "description") for user entities of the system during some or all of the period May 1, 2015 to October 31, 2015, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

a. the description fairly presents the Managed Services Operations system made available to user entities of the system during some or all of the period May 1, 2015 to October 31, 2015 for processing their transactions. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of Landis+Gyr Technology, Inc.’s controls are suitably designed and operating effectively, along with related controls at Landis+Gyr Technology, Inc. The criteria we used in making this assertion were that the description:

i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable:

(1) the types of services provided, including, as appropriate, the classes of transactions processed.

(2) the procedures, within both automated and manual systems, by which services are provided, including as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

(3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system.

(4) how the system captures and addresses significant events and conditions, other than transactions.

(5) the process used to prepare reports or other information provided to user entities of the system.

(6) specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls contemplated in the design of the service organization's controls.

(7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control

activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

ii. does not omit or distort information relevant to the scope of the Managed Services Operations system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Managed Services Operations system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the description includes relevant details of changes to the service organization's system during the period covered by the description.

c. the controls related to the control objectives stated in the description, which together with the complementary user entity controls referred to above, if operating effectively, were suitably designed and operated effectively throughout the period May 1, 2015 to October 31, 2015 to achieve those control objectives. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

III. Description of Landis + Gyr Technology, Inc.’s Managed Services Operations System

Description of Landis+Gyr Technology Inc.’s Managed Services Operations System

Overview of Company and Services

OVERVIEW OF OPERATIONS

Landis+Gyr (L+G) has a long-standing presence in the utility industry. In the late 1970s and mid-1980s, Schlumberger Limited purchased three meter manufacturing businesses in the United States: Sangamo (electric), Neptune (water), and Sprague (gas). In the early 1990s all of these businesses were looking at automated meter reading (AMR) technologies to help bolster sales and provide market differentiation. A separate unit, data management services (DMS), was formed to look at AMR technologies that could be leveraged by the three metering businesses.

In 1998, the three meter manufacturing businesses and DMS were combined into a joint organization, Resource Management Services (RMS), to help create synergies between the businesses and leverage AMR technology for use by the entities. Alliances were formed with both Itron and Cellnet Data Systems to use their AMR technologies in Schlumberger metering products.

In January 2000, Schlumberger purchased the assets of Cellnet Data Systems, including its outsourced meter-reading contracts. The purchase of the assets was finalized in the second quarter of 2000 and Cellnet became part of Schlumberger RMS, which then operated under several names, the most recent being Real-Time Energy Management Solutions (RTEMS). With the purchase of Sema, a UK-based consulting company which was purchased in 2001, Cellnet was included within the SchlumbergerSema Energy and Utility Practices offering. In a deal announced in September 2003 and finalized in January 2004, Schlumberger Limited sold the RTEMS business, now called Cellnet, to Atos Origin.

In July 2004, Cellnet management teamed with GTCR Golder Rauner, LLC, a private equity firm, to acquire Cellnet from Atos Origin. In January 2007, Bayard Group, a global investor in energy measurement and efficiency technologies, acquired Cellnet. In September 2007, Bayard announced that Cellnet and its sister company, Hunt Technologies LLC, which Bayard had acquired in 2006 would be run as one division, Landis+Gyr Energy Management Solutions. On July 29, 2011, the entirety of Landis+Gyr world-wide was sold to Toshiba Corporation and now operates within Toshiba's Social Infrastructure Systems Company.

L+G based in Alpharetta, Georgia, provides automated metering infrastructure (AMI) and distribution automation (DA) solutions to the utility industry through a number of business model options including outsourcing, build and transfer, and technology purchase. L+G offerings fall into two general categories: Data Solutions and UtiliNet.

OFFERING OVERVIEW

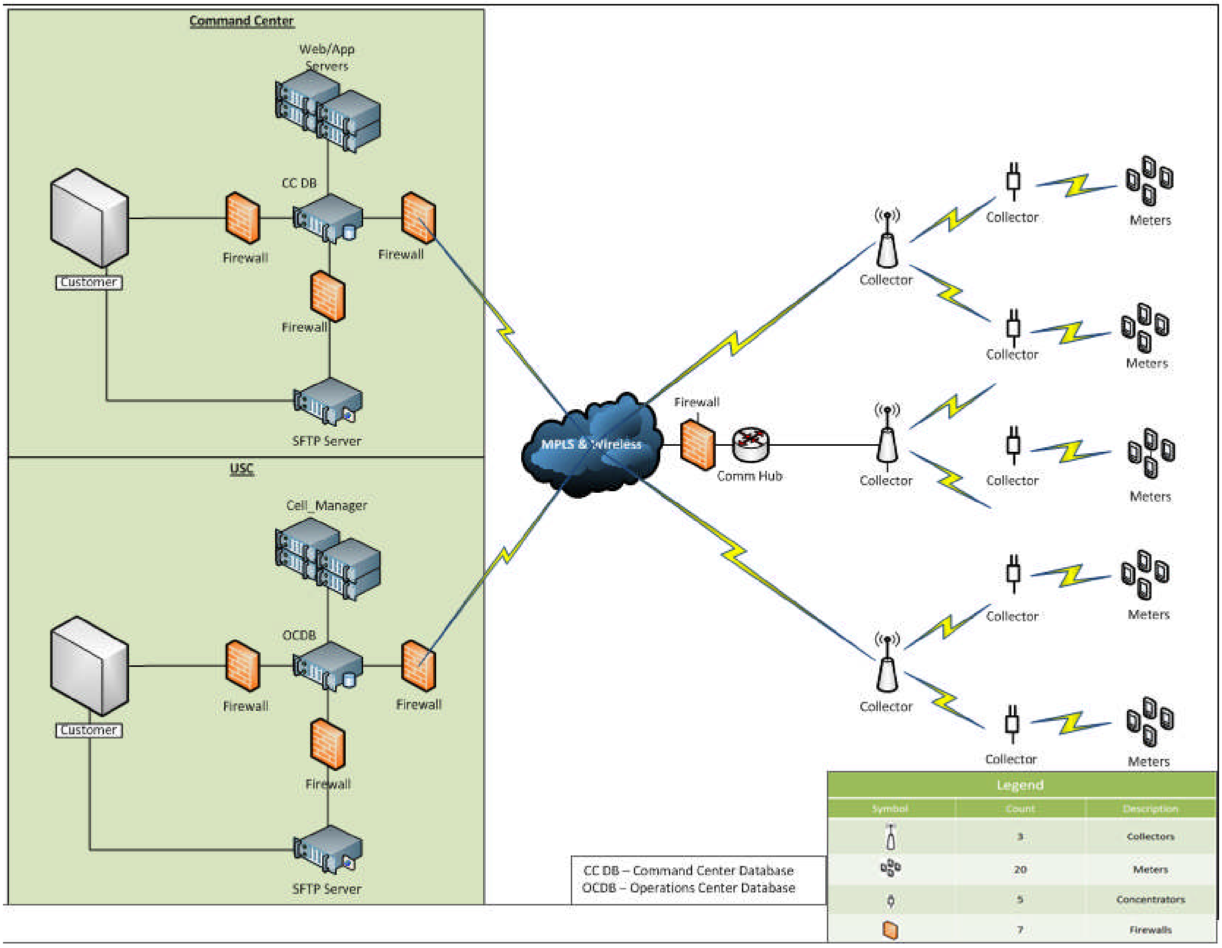
Data Solutions

L+G currently collects approximately 14 million meter reads daily for 24 major utilities in long-term Business Process Outsourcing (BPO) contracts. The Company also manages over 100 billion bytes of data daily for these customers and delivers this data to each customer for use in their enterprise applications such as Customer Information Systems (CIS), Meter Data Management (MDM) and Outage Management Systems (OMS).

Data management is critical to the process of managing and deriving the required value from the billions of bytes of data acquired in a real-time AMR network. L+G provides network monitoring and operations services as well as database management services with meter data at the operations centers located in Lenexa, Kansas and Atlanta, Georgia. AMR services are available for electric, gas, and water meters.

Meters are equipped with a radio frequency (RF) module that transmits interval based meter information. This information includes a time stamp, meter ID and meter reading value which is transmitted at set intervals. Interval time periods vary depending on customer requirements. The concentrator collects data from the meters. The concentrator communicates over the air to collector devices within a quarter mile radius. The collector connects to the cell manager (UtiliNet Solutions Center - USC - Server) or Command Center (CC) application server through one of several channels which includes leased lines, modems, and direct connections. The collector then responds back to the cell manager (USC Server) or Command Center application server through a leased line or a secure wireless router called a CTEK or Raven-X. The Cell Manager or CC application server controls the L+G RF network and maintains the connections between each device in the field. The meter reads are processed on the cell managers or CC system. For USC systems, data files per collector are created on the cell managers; for CC systems, the data is routed directly through to the application server. USC data files are then loaded into the database for each customer. Command Center data is processed into the database as each reading is received. The Operations Center database (OCDB) or Command Center database (CCDB) holds the historical meter data for each customer. Data from the network is loaded into the databases as it is received from the RF network. Once the data is loaded, separate processes run to extract or build the meter read report files for each utility customer.

Meter Reading Data Flow



Utilinet

The UtiliNet wireless network not only enables utilities to communicate with end devices in the field, it provides distributed control throughout the network. Utilities stay in touch, minute-by-minute, with critical user entity information and functionality to help utility companies achieve both operational and financial efficiencies. Utilities can read meters and collect load data at configurable intervals. This enables the utility to make distribution-planning decisions based on data collected the current day or last year.

Because UtiliNet radios are part of a network, utilities can share metering data with their customers, enabling the customer and utility to work together to make economic usage decisions. UtiliNet puts utilities in touch with user entity information wirelessly.

RELEVANT IT APPLICATION OVERVIEW

The infrastructure for the UtiliNet Solutions Center (USC) and Command Center (CC) applications are as listed below:

Application Name	Database	Operating System	Hardware
USC	Oracle 10g (OCDB) Oracle 12C	Solaris 10/11 Cell Net operating system (CNOS)	SPARC Servers and Storage Area Network (SAN)/Network-Attached Storage (NAS) storage
Command Center	Oracle 10g (CCDB) Oracle 11g (CCDB)	Solaris 10 Linux Windows Server	X86 Servers and SAN/ NAS storage

Relevant Aspects of the Control Environment, Risk Assessment Process, Monitoring and Information and Communication

CONTROL ENVIRONMENT

Organization

L+G's operational, technological and administrative activities have been organized into the following organizational structure which facilitates separation of key functions:

Data Solutions

Field offices (Program offices) are responsible for customer management, including network and endpoint maintenance, network communication, inventory control, and problem resolution for items identified by Customer Operations in Lenexa, KS. Items such as network and endpoint maintenance may also be addressed by the utility, based on utility preference and contractual requirements.

Personnel at Customer Operations are responsible for day-to-day operations and functions of the network infrastructure, process monitoring, daily data delivery and problem escalation, isolation and resolution.

Support Services

The Security Engineer and Network Engineers at Customer Operations are responsible for overseeing the logical security efforts and maintaining configuration of the network components, working with telecommunications, firewall systems, disaster recovery, and production systems.

Systems Administrators manage and maintain hardware and software that supports delivery of customer data.

The Service Desk serves as the interface between the program offices in the field, support personnel, and Customer Operations for communicating issues and requests for service. In addition, they are responsible for managing the collection of data and data processing. These personnel monitor database processes and troubleshoot errors identified by exception reporting processes.

Database Administrators design and control access to the application databases as well as manage table space and troubleshoot database issues.

Network Operations Center (NOC)

The L+G Service Desk team is responsible for monitoring systems and services 24 hours per day, seven days per week (24 x 7) and monitoring system performance and availability. It is the responsibility of the Service Desk team to initiate any internal communications to other departments within Customer Operations and to field support units regarding any business/service interruption. The Service Desk team also has the responsibility of opening cases and ensuring that qualifying issues are escalated to the appropriate group as necessary.

Product Management

Product Management is responsible for facilitating the development and revision of long-term strategy for product capability and functionality. They are also responsible for developing business requirements and functional specifications for enhancements and new products. Product Management focuses on developing the strategy for L+G products and service offerings and aligning development with market demand. Product Management is also responsible for promoting the product and service lines to new clients and for promoting L+G and corporate advertising campaigns.

Development

In general, the Development organization is responsible for the design of front office information technology systems, as well as endpoint and network equipment development. To achieve these tasks, the Development organization is divided into the following departments: Systems, Hardware, Software, and Quality.

Personnel Policies and Procedures

L+G has procedures in place for hiring, training, evaluating, promoting, and compensating employees as well as providing employees the resources necessary to perform their assigned responsibilities. The L+G Human Resources (HR) department reviews all applicants. Hiring procedures require that the proper educational levels have been attained along with required job related certifications, and industry experience, if applicable. If qualified, interviews with the candidate are conducted with various levels of management and staff. Prior to hiring, candidates undergo background investigations, consisting of prior employer reference checks, credit check, criminal record analysis, and educational reference checks. Discrepancies noted in background investigations are documented and investigated by the HR department.

New employees are required to read L+G's corporate policies and procedures and sign the acknowledgement form stating that they have read and understand the policies and procedures.

Written position descriptions for employees are maintained on file in HR. The descriptions are reviewed and revised as necessary by department managers and HR.

Employee performance reviews, promotion and compensation adjustments are performed annually. In Customer Operations, each employee is provided training specific to their job function by the hiring manager.

L+G has a written policy in place which addresses voluntary and involuntary employee terminations. Procedures are in place to collect company materials, deactivate card keys, and revoke physical and logical security access.

RISK ASSESSMENT PROCESS

L+G management has a risk assessment process in place to identify where key risks may exist to the corporation and to develop action plans to mitigate those risks. Vice President level personnel provide the Chief Executive Officer (CEO) with reports regarding their team's status and plans to address those identified risks. L+G proactively addresses potential risks on a continuous basis and implements appropriate action plans. Risk assessments are based on reliable and timely information obtained from knowledgeable internal and external sources. The CEO communicates risks and overall company status to the Board of Directors during the quarterly meetings.

Further, customer and project related statistics are available to executive management in "real time" and include information such as

- overall health;
- project information;
- upcoming milestones;
- risks and issues;
- customer satisfaction;
- schedule; and
- quality.

MONITORING

L+G has implemented a variety of activities and exception reports that measure the effectiveness of various processes involved in providing services to utility customers. Examples include reports of transaction volumes, system uptime and availability and capacity management as well as processing logs. In addition, a 24 x 7 monitoring center is in operation to track processing and transmissions. Exceptions to normal or scheduled processing due to hardware, software or procedural problems are logged, reported, and resolved. Appropriate levels of management review these reports daily, and action is taken as necessary. Procedures and tools to assist in monitoring daily activities are purchased and/or developed as needed to accommodate changes to the systems environment.

L+G establishes contracts with each customer that outlines the reporting and delivery requirements for meter readings. The contracts also establish timing of delivery and penalties incurred by L+G for failing to meet the contractually defined delivery schedule.

Statistics from the company are compiled monthly and a key performance indicator (KPI) report is created. This report is reviewed by operations management on a monthly basis, which entails follow up and resolution where KPI thresholds were not met, and focuses on performance indicators, such as:

- incident/problem reporting;
- service level agreement (SLA) performance;
- system availability and performance;
- file delivery performance - Current month and annual performance trend;
- operational level agreement (OLA) reporting; and
- call volume reporting.

Monitoring staff at the Customer Operations Center track delivery schedules and alert appropriate personnel when issues arise. L+G also has a Quality, Environmental, Health and Safety (QEHS) department who performs internal operational audits.

INFORMATION AND COMMUNICATION

L+G has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated as necessary to reflect current best practices. Updates are performed based upon changes and improvements that occur, and are subject to approval by management. Departmental managers monitor adherence to company policies and procedures as part of daily activities.

L+G personnel hold departmental status meetings, along with strategic planning meetings, to identify and address software development issues, client problems, and project management concerns. In addition, the management staff participates in monthly status meetings.

For each product, there is a selected product manager who is the focal point for communication regarding the product's direction. Additionally, there are personnel that have been designated to interface with the client if processing or systems development issues impact client organizations. Electronic messaging has been incorporated into many of L+G's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with L+G employees.

Overview of Landis+Gyr's Managed Services Operations System

The description that follows outlines the Managed Services Operations System processes and controls that are performed by Landis+Gyr Technology, Inc. for its customers. This should be read in conjunction with the detailed control objectives and control activities described in Section IV that are intended to be incorporated herein by reference.

Incident Management

Control Objective #1: ***Controls provide reasonable assurance that application, database, and system processing problems and errors are recorded, analyzed, and resolved in a timely manner.***

L+G utilizes the Microsoft Customer Relation Manager (CRM) tool to track production issues. L+G has documented a formal incident management process for issue handling and resolution procedures, which is stored on L+G's intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager, as documented in the Document Control Procedure.

Standard operating procedure documents also list escalation paths for different issues that are of high priority or those that cannot be resolved in a timely manner.

Monitoring of devices, applications, databases and systems processing is performed via an automated monitoring system and scripts, which send email notifications to the Customer Operations Center staff and create a CRM ticket, as applicable, when a potential issue has been detected. In the event an error or a malfunction occurs in the field, an L+G employee can open a service request ticket. Incidents may be initiated by a customer, L+G personnel, or via automated monitoring alerts which are sent to Customer Operations Center staff and documented within the shift brief logs. A Customer Operations Center staff member creates a CRM ticket to record the details of the incident identified, which is then escalated and resolved in a timely manner, following standard operating procedure documentation. The Customer Operations Center monitors the tickets until resolution. Since service request tickets are time-stamped, the Customer Operations Center can monitor updates real-time and relay estimated resolution time frames to the customer. If the transmission of data to the customer is delayed, the Customer Operations Center notifies the customer or the appropriate customer facing entity and provides an estimated time to correct the issue.

Trouble tickets are assigned to one of four severity levels: low, medium, high, or critical. The descriptions of the tickets and response times are as follows:

Level	Description
Low	Investigate when possible. Respond to the submitter as time allows. These tickets will be reviewed on a regular basis. There is no automatic escalation.
Medium	Respond to the submitter by the next business day. There is no automatic escalation.
High	Immediate notification to assignee; response within 15 minutes. Escalation within 45 minutes if no progress made.
Critical	Immediate notification to assignee; immediate response. Escalation within 30 minutes if no progress made.

High or critical incidents identified by the Customer Operations Center, special instructions, on call information and other information pertinent to providing services and support to L+G customers are logged into a "shift brief" log. This list is kept up-to-date with relevant information updates for the next shift, such as new high impact issues, updates to high impact issues, and resolution of these incidents.

Statistics from the company are compiled monthly and a key performance indicator (KPI) report is created. This report is reviewed by operations management on a monthly basis, which entails follow up and resolution where KPI thresholds were not met, and focuses on performance indicators, such as:

- incident/problem reporting;
- service level agreement (SLA) performance;
- system availability and performance;
- file delivery performance - Current month and annual performance trend;
- operational level agreement (OLA) reporting; and
- call volume reporting.

Application Changes

Control Objective #2: ***Controls provide reasonable assurance that application changes to the USC or Command Center applications are authorized, tested, approved, documented and properly implemented.***

L+G has documented formal policies and procedures to manage and control software development, including both new products and releases for existing products, which are stored on L+G’s intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager, as documented in the Document Control Procedure. Development processes and procedures address the USC or Command Center applications, which are L+G's proprietary applications used to serve customers. Development requests can originate from multiple sources, the most typical of which are outlined below:

- Requests for enhancements or fixes may come from a support staff member who generates a service ticket. Requests are either created for defects, or enhancements to the USC or Command Center applications.
- Requests from L+G personnel, who serve as the user organization interface, are generated in the CRM incident management system on behalf of the user organization. In some cases these may be assigned to the Product Management team for further review and approval prior to becoming an official request.
- Requests for enhancements may come from the Product Management team based upon market analysis.

Minor changes are typically grouped together in the form of a patch for implementation.
Major modifications are classified as a version change for the application.

Application changes are documented, prioritized, reviewed and approved at the weekly Software Change Control Board (SCCB) meeting prior to development as documented within the Team Foundation Server (TFS) ticket. Urgent or emergency changes follow the standard software development process; however, SCCB approval may be received via email prior to the SCCB meeting. Once approved, a TFS ticket is routed for development for both standard and emergency changes.

Once it is determined by the SCCB that a project or change should be implemented, the L+G development team begins working on the item in a segregated development environment. The development team utilizes version control tools to manage access and modifications to application code.

Requirements are documented in the TFS system, which is the source code management tool used for version control for USC (OCDB) and Command Center software code. The version control tools also allow developers to revert to prior versions of code if necessary. Each developer maintains a username, password and access group membership in order to gain access to the system. Developers are required to "check-out" modules of code to make changes in development. A code module that is being updated in the version control tool can only be accessed by one individual. Each time a change is made to a code module, the version control tool log is updated to indicate the time and username of the individual who made the change. Management has the ability to produce reports from the version control tools that outline modules of code checked-out in a state of change and list the individual who accessed the code.

USC (CNOS) software code is maintained in Revision Control System (RCS); access to and permissions for what actions a developer can perform in TFS and RCS are maintained within the individual tools by the tool's administrator.

Initial functional requirements are provided in the form of user stories in TFS. The development group breaks each user story down into a list of tasks, each with a task description that details the modification to the code. The group also creates functional specifications that detail the modifications to the code. Upon successful completion of development, the code is then transitioned to the Software Quality Assurance (SQA) group from the official source control system for independent validation. The functional specifications are referenced in the release notes for use by SQA. The L+G SQA team implements changes in a dedicated Customer Operations test and evaluation environment.

The test environment contains copies of live production data which is used to increase the assurance that the change will operate properly in production. The testing group follows a test plan, which it develops, and creates a test report to provide details and testing results. The SQA group compares the changes in the code to the identified requirements in order to increase the assurance that functionality matches what is expected. Testing approval by the SQA team is required before an application change can be implemented into production.

Additionally, when possible, a single customer site is selected for initial implementation prior to implementation at other customer locations. If the change is determined to be stable after operation in the test environment, SQA testing and initial implementation, the customers that will be affected by the change are notified by L+G of an implementation date and time.

After a change has passed through testing without further modifications required, the compiled version of code that was tested is released by Release Management to Customer Operations through established software release procedures for elevation to production. Approval to migrate application changes to the production environment is obtained from the Change Advisory Board (CAB), consisting of management and supervisory and technical personnel from each of the operations areas including Systems, Database, NOC, Program Offices and Network Administration and is documented in the Request for Change (RFC) ticket. A CAB meeting is held twice a week to discuss, approve and schedule changes ready for implementation.

Access to migrate changes to the production environment is renewed on an annual basis. To renew access, a User Request Form (URF) must be completed for each employee that requires access and the renewal of access is approved by the employee's manager and system owner. Failure to complete a renewal URF by the specified time will result in revocation of access privileges.

Once the change has been noted as approved by the CAB, the change is implemented into the production environment on the specified date by appropriate individuals (i.e., Production Support, Database Administrators, and System Administrators, etc.). Individuals responsible for developing changes do not have access to migrate changes to the production environment. The individual responsible for the change, or designee, performs a post implementation validation and upon successful validation, requests the RFC to be "Closed," which signifies successful implementation of the change. The RFC is reviewed and closed by the Change Manager. Successful implementations will be closed. If the installation was unsuccessful, or the installation notes raise a concern, the issue will be discussed during the next CAB meeting and a determination made as to the proper next course of action.

Production Change Management

Control Objective #3: *Controls provide reasonable assurance that changes to the production operating environment are authorized, tested, approved, documented, and properly implemented.*

For the purpose of this control objective, the production environment consists of the devices, software, hardware, firmware, settings, and ancillary changes within the NOC affecting customer deliverables. L+G has documented formal policies and procedures to manage and control production changes, which are stored on L+G's intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager, as documented in the Document Control Procedure.

Standard Changes

L+G uses a dedicated change management system specifically for change management tracking and approval in the production environment. L+G utilizes a standard change management form within the change management system for each change that is initiated. The form outlines, at a high level, the purpose of the change, the level of risk, any costs, potential service interruption, expected results, and a contingency/remediation plan.

A Request for Change (RFC) ticket is completed in the change management system by the individual requesting the change, to record the details of the proposed changes. All changes are subject to the appropriate levels of testing, which are based on the nature of the change, prior to implementation, and evidence of testing is documented and retained in the RFC. Changes of significant file size are sent to Customer Operations via file transfer and contain a zipped package of the changes and detailed instructions on installation. The installation instructions are a duplicate of the steps followed by the testing group to install the change in the testing environment. Smaller changes, such as patches, are also sent via file transfer to Customer Operations Center personnel.

After a change has passed through testing without further modifications required, the compiled version of code that was tested is released by Release Management to Customer Operations through established software release procedures. Approval to migrate application changes to the production environment is obtained from the Change Advisory Board (CAB) and is documented in the RFC ticket. The CAB includes members of management, supervisory and technical personnel from each of the operations areas including Systems, Database, NOC, Program Offices and Network Administration. A CAB meeting is held twice a week to discuss, approve and schedule changes ready for implementation.

The change management system is structured such that a single RFC can be created and duplicated when the change affects multiple customer sites. As changes may apply to multiple sites, this method is used to generate site specific RFC's as appropriate and ensures documentation associated with the change is the same for each site. If the change affects multiple sites, the sites are scheduled for implementation individually, or in certain situations may be scheduled to occur concurrently, such as during an established maintenance window. Typically changes do not cause a delay or outage in providing services to customers as implementations occur during a scheduled maintenance window, or outside of normal business hours when possible.

Operating System (OS) level, database (including direct data changes), and/or third party software patch updates follow the standard change management process and are documented in an RFC and appropriate approval from the CAB is obtained prior to migrating a change to the production environment. Detailed functional testing procedures are included with step-by-step installation and remediation procedures that must be followed for patches. Testing is performed in the testing phase and issues are corrected before implementation in the production environment. Changes implemented to the OS and/or hardware are performed by the System Administration team. OS patches are identified from several sources including security alerts, vendor email alerts, application requirements, and vendor recommendations. L+G performs in-house server maintenance. If a patch, such as an emergency security patch, must be implemented prior to the next change management meeting, it is deployed after testing is completed and the ticket is processed through L+G's emergency approval process (see below).

Once the change has been noted as approved by the CAB, the change is implemented into the production environment on the specified date by appropriate individuals (i.e., Production Support, Database Administrators, Engineers, Service Desk Specialists, and System Administrators, etc.). Individuals responsible for developing changes do not have access to migrate changes to the production environment. The individual responsible for the change, or designee, performs a post implementation validation, as applicable, and upon successful validation, requests the RFC to be "Closed". Closing the RFC signifies successful implementation of the change.

L+G receives e-mail alerts from vendors notifying L+G of upcoming patches. L+G performs patch implementations to production devices as required.

Pre-authorized Changes

L+G has implemented a process for pre-authorizing certain routine maintenance tasks. Pre-authorized changes are a controlled subset of common change types and are considered to be routine maintenance tasks that require pre-authorized CAB approval. These changes still receive approval prior to implementation, however, are not required to be discussed during the CAB meetings as they are pre-authorized. In order for a change to be considered as pre-authorized, the change must not be expected to cause any "downtime" to the system, or impact system functionality, user interaction with the system, or other required elements of system availability or operation and must be transparent to the end users of the system.

Change types submitted for inclusion in the pre-authorized change list require an initial review and approval by the CAB, or a subset of CAB members as applicable.

Pre-authorized changes must be reviewed and approved by the Change Manager prior to implementation in the production environment. The Change Manager may, at his/her discretion, approve an RFC of this nature without formal CAB review, or may elect to bring the request to the CAB for consideration and approval.

L+G maintains the list of pre-authorized changes on L+G's intranet.

Emergency and Out-of-Cycle Changes

Emergency and Out-of-Cycle change requests are documented in the same manner as standard changes with regards to the requirements for a change request ticket. The main differences in process are as follows:

During Normal Business Hours and After Hours Emergency Changes

Emergency or out of cycle changes are changes that cannot wait until the next CAB meeting for review. Emergency changes are typically "break/fix" in nature, and/or are causing a significant impact on a customer's business. Out-of-Cycle changes, although not of an emergency nature, typically relate to unscheduled outages or incidents where the change cannot wait for CAB approval.

In the event all members of the emergency approvers group are not available to approve a change request, approval may be obtained from the "available" members of the group based on majority. Availability status may be communicated from any member of the management team based on their knowledge of the availability and schedules of other members of the management staff. The Director of Customer Operations reserves the right to accept or reject an emergency or out-of-cycle change request without majority approval.

As L+G customer operations is a 24 x 7 operation, after hours "break/fix" emergency work may be approved and implemented at the discretion of the senior manager/supervisor on duty. Change management tickets must be created, and the CAB chair informed of the incident. Emergency and out of cycle changes follow the standard change management process and are documented in an RFC. Break/Fix scenarios include issues that are currently negatively impacting a customers or L+G's business, or with reasonable certainty, will have such an impact prior to the next business day. Issues that can wait until the next business day for approval are not considered to be of a break/fix nature, and must be approved through the standard approval process prior to implementation.

Emergency and out-of -cycle changes which occur during normal business hours must be approved by a quorum (majority) of the "emergency approvers group", consisting of designated members of the management staff, before a change can be migrated to the production environment. Emergency and out-of-cycle changes follow the standard change management process and are documented in an RFC.

Physical Access

Control Objective #4: *Controls provide reasonable assurance that physical access to computer equipment and storage media is restricted to properly authorized individuals.*

L+G has documented formal policies and procedures to control badge access management, which is stored on L+G's intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager, as documented in the Document Control Procedure.

L+G Facilities

L+G computer equipment and storage media is maintained in the Customer Operations Center and data center in Lenexa, Kansas. Access to the Customer Operations Center and data center is controlled using electronic card readers.

Electronic card access is required for entry into the main facility. Physical access to visitor badges is controlled and visitor badges are secured when not in use. All visitors to the Lenexa L+G facility, including visiting L+G employees, are required to obtain and use a visitor's badge in order to access the building via the card reader system. Visitors gain entry to the facility through a locked reception area that is monitored 24 x 7 by L+G Customer Operations Center staff. Upon entering, visitors are asked to sign in on a visitor's log and are assigned a visitor's badge by the appropriate L+G personnel. Badge assignment is tracked via an electronic system which logs the individual's name, reason for access, badge number assigned, level of access, and due date for return of the badge at the conclusion of the visit. Visitor badges are electronic badges and provide general access to the building but not to interior zones of the building. L+G employees who are visiting the facility from another location or contractors may be issued temporary electronic visitor badges that provide general access only. This badge does not allow entry into the secured access areas such as the data center, unless specifically defined within the system.

A secondary facility entrance is located at the rear of the building and also requires an electronic access card to open. Card access is only available through the rear door during normal business hours. The door is configured to be locked and does not allow card access outside normal business hours. Exterior entrances to the L+G facility and interior doors that provide access to the data center are electronically controlled and monitored with a closed circuit camera system. The camera system is automatically activated by motion in front of the camera. In addition, the camera system provides a real-time display in the NOC. The loading dock, also monitored by the security camera at the rear of the building, requires unlocking through the interior of the building. After-hours entry requires card access specifically approved for timeframes outside of normal business hours. The manager determines who should be granted access outside of normal business hours.

Lenexa, Kansas Data Center

L+G maintains storage media in the controlled data center environment. L+G visitors to the data center must be escorted by a Customer Operations L+G employee while they are within the data center. The data center room utilizes the same electronic card reader system for entry. Only L+G personnel with a business need are granted data center access privileges through the electronic access card system. The Manager of Infrastructure Engineering, or designee, determines if an individual should have data center access.

Card access and authorization is administered through the Identicard application and is used to control access to specified areas. Card access and authorization is administered and managed by the Facilities Coordinator. Access to the L+G Customer Operations Center facilities (including access to the data center) is requested through an infrastructure form for new hires and emails for existing employees and must be approved by the employee's hiring manager or supervisor. Employees are granted access either to the general office space or to the general office space and the data center. Hours of the day in which a card provides access can also be limited.

When an employee is terminated or leaves voluntarily, and an infrastructure form for termination is submitted for processing to ensure all physical access is revoked by obtaining the physical badge (immediate revocation) followed by system deactivation of the badge account within 24-48 hours of the termination notification.

The Manager of Infrastructure Engineering, or designee, can request reports from the Facilities Coordinator listing employees based on access rights, violations, or access in a particular timeframe. The security application logs the use of access cards and identifies the location accessed and time of use. When an unauthorized badge is used to attempt entry to a secure area, this action is also logged by the application. Physical access to the L+G Customer Operations Center, including the data center, is reviewed on a monthly basis by the Manager of Infrastructure Engineering, or designee, to ensure the appropriateness of users accessing, or attempting to access the facilities.

Logical Access

Control Objective #5: *Controls provide reasonable assurance that logical access to systems and applications is restricted to authorized personnel.*

General Information

The Manager of Infrastructure Engineering, or designee is responsible for overseeing logical security efforts and security monitoring functions for production environments and directs the Systems Administration, Database Administration and Network Engineering teams to maintain secure configurations of network components and production servers.

L+G has documented formal policies and procedures that outline adding and removing user access to the systems, which are stored on L+G's intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager and Security Engineer, as documented in the Document Control Procedure.

L+G Human Resources require new employees to sign a Confidentiality and Conflict of Interest document and the L+G Business Ethics Policy.

Access Requests

User access to the production servers and databases, including administrative access, for employees, or modifications to current access permissions is obtained through the User Request Form (URF) procedure and access is commensurate with user's job functions. URF's must pass through two approval stages in order to be processed. In order to gain logical access to L+G production systems, the URF form must be approved by the requester's manager, or designee, and is then submitted to the designated Systems Administrator (SA) Supervisor or Database Administrator (DBA) Supervisor for final approval. During the final approval stage each URF is thoroughly reviewed and approved or rejected based upon multiple criteria, including, but not limited to, account type requested, known customer specific or L+G security requirements, job function, technical expertise, appropriateness of the privileges requested and accuracy of information provided in the URF form.

Access to the production servers and databases, including administrative access, is renewed on an annual basis. To renew access, a URF must be completed for each employee that requires access and the renewal of access is approved by the employee's manager, or designee, and system owner. Failure to complete a renewal URF by the specified time will result in revocation of access privileges.

Access Termination

A standard procedure exists for the revocation of access, including administrative access, to IT resources when associates are terminated. This includes notification by HR to the Customer Operations Manager and Supervisor using a standard infrastructure form and the removal of network and virtual private network (VPN) access. Once termination notifications are received, the system administrators and or database administrators revoke or delete access to the appropriate systems.

Network and System Access

The production local area network (LAN) at L+G is housed in the Customer Operations Data Center and is isolated from all other networks through the use of firewall devices. Access is through a firewall and access methods include: common carrier network, virtual private network, Internet, or direct local area network connection. Logical access to production networks is implicitly denied by the firewalls. Required access is explicitly permitted by rules in the firewalls.

Managed services customers have dedicated subnets within the production network. The router and/or firewall access lists only allow connections from a customer to its specific production subnet. The L+G switch that creates the virtual LAN contains an ACL (Access Control Listing) that prohibits communication between managed services customer subnets.

L+G employees access the production network via the corporate network. Access to the corporate network is either via the corporate office LAN or via remote access VPN. The VPN uses dual-factor authentication and requires a user name, password and security token to gain access. Once on the corporate network, users must then connect to and authenticate through the production firewall in order to access the production network. The production firewall authenticates users against an L+G LDAP server. The password settings within the LDAP environment are reviewed on an annual basis by the System Administration team to ensure consistency with company policy.

In addition to the above protection each UNIX server utilizes a host/allow file to restrict access to specific address ranges. Super user access to UNIX (SUDO) is renewed on an annual basis. To renew access, a URF must be completed for each employee that requires access and the renewal of access is approved by the employee's manager, or designee, and system owner. Failure to complete a renewal URF by the specified time will result in revocation of access privileges.

Windows production servers utilize Active Directory for authentication. The password settings within the Active Directory environment are reviewed on an annual basis by the System Administration team to ensure consistency with company policy.

Database Settings

The L+G databases are maintained by the Database Administration team. Administrative access to the databases is restricted to the database administrators. Other authorized support personnel may be provided database privileges based on their roles, responsibility and their position. The password settings within the Oracle database environment are reviewed on an annual basis by the Database Administration team to ensure consistency with company policy.

Data Backup

Control Objective #6: *Controls provide reasonable assurance that application, operating systems, files and data are backed up on a scheduled basis, rotated to an offsite location and backup recovery tests are performed periodically.*

USC Systems and Applications

Database backups are performed daily. Oracle Recovery Manager (RMAN) processes run a backup to storage area network (SAN) / network-attached storage (NAS) disk. Data stored on both the SAN and NAS is protected from loss or being written over and has multiple spare drives available. These backups are copied to tape at least once per week and stored offsite, with the latest backup kept onsite. Symantec NetBackup software is used to manage the backup process and a backup schedule has been set for each of the servers on which data is stored. A complete RMAN backup of the database to tape occurs daily and a backup schedule has been set for each of the servers. The system is configured to automatically send an email notification to the Database Administrators email group in the event of a failed backup. This process applies to Oracle databases for both the USC and Command Center systems.

L+G has contracted with a third party vendor to provide off-site storage. Backup tapes are sent offsite every 30 to 60 days, depending on the availability and capacity of the tapes, and returned onsite as they expire. For each set of tapes that is sent offsite, L+G prepares an Offsite Inventory/ Rotation Schedule document that lists the tape reference numbers (bar code) and the return date for the tapes. In the event that tapes need to be retrieved from offsite storage, the vendor has an authorization list with the names of L+G employees authorized to request tapes.

Backup recovery tests are performed quarterly and restoration using backup tapes is tested on an ad hoc basis. Information is restored to a centralized location where it can be accessed by test systems.

L+G also incrementally backs up to NAS/NFS storage on a daily basis to local tape. A full backup of the fileserver is executed by the Netbackup system and occurs on a weekly basis.

On a weekly basis, Sun Explorer is executed on critical UNIX servers. This is a data collection process which archives operating system files. These backups are stored on a NAS volume retaining no less than four weeks of backups.

Command Center Systems and Applications

Backups for Command Center include the operating system, Command Center application and Oracle database. Backups of both virtual server configuration and databases are performed daily to support recovery in the event of a serious issue. Virtual servers are backed up using Veeam Backup & Replication software.

Data Processing

Control Objective #7: *Controls provide reasonable assurance that data processing is appropriately authorized and scheduled, and deviations from scheduled processing are identified and resolved.*

Day-to-day operation of the data center and data processing is the responsibility of Customer Operations Center personnel. The L+G Customer Operations Center is staffed and monitored 24 x 7. Responsibilities of this team include monitoring consoles, batch processing, and preparation of deliverables to ensure that processing is performed effectively and problems are identified and corrected in a timely manner.

A schedule is provided by each applicable customer for the upcoming year's holidays and billing dates. This data for the subsequent year is entered into the system at the end of the current year and tracked by L+G in a CRM ticket. Schedule modifications and validation are tracked in L+G's ticketing system and follow the standard incident management process.

The Customer Operations Center is responsible for monitoring scheduled jobs and ensuring the successful completion of jobs scheduled, as well as identifying any production job failures via the monitoring tool. In the event of high priority or critical errors in data processing, the Customer Operations Center notifies the appropriate personnel required to resolve the issue and a CRM ticket is created to track the incident to resolution.

System logs are produced during each step of data processing to allow L+G support staff to identify the source of processing issues. Logs also aid in identifying potential causes of issues. Analysts are generally able to identify the problems easily from the logs but in some cases analysts may have to perform additional testing to identify the root cause of an issue or anomaly.

Statistics from the company are compiled monthly and a key performance indicator (KPI) report is created. This report is reviewed by operations management on a monthly basis, which entails follow up and resolution where KPI thresholds were not met, and focuses on performance indicators, such as:

- incident/problem reporting;
- service level agreement (SLA) performance;
- system availability and performance;
- file delivery performance - Current month and annual performance trend;
- operational level agreement (OLA) reporting; and
- call volume reporting.

Cron is used as the process scheduler, and additions, modifications or deletions to scheduled processes are tracked within RFC tickets via L+G's change management process. Access to modify the process scheduler is restricted to authorized personnel with SUDO permissions, controlled through the use of the "sudoers" files on each customers’ server. An annual access renewal and review is performed to ensure access remains commensurate with job responsibilities.

Data Transmission

Control Objective #8: ***Controls provide reasonable assurance that data transmissions between the Company and external parties are secure, segregated and received from authorized sources.***

L+G customers transmit and receive data from Customer Operations on a daily basis. The majority of L+G's customers utilize private networks. These networks are only accessible by the customer and L+G. The network lines between the customers and L+G are redundant to prevent delays or transmission loss in the event of a network issue. There are effectively two isolated lines from L+G to each customer utilizing this architecture for data transfers. Customers access virtual LANs to retrieve data files from L+G. Customers, including those entities that share data services on a single database and access the same virtual LAN, access data in three primary ways on their virtual LAN: through structured query language (SQL) queries to the Oracle database, secure file transfer protocol (SFTP) to retrieve files posted by L+G, or via the use of a secure (https) web browser interface. Each customer, except for those entities that share data services on a single database, has a secure, designated switch access list that manages the virtual LAN, blocks traffic between each of the customer's virtual LANs and prevents customers from accessing each other's data and the devices used to store and process data. For customers that share data services on a single database and access the same virtual LAN, restrictions are maintained within the database to prevent access to another customer's data.

The access listings on the switches are based on approved IP addresses and other traffic attempting to access the networks is blocked. Firewalls are also utilized to prevent unauthorized network access and maintain similar access lists as the network switches.

Customers may also perform data exchanges through standard file transfer protocol (FTP) transmission protocol. Each customer is assigned a unique IP address and designated secure FTP sites. A unique username and password are setup for each customer submitting transactions via FTP to ensure that data submitted is secure and segregated. L+G strongly recommends the use of secure FTP (SFTP) by its customers that utilize FTP and provides assistance in migrating to SFTP. However, the customer ultimately determines which protocol is used. Over 95% of L+G's customers using FTP transmissions utilize SFTP, which provides encryption functionality for the data being transferred. Customers are limited to accessing only the directory structure and virtual OS used to transfer their data files. Additionally, customers are blocked from accessing other segments of the L+G network from the SFTP server.

Data Recording

Control Objective #9: *Controls provide reasonable assurance that meter data is uniquely identifiable, recorded and processed completely and accurately.*

Collectors in the field transmit meter readings to the USC or Command Center systems at L+G Customer Operations. Once the information is delivered to the USC database (OCDB) and Command Center database (CCDB), the meter readings are placed in a historical storage table in the production database. The meter records contained in the database detail devices which are expected to be in service. Meter readings are associated to customers via a database table. Each meter is assigned a unique meter ID and a utility identifier/meter serial number, which is utilized to prevent duplicates within the table. The database table which maintains records of meters in service is structured to allow only unique meter information. This increases the assurance that meter readings from the field correspond to the correct information for creating the report files provided to customers.

Data received and recorded from the field utilizes a standardized and uniform format. Field data that is collected from the network is loaded directly into the database without transformation to maintain data integrity and increase the assurance of accurate representation of the meter readings. Firewalls also protect the L+G internal network from unauthorized access when retrieving field data.

L+G may receive data files from customers for use in "syncing" head-end databases. These files provide updates for the head-end database regarding customer meter changes. Customers provide files that indicate added meters, removed meters, or meters that have changed accounts for billing purposes. The meter updates are incorporated into the table that maintains the unique meter information. These files are received from customers on a set periodic basis, as determined by the customer. Automated checks in the database ensure the record counts submitted by the customers agree to the record counts processed within the L+G database.

Cumulative readings for each meter are developed and compared to prior day readings. In the event there are missing or incorrect readings, the next valid reading will correct the cumulative reading for that meter. If a reading is lower than the previous day, the reading is automatically flagged for investigation by a local field analyst. For USC systems only, the Service Desk is alerted via L+G's automated monitoring system when the count of meter readings processed may potentially be low and the matter is investigated to determine if the meter readings are incorrect or if a meter was replaced.

Each applicable customer within the USC platform has a file size threshold which is configured in the system and used to determine successful processing and building of the data file extracts. If this threshold is not met, the file is flagged and an alarm is raised to the Service Desk by the monitoring system. Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.

Each meter reading is noted with an "A" or "system" for system based reading, or an "M" or "individual user ID" for manual reading. Manual readings are flagged as such and, if uploaded in sufficient time, serve as the reading for the billing information sent to the customer. The threshold for stale meters and manual reads is determined by the customer. When a "fresh" reading for a meter is not available, the most recent field reading captured by the database is utilized. A threshold, or read window, is established that indicates a minimum timeframe prior to the billing information due date for meters to be read manually, if current readings are not available. Meters that have exceeded the threshold for reliable readings are marked by the system for L+G field personnel to perform a manual read ('M'), and a local reading, directly from the meter, is manually obtained and uploaded into the database by the field personnel. L+G field personnel receive regular reports of meters that require manual readings. Not all sites filter "stale" readings. Some utilities may choose to disregard a read window and may require every meter with whatever read is available regardless of the age to be delivered. The utility decides what data can be used for billing purposes. Changes to customer read windows are made following the standard change management process.

In addition to file size thresholds, each applicable customer within USC has a file delivery time threshold which is configured in the system and is used to ensure delivery of the file within established parameters. If this threshold is not met, an alarm is raised to the Service Desk by the monitoring system. Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.

L+G has procedures in place to compare the reported volume of daily meter readings to the meters expected to be in service. The details of this verification are sent to the Service Desk for review. Variations are noted within the information sent to the Service Desk and are investigated. The head-end database records two dates pertaining to readings which indicate the day the reading was entered in the database and the date the reading was captured from the field. Meter reading counts are logged to confirm completeness with total meter readings expected. Customer Operations Center analysts use the existing incident management procedures to open CRM tickets, as applicable, for variances that are outside expected thresholds and cannot be explained, and to engage the appropriate resources required to resolve the incident in a timely manner. There is typically a minor difference in the number of records received from the network and the number processed for final reporting due to invalid readings from field devices that typically are the result of incomplete information or formatting issues. A significant difference in the number received from the network and the number processed by the database would warrant investigation.

The final head-end system files prepared for the customer are created and placed in a directory for retrieval by the customer. Based on customer preference, L+G includes a checksum with the reporting files which are transmitted. Customers are responsible for reviewing the checksum to validate the completeness and accuracy of the content of each reporting file transmitted. The actual size of the file created is logged by the system. The Service Desk reviews the system log and notes the typical file size for each customer. Files that vary significantly from the expected file size are investigated. Large files may be the result of a customer failing to retrieve a prior day's file and new data being appended to an existing file. These checks on the final report file are completed prior to the scheduled file delivery time for each customer.

Statistics from the company are compiled monthly and a key performance indicator (KPI) report is created. This report is reviewed by operations management on a monthly basis, which entails follow up and resolution where KPI thresholds were not met, and focuses on performance indicators, such as:

- incident/problem reporting;
- service level agreement (SLA) performance;
- system availability and performance;
- file delivery performance - Current month and annual performance trend;
- operational level agreement (OLA) reporting; and
- call volume reporting.

Data Output

Control Objective #10: *Controls provide reasonable assurance that data output is distributed in a timely manner to appropriate users.*

Files developed for customers are posted to specific directories that are utilized only for that respective customer's information. The data collected is routed to a segregated virtual LAN that is utilized for that particular customer. Access to customer directories is restricted through the use of firewalls that maintain detailed access listings which prevent unauthorized users from accessing a customer's data files. In addition, firewalls limit the types of services customers can use to retrieve their data. Services that are used by the customers are agreed upon between the customer and L+G.

Customers, including those entities that share data services on a single database, access virtual LANs to retrieve data files from L+G. Each customer has a secure, designated switch access list that manages the virtual LAN and blocks traffic between each of the customer's virtual LANs and prevents customers from accessing each other's data and the devices used to store and process the data. For customers that share data services on a single database and access the same virtual LAN, restrictions are maintained within the database to prevent access to another customer's data. Typically, customers retrieve billing files on a regular schedule for weekdays.

Billing files, or meter reading files, are transmitted to customers on a daily basis. L+G utilizes a file checker program to verify that the file for each customer is available at the designated time and is within defined file size thresholds, as defined by the customer's file schedule. In the event a file is not present when expected, automated alerts are raised to Service Desk staff, by the monitoring system, to begin investigating the incident. When issues are discovered, a CRM ticket is created, as applicable, to resolve the issue, if the issue cannot be resolved by the Service Desk staff. Customers access the directory and retrieve the processed file for use within their systems.

Statistics from the company are compiled monthly and a key performance indicator (KPI) report is created. This report is reviewed by operations management on a monthly basis, which entails follow up and resolution where KPI thresholds were not met, and focuses on performance indicators, such as:

- incident/problem reporting;
- service level agreement (SLA) performance;
- system availability and performance;
- file delivery performance - Current month and annual performance trend;
- operational level agreement (OLA) reporting; and
- call volume reporting.

Complementary User Entity Controls

L+G's controls over managed services operations are designed with the assumption that certain controls would be implemented by the customer. In certain situations, the application of such controls by user entities is necessary to achieve certain control objectives identified in this report. The complementary user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by the customers. There may be additional controls that would be appropriate to the processing of user transactions that are not identified in this report. User auditors should determine whether customers have established controls in these areas.

Control Objective #1: Incident Management

- Controls should be established to ensure field staff report and respond to device repair issues in a timely manner (applicable to customers that do not use L+G field staff).

Control Objective #2: Application Changes

- Controls should be established to ensure participation in customer acceptance and pilot testing to ensure that system functionality is in accordance with previously defined specifications.

Control Objective #4: Physical Access

- Controls should be established to ensure physical access to L+G systems from customers is monitored and maintained.
- Controls should be established to ensure field equipment is not manipulated or altered by unauthorized personnel.

Control Objective #5: Logical Access

- Controls should be established to ensure physical and logical access to L+G systems from customers is monitored and maintained.
- Controls should be established to ensure the provisioning, modification and revocation of logical access to the user entity's application instance is properly managed and maintained.

Control Objective #7: Data Processing

- Controls should be established to ensure accurate information is provided to L+G for the customers' data processing and reporting requirements in a timely manner.

Control Objective #8: Data Transmission

- Controls should be established to ensure data transmissions are complete, accurate and secure through the use of protected transmission protocol.
- Controls should be established to ensure data transmissions are complete and accurate through the use of checksums or other reconciliation total controls.
- Controls should be established to ensure that secure protocol is utilized by customers that utilize file transfer protocol.

Control Objective #9: Data Recording

- Controls should be established to ensure accurate and timely information is provided to L+G for additions, changes, and deletions to in-service meters.
- Controls should be established to ensure that a reading is received for each meter expected to be in service.
- Controls should be established to ensure meters are identified for manual reads by customer field personnel (applicable to customers that do not use L+G field staff).
- Controls should be established to ensure that secure protocol is utilized by customers that utilize file transfer protocol.
- Controls should be established to ensure meter data information provided correlates

to the customer(s) expected customer usage data such as consumption, rate types, meters expected to be in service and other data deemed applicable by the utility (applicable to customers who request and receive data for all meters, including stale meters).

Control Objective #10: Data Output

- Controls should be established to ensure data processed and delivered by L+G is acquired in a timely manner.
- Controls should be established to ensure that secure protocol is utilized by customers that utilize file transfer protocol.
- Controls should be established to ensure meter data information provided correlates to the customer(s) expected customer usage data such as consumption, rate types, meters expected to be in service and other data deemed applicable by the utility (applicable to customers who request and receive data for all meters, including stale meters).

IV. Landis+Gyr Technology, Inc.’s Control Objectives and Controls, and PricewaterhouseCoopers’ Tests of Operating Effectiveness and Results of Tests

PwC tested relevant aspects of L+G’s control environment and the controls specified on the following pages. PwC’s tests covered only those controls provided by L+G and did not cover controls which may be specific to individual customers of L+G.

Tests of the control environment, risk assessment, information and communication, and monitoring include inquiry of appropriate management, supervisory, and staff personnel, observation of L+G's activities, inspection of L+G documents and records. The results of these tests were considered in planning the nature, timing, and extent of testing of the controls designed to achieve the control objectives described on the following pages.

Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listings to assess the completeness and accuracy (reliability) of information utilized in the performance of our testing of the controls.

Incident Management

***Control Objective #1**: Controls provide reasonable assurance that application, database, and system processing problems and errors are recorded, analyzed, and resolved in a timely manner.*

#	Control Activity	Test of Operating Effectiveness	Test Results
1.1	L+G has documented a formal incident management process for issue handling and resolution procedures, which are stored on L+G's intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager, as documented the Document Control Procedure.	**Inspection** Inspected the incident management policies and procedures to determine whether they: • outline the process of issue handling and resolution procedures; • are stored on L+G's intranet; and • were reviewed by the respective process owner/manager, as documented in the Document Control Procedure.	No exceptions noted.
1.2	Monitoring of devices, applications, databases and systems processing is performed via an automated monitoring system and scripts, which send email notifications to the Customer Operations Center staff and create a CRM ticket, as applicable, when a potential issue has been detected.	**Observation** Observed the monitoring scripts to determine whether email notifications are generated to the Customer Operations Center staff and a CRM ticket is created, as applicable, when a potential issue has been detected.	No exceptions noted.
		Observation Observed the submission of a system error to determine whether an email notification to the Customer Operations Center staff was generated as a result of the unsuccessful submission.	No exceptions noted.
		Observation Observed the submission of a system error to determine whether a CRM ticket was generated as a result of the unsuccessful submission.	No exceptions noted.
1.3	Incidents may be initiated by a customer, L+G personnel, or via automated monitoring alerts. Incidents are sent to Customer Operations Center staff, and documented within the shift brief logs.	**Inspection** Inspected the shift brief logs for a sample of shifts and customers to determine whether incidents are sent to Customer Operations Center staff, and documented within the shift brief logs.	No exceptions noted.

Incident Management

***Control Objective #1**: Controls provide reasonable assurance that application, database, and system processing problems and errors are recorded, analyzed, and resolved in a timely manner.*

#	Control Activity	Test of Operating Effectiveness	Test Results
1.4	Statistics from the company are compiled monthly and a key performance indicator (KPI) report is created. This report is reviewed by operations management on a monthly basis, which entails follow up and resolution where KPI thresholds were not met, and focuses on performance indicators, such as: • incident/problem reporting; • SLA performance; • system availability and performance; • file delivery performance - Current month and annual performance trend; • OLA reporting; and • call volume reporting.	**Inspection** Inspected evidence of review of KPI reports for a sample of months to determine whether statistics from the company are compiled monthly and the report is reviewed by operations management on a monthly basis.	No exceptions noted.
		Inspection Inspected KPI reports for a sample of months to determine whether they include: • follow up and resolution where KPI thresholds were not met, and • performance indicators such as: o incident/ problem reporting, o SLA performance, o system availability and performance, o file delivery performance, o OLA reporting; and o call volume reporting.	No exceptions noted.
1.5	A Customer Operations Center staff member creates a Customer Relation Manager (CRM) ticket to record the details of the incident identified, which is then escalated and resolved in a timely manner, following standard operating procedure documentation.	**Inspection** Inspected CRM tickets for a sample of incidents to determine whether: • a Customer Operations Center staff member creates a CRM ticket to record the details of the incident identified, and • the CRM is escalated and resolved in a timely manner, following standard operating procedure documents.	No exceptions noted.

Application Changes

Control Objective #2: *Controls provide reasonable assurance that application changes to the USC or Command Center applications are authorized, tested, approved, documented and properly implemented.*

#	Control Activity	Test of Operating Effectiveness	Test Results
2.1	L+G has documented formal policies and procedures to manage and control software development, including both new products and releases for existing products, which are stored on L+G's intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager, as documented in the Document Control Procedure.	**Inspection** Inspected the software development policies and procedures to determine whether they: • outline the process to manage and control software development, including both new products and releases for existing products; • are stored on L+G's intranet; and • were reviewed by the respective process owner/manager, as documented in the Document Control Procedure.	No exceptions noted.
2.2	Application changes are documented, prioritized, reviewed and approved at the weekly Software Change Control Board (SCCB) meeting prior to development, as documented within the TFS ticket. Urgent or emergency changes follow the standard software development process; however, SCCB approval may be received via email prior to the SCCB meeting.	**Inspection** Inspected TFS tickets for a sample of application changes to determine whether changes were documented, prioritized, reviewed and approved at the weekly SCCB meeting, prior to development.	No exceptions noted.
		Inspection Inspected TFS tickets and email evidence of SCCB approval for a sample of emergency application changes to determine whether changes were documented, prioritized, reviewed and approved by the SCCB, prior to development.	No exceptions noted.
2.3	**UNIX** Access to migrate changes to the production environment is renewed on an annual basis. To renew access, a User Request Form (URF) must be completed for each employee that requires access and the renewal of	**Inspection** Inspected the annual access renewal to determine whether management initiates an annual access renewal of individuals with access to migrate changes to the production environment.	No exceptions noted.

Application Changes

Control Objective #2: *Controls provide reasonable assurance that application changes to the USC or Command Center applications are authorized, tested, approved, documented and properly implemented.*

#	Control Activity	Test of Operating Effectiveness	Test Results
	access is approved by the employee's manager and system owner. Failure to complete a renewal URF by the specified time will result in revocation of access privileges. Individuals responsible for developing changes do not have access to migrate changes to the production environment.	**Inspection** Inspected URF tickets for a sample of users with access to migrate changes to the production environment to determine whether access was renewed and approved by the employee's manager and system owner and whether access was revoked upon failure to complete a renewal URF.	No exceptions noted.
		Inspection Inspected listing of users with access to migrate changes to the production environment to determine whether individuals responsible for developing changes are restricted.	No exceptions noted.
	Oracle database Access to migrate changes to the production environment is renewed on an annual basis. To renew access, a User Request Form (URF) must be completed for each employee that requires access and the renewal of access is approved by the employee's manager and system owner. Failure to complete a renewal URF by the specified time will result in revocation of access privileges. Individuals responsible for developing changes do not have access to migrate changes to the production environment.	**Inspection** Inspected the annual access renewal to determine whether management initiates an annual access renewal of individuals with access to migrate changes to the production environment.	No exceptions noted.
		Inspection Inspected URF tickets for a sample of users with access to migrate changes to the production environment to determine whether access was renewed and approved by the employee's manager and system owner and whether access was revoked upon failure to complete a renewal URF.	No exceptions noted.
		Inspection Inspected listing of users with access to migrate changes to the production environment to determine whether individuals responsible for developing changes are restricted.	No exceptions noted.

Application Changes

Control Objective #2: *Controls provide reasonable assurance that application changes to the USC or Command Center applications are authorized, tested, approved, documented and properly implemented.*

#	Control Activity	Test of Operating Effectiveness	Test Results
2.4	The L+G Software Quality and Assurance (SQA) team implements changes in a dedicated Customer Operations test and evaluation environment. The testing group follows a test plan, which it develops, and creates a test report to provide details and testing results. Testing approval by the SQA team is required before an application change can be implemented into production.	**Inspection** Inspected test reports and test results for a sample of changes to determine whether the changes were implemented in a dedicated Customer Operations test and evaluation environment, whether testing was performed by the SQA team and whether SQA approval was obtained before a change was migrated into the production environment.	No exceptions noted.
2.5	After a change has passed through testing without further modifications required, the compiled version of code that was tested is released by Release Management to Customer Operations through established software release procedures for elevation to production. Approval to migrate application changes to the production environment is obtained from the Change Advisory Board (CAB), and is documented in the Request for Change (RFC) ticket.	**Inspection** Inspected RFC tickets for a sample of changes to determine whether tested changes were released by Release Management to Customer Operations and whether CAB approval was obtained before a change was migrated to the production environment.	No exceptions noted.
2.6	Once the change has been noted as approved by the CAB, the change is implemented into the production environment on the specified date by appropriate individuals (i.e., Production Support, Database Administrators, and System Administrators). Individuals responsible for developing changes do not have access to migrate changes to the production environment. The individual responsible for the change, or designee, performs a post implementation validation and upon successful validation, requests the RFC to be "Closed," which signifies successful implementation of the	**Inspection** Inspected a sample of RFC tickets to determine whether: • the change is implemented into production environment on the specified date by appropriate individuals (i.e., Product Support, Database Administrators, and System Administrators), and • upon successful post implementation validation of the change, the individual responsible for the change, or designee, requests the ticket to be "Closed," which signifies successful implementation.	No exceptions noted.

Application Changes			
Control Objective #2: *Controls provide reasonable assurance that application changes to the USC or Command Center applications are authorized, tested, approved, documented and properly implemented.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
	change.	**Inspection** Inspected a listing of users with access to migrate changes to production to determine whether access to migrate changes to production is restricted to authorized personnel and whether individuals responsible for developing changes do not have access to migrate changes to the production environment.	No exceptions noted.

Production Change Management

Control Objective #3: *Controls provide reasonable assurance that changes to the production operating environment are authorized, tested, approved, documented, and properly implemented.*

#	Control Activity	Test of Operating Effectiveness	Test Results
3.1	L+G has documented formal policies and procedures to manage and control production changes, which are stored on L+G's intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager, as documented in the Document Control Procedure.	**Inspection** Inspected the production change management policies and procedures to determine whether they: • outline the process to manage and control production changes; • are stored on L+G's intranet; and • were reviewed by the respective process owner/manager, as documented in the Document Control Procedure.	No exceptions noted.
3.2	A Request for Change (RFC) ticket is completed in the Change Management system by the individual requesting the change to record the details of the proposed changes. All changes are subject to the appropriate levels of testing, which are based on the nature of the change, prior to implementation and evidence of testing is documented and retained in the RFC.	**Inspection** Inspected the RFC tickets for a sample of production changes to determine whether a ticket was completed by the individual requesting the change to record the details of the proposed changes.	No exceptions noted.
		Inspection Inspected test cases and results within the RFC ticket for a sample of production changes to determine whether appropriate levels of testing were performed, based on the nature of the change, prior to implementation into the production environment.	No exceptions noted.
3.3	Emergency and out-of-cycle changes must be approved by a quorum (majority) of the "emergency approvers group", consisting of the Director of Customer Operations and designated members of the management staff, before a change can be migrated to the production environment.	**Inspection** Inspected email evidence of approval by a quorum of the "emergency approvers group" for a sample of emergency or out-of-cycle production changes to determine whether appropriate approval was obtained before a change was migrated to the production environment.	No exceptions noted.

Production Change Management			
Control Objective #3: *Controls provide reasonable assurance that changes to the production operating environment are authorized, tested, approved, documented, and properly implemented.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
3.4	After a change has passed through testing without further modifications required, the compiled version of code that was tested is released by Release Management to Customer Operations through established software release procedures for elevation. Approval to migrate application changes to the production environment is obtained from the Change Advisory Board (CAB). Pre-authorized changes are a controlled subset of common change types and are considered to be routine maintenance tasks that require pre-authorized CAB approvals.	**Inspection** Inspected the RFC tickets for a sample of changes to determine whether CAB approval was obtained before a change was migrated to the production environment, and whether all pre-authorized change types had initial approval by the CAB, as applicable.	No exceptions noted.
3.5	Operating system (O/S) level, database (including direct data changes), and/or third party software patch updates follow the standard change management process documented in an RFC, and appropriate approval from the CAB is obtained prior to migrating a change to the production environment.	**Inspection** Inspected the RFC tickets for a sample of operating system (O/S) level, database, and/or third party software patch updates to determine whether appropriate approval was obtained before a change was migrated to the production environment.	No exceptions noted.
3.6	Once the change has been noted as approved by the CAB, the change is implemented into the production environment on the specified date by appropriate individuals (i.e., Production Support, Database Administrators, Engineers, Service Desk Specialists, and System Administrators). Individuals responsible for developing changes do not have access to migrate changes to the production environment. The individual responsible for the change, or assignee, performs a post implementation validation and upon successful validation, requests the RFC to be "Closed". Closing the RFC	**Inspection** Inspected a sample of RFC tickets to determine whether: • the change is implemented into production environment on the specified date by appropriate individuals (i.e., Product Support, Database Administrators, Engineers, Service Desk Specialists, and System Administrators), and • upon successful post implementation validation of the change, the individual responsible for the change, or designee, requests the ticket to be "Closed," which signifies successful implementation.	No exceptions noted.

Production Change Management

Control Objective #3: *Controls provide reasonable assurance that changes to the production operating environment are authorized, tested, approved, documented, and properly implemented.*

#	Control Activity	Test of Operating Effectiveness	Test Results
	signifies successful implementation of the change.	**Inspection** Inspected a listing of users with access to migrate changes to production to determine whether access to migrate changes to production is restricted to authorized personnel and whether individuals responsible for developing changes do not have access to migrate changes to the production environment.	No exceptions noted.

Physical Access

Control Objective #4: *Controls provide reasonable assurance that physical access to computer equipment and storage media is restricted to properly authorized individuals.*

#	Control Activity	Test of Operating Effectiveness	Test Results
4.1	L+G has documented formal policies and procedures to control badge access management, which are stored on L+G's intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager, as documented in the Document Control Procedure.	**Inspection** Inspected the badge access management policies and procedures to determine whether they: • outline the process of badge access management; • are stored on L+G's intranet; and • were reviewed by the respective process owner/manager, as documented in the Document Control Procedure.	No exceptions noted.
4.2	L+G computer equipment and storage media is maintained in the Customer Operations Center and data center in Lenexa, Kansas. Access to the Customer Operations Center and data center is controlled using electronic card readers.	**Observation** Observed the presence of L+G's computer equipment and storage media within the Customer Operations Center and Lenexa data center.	No exceptions noted.
		Observation Observed the physical access controls around the Customer Operations Center and Lenexa data center to determine whether access to the Customer Operations Center and data center was controlled using electronic card readers.	No exceptions noted.
4.3	Exterior entrances to the L+G facility and interior doors that provide access to the data center are electronically controlled and monitored with a closed circuit camera system.	**Observation** Observed the physical access controls around the exterior entrances and interior doors to the L+G facility to determine whether access to the facility and data center are electronically controlled and monitored with a closed circuit camera system.	No exceptions noted.

Physical Access

Control Objective #4: *Controls provide reasonable assurance that physical access to computer equipment and storage media is restricted to properly authorized individuals.*

#	Control Activity	Test of Operating Effectiveness	Test Results
4.4	Access to the L+G Customer Operations Center facilities (including access to the data center) is requested through an infrastructure form for new hires and emails for existing employees and must be approved by the employee's hiring manager or supervisor.	**Inspection** Inspected infrastructure forms for a sample of access requests to determine whether access to the L+G Customer Operations Center facilities (including access to the data center) was requested through an infrastructure form and approved by the employee's hiring manager or supervisor.	No exceptions noted.
4.5	When an employee is terminated or leaves voluntarily, an infrastructure form for termination is submitted for processing to ensure all physical access is revoked by obtaining the physical badge (immediate revocation) followed by system deactivation of the badge account within 24-48 hours of the termination notification.	**Inspection** Inspected infrastructure forms for a sample of terminated employees to determine whether access to the Lenexa L+G facilities was removed by the facilities team and security badges were collected from the employee within 24 to 48 hours of termination.	No exceptions noted.
		Inspection Inspected the population of terminated employees to determine whether access to the Lenexa L+G facilities and data center was revoked.	No exceptions noted.
4.6	Physical access to the L+G Customer Operations Center, including the data center, is reviewed on a monthly basis by the Manager of Infrastructure Engineering or designee to ensure the appropriateness of users accessing, or attempting to access the facilities.	**Inspection** Inspected a sample of monthly access reviews and access logs to determine whether physical access to the L+G Customer Operations Center, including data center, is reviewed on a monthly basis by the Manager of Infrastructure Engineering or designee to ensure the appropriateness of users accessing the facilities.	Exception noted. For the total population of six monthly access reviews of the L+G Customer Operations Center, including the data center, evidence of review could not be provided for May - July 2015.

Physical Access			
Control Objective #4: *Controls provide reasonable assurance that physical access to computer equipment and storage media is restricted to properly authorized individuals.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
		Inspection Inspected listing of users with access to the L+G Customer Operations data center to determine whether individuals with access to the data center are appropriate.	No exceptions noted.

Logical Access

Control Objective #5: *Controls provide reasonable assurance that logical access to systems and applications is restricted to authorized personnel.*

#	Control Activity	Test of Operating Effectiveness	Test Results
5.1	L+G has documented formal policies and procedures that outline adding and removing user access to the systems, which are stored on L+G's intranet. Documented policies and procedures are reviewed and updated as necessary, by the respective process owner/manager and Security Engineer, as documented in the Document Control Procedure.	**Inspection** Inspected the user access policies and procedures to determine whether they: • outline the process of adding and removing user access to the systems; • are stored on L+G's intranet; and • were reviewed by the respective process owner/manager and Security Engineer, as documented in the Document Control Procedure.	No exceptions noted.
5.2	L+G Human Resources require new employees to sign a Confidentiality and Conflict of Interest document and the L+G Business Ethics Policy.	**Inspection** Inspected Confidentiality and Conflict of Interest and Business Ethics Policy acknowledgement forms for a sample of new employees to determine whether new employees signed the required forms.	No exceptions noted.
5.3	User access to the production servers and databases, including administrative access, for employees, or modifications to current access permissions is obtained through the User Request Form (URF) The URF form must be approved by the requestor's manager, or designee, and is then submitted to the designated Systems Administrator (SA) Supervisor or Database Administrator (DBA) Supervisor for final approval.	**Inspection** Inspected URF tickets for a sample of user access requests to the production servers and databases, including administrative access to determine whether access, was approved by the requestor's manager, or designee, and submitted to the designated SA Supervisor or DBA Supervisor for final approval.	No exceptions noted.
5.4	Once termination notifications are received, the system administrators and or database administrators revoke or delete access to the appropriate systems.	**Inspection** Inspected infrastructure forms for a sample of terminated employees to determine whether once the termination notifications were received, a form was created to revoke or delete access to the appropriate system.	No exceptions noted.

Logical Access			
Control Objective #5: *Controls provide reasonable assurance that logical access to systems and applications is restricted to authorized personnel.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
		Inspection Inspected current network, operating system and database access listings to determine whether system access, including administrative access, was revoked or deleted for the sample of terminated employees.	No exceptions noted.
5.5	**Unix** Access to the production servers and databases, including administrative access, is renewed on an annual basis. To renew access, a renewal URF must be completed for each employee that requires access and the renewal of access is approved by the employee's manager, or designee, and system owner. Failure to complete a renewal URF by the specified time will result in revocation of access privileges.	**Inspection** Inspected the annual access renewal to determine whether management initiates an annual access renewal of individuals with access to the production servers and databases, including administrative access.	No exceptions noted.
		Inspection Inspected URF tickets for a sample of users with access to production servers and databases, including administrative access, to determine whether access was renewed and approved by the employee's manager and system owner and whether access was revoked upon failure to complete a renewal URF.	No exceptions noted.
		Inspection Inspected a listing of users with administrative access to the production servers and databases to determine whether access is appropriately restricted.	No exceptions noted.
	Oracle Database Access to the production servers and databases, including administrative access, is renewed on an annual basis. To renew access, a renewal URF must be completed for each employee that requires access and the renewal of access is approved by	**Inspection** Inspected the annual access renewal to determine whether management initiates an annual access renewal of individuals with access to the production servers and databases, including administrative access.	No exceptions noted.

Logical Access			
Control Objective #5: *Controls provide reasonable assurance that logical access to systems and applications is restricted to authorized personnel.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
	the employee's manager, or designee, and system owner. Failure to complete a renewal URF by the specified time will result in revocation of access privileges.	**Inspection** Inspected URF tickets for a sample of users with access to production servers and databases, including administrative access, to determine whether access was renewed and approved by the employee's manager and system owner and whether access was revoked upon failure to complete a renewal URF.	No exceptions noted.
		Inspection Inspected a listing of users with administrative access to the production servers and databases to determine whether access is appropriately restricted.	No exceptions noted.
5.6	Super user access to UNIX (SUDO) is renewed on an annual basis. To renew access, a URF must be completed for each employee that requires access and the renewal of access is approved by the employee's manager and system owner. Failure to complete a renewal URF by the specified time will result in revocation of access privileges.	**Inspection** Inspected the annual access renewal to determine whether management initiates an annual access renewal of individuals with SUDO access to UNIX.	No exceptions noted.
		Inspection Inspected URF tickets for a sample of users with SUDO access to UNIX to determine whether access was renewed and approved by the employee's manager or system owner and whether access was revoked upon failure to complete a renewal URF.	No exceptions noted.
		Inspection Inspected a listing of users with SUDO access to UNIX to determine whether SUDO access is restricted to appropriate individuals.	No exceptions noted.

Logical Access			
Control Objective #5: *Controls provide reasonable assurance that logical access to systems and applications is restricted to authorized personnel.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
5.7	Logical access to production networks is implicitly denied by the firewalls. Required access is explicitly permitted by rules in the firewalls.	**Observation** Observed the access control list (ACL) that exists on the L+G switch for the population of customers to determine whether customers are restricted to their own production subnet and logical access to the production networks is implicitly denied by the firewalls.	No exceptions noted.
		Observation Observed a customer's production subnet to determine whether the L+G switch that creates the virtual LAN contains an ACL that does not allow communication among any of the customer virtual LANs and logical access is explicitly permitted by rules in the firewalls.	No exceptions noted.
5.8	The password settings within the LDAP (Unix) environment are reviewed on an annual basis by the System Administration team to ensure consistency with company policy.	**Inspection** Inspected evidence of management's review of the LDAP (Unix) environment password settings to determine whether they were reviewed on an annual basis by the System Administration team to ensure consistency with company policy.	No exceptions noted.
5.9	The password settings within the Oracle database environment are reviewed on an annual basis by the Database Administration team to ensure consistency with company policy.	**Inspection** Inspected evidence of management's review of the Oracle database environment password settings to determine whether they were reviewed on an annual basis by the Database Administration team to ensure consistency with company policy.	No exceptions noted.

Data Backup

Control Objective #6: *Controls provide reasonable assurance that application, operating systems, files and data are backed up on a scheduled basis, rotated to an offsite location and backup recovery tests are performed periodically.*

#	Control Activity	Test of Operating Effectiveness	Test Results
6.1	Symantec NetBackup software is used to manage the backup process and a backup schedule has been set for each of the servers on which data is stored. The system is configured to automatically send an email notification to the Database Administrators email group in the event of a failed backup. Failed backups are resolved.	**Inspection** Inspected global NetBackup settings and a sample of backup logs to determine whether NetBackup software is used to manage the backup process and a backup schedule has been set for each of the servers on which data is stored.	No exceptions noted.
		Inspection Inspected the system configurations to determine whether the system is configured to automatically send email notification to the Database Administrators email group in the event of a failed backup.	No exceptions noted.
		Inspection Inspected status emails for a sample of days to determine whether backup failures were resolved.	No exceptions noted.
6.2	L+G has contracted with a third party vendor to provide off-site storage. The backup tapes are sent offsite every 30 to 60 days, depending on the capacity of the tape, and returned onsite as they expire. For each set of tapes that is sent offsite, L+G prepares an offsite inventory/rotation schedule document that lists the tape reference numbers (bar code) and the return date for the tapes.	**Inspection** Inspected the contract with the third party off-site storage provider to determine whether L+G has contracted with a third-party provider to provide off-site storage.	No exceptions noted.
		Inspection Inspected a sample of inventory/ rotation logs listing the tape reference numbers (bar code) and the return date for the tapes to determine whether L+G tracks pick-up and delivery of tapes by Media Services every 30 to 60 days.	No exceptions noted.
6.3	Backup recovery tests are performed semi-annually. Completed tests are documented in a CRM ticket or email.	**Inspection** Inspected a sample of CRM tickets and emails to determine whether backup recovery tests are being performed semi-annually.	No exceptions noted.

Data Processing

Control Objective #7: *Controls provide reasonable assurance that data processing is appropriately authorized and scheduled, and deviations from scheduled processing are identified and resolved.*

#	Control Activity	Test of Operating Effectiveness	Test Results
7.1	A schedule is provided by each customer for the upcoming year's holidays and billing dates. This data for the subsequent year is entered into the system at the end of the current year and tracked by L+G in a CRM ticket. Schedule modifications and validation are tracked in L+G's ticketing system and follow the standard incident management process.	**Inspection** Inspected CRM tickets for a sample of customers to determine whether a schedule was provided by each customer for the upcoming year's holidays and billing dates.	No exceptions noted.
		Inspection Inspected the current schedule configured in the database for a sample of customers to determine whether the current database configurations agree to the schedule provided by each customer.	No exceptions noted.
		Inspection Inspected CRM tickets for a sample of customer schedule modifications to determine whether changes to customer holidays and billing dates are tracked in L+G's ticketing system and follow the standard incident management process.	No exceptions noted.
7.2	Statistics from the company are compiled monthly and a key performance indicator (KPI) report is created. This report is reviewed by operations management on a monthly basis, which entails follow up and resolution where KPI thresholds were not met, and focuses on performance indicators, such as: • incident/problem reporting; • SLA performance; • system availability and performance; • file delivery performance - Current month and annual performance trend; • OLA reporting; and • call volume reporting.	**Inspection** Inspected evidence of review of KPI reports for a sample of months to determine whether statistics from the company are compiled monthly and the report is reviewed by operations management on a monthly basis.	No exceptions noted.
		Inspection Inspected KPI reports for a sample of months to determine whether they include: • follow up and resolution where KPI thresholds were not met, and • performance indicators such as: o incident/ problem reporting, o SLA performance, o system availability and performance, o file delivery performance, o OLA reporting; and o call volume reporting.	No exceptions noted.

Data Processing			
Control Objective #7: *Controls provide reasonable assurance that data processing is appropriately authorized and scheduled, and deviations from scheduled processing are identified and resolved.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
7.3	Each customer within the platform has a file delivery time threshold which is configured in the system and is used to ensure delivery of the file within established parameters. If this threshold is not met, an alarm is raised to the Services Desk by the monitoring system. Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.	**Observation** Observed the file delivery time threshold configuration to determine whether a threshold is configured in the system and is used to ensure delivery of the file within established parameters.	No exceptions noted.
		Observation Observed the monitoring scripts that are configured to send alerts to the Service Desk upon system error to determine whether an alarm is raised by the monitoring system if the file delivery time is outside of the designated threshold.	No exceptions noted.
		Observation Observed the submission of an incoming file outside of the file delivery time threshold to determine whether an alarm was raised to the Service Desk by the monitoring system.	No exceptions noted.
		Inspection Inspected CRM tickets and tasks related to a semi-annual file delivery time threshold review to determine whether Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.	No exceptions noted.
7.4	Each customer within the platform has a file size threshold which is configured in the system and is used to determine successful processing and building of the data file extracts. If this threshold is not met, an alarm is raised to the Service Desk by the monitoring system. Customer Operations performs a semi-annual	**Observation** Observed the file size threshold configuration to determine whether a threshold is configured in the system and is used to determine successful processing and building of the data file extracts.	No exceptions noted.

Data Processing

Control Objective #7: *Controls provide reasonable assurance that data processing is appropriately authorized and scheduled, and deviations from scheduled processing are identified and resolved.*

#	Control Activity	Test of Operating Effectiveness	Test Results
	review of each customer's thresholds to confirm they are still appropriately configured in the system.	**Observation** Observed the monitoring scripts that are configured to send alerts to the Service Desk upon system error to determine whether an alarm is raised by the monitoring system if the file size is outside of the designated threshold.	No exceptions noted.
		Observation Observed the submission of an incoming file outside of the file size threshold to determine whether an alarm was raised to the Service Desk by the monitoring system.	No exceptions noted.
		Inspection Inspected CRM tickets and tasks related to a semi-annual file size threshold review to determine whether Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.	No exceptions noted.
7.5	Cron is the process scheduler, and additions, modifications or deletions to scheduled processes are managed via L+G's change management process.	**Inspection** Inspected RFC tickets for a sample of additions, modifications or deletions to the Cron process scheduler to determine whether L+G's change management process was followed for changes to the job scheduler.	No exceptions noted.
7.6	Access to modify the process scheduler is restricted to authorized personnel with SUDO permissions, controlled through the use of the "sudoers" files on each customers server. An annual access renewal and review is performed to ensure access remains commensurate with	**Inspection** Inspected the annual access renewal to determine whether management initiates an annual access renewal of individuals with access to modify the process scheduler to ensure access is restricted to authorized personnel.	No exceptions noted.

Data Processing			
Control Objective #7: *Controls provide reasonable assurance that data processing is appropriately authorized and scheduled, and deviations from scheduled processing are identified and resolved.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
	job responsibilities. To renew access, a User Request Form (URF) must be completed for each employee that requires access and the renewal of access is approved by the employee's manager and system owner.	**Inspection** Inspected URF tickets for a sample of users with access to modify the process scheduler to determine whether access was renewed and approved by the employee’s manager and system owner and whether access was revoked upon failure to complete a renewal URF.	No exceptions noted.
		Inspection Inspected listing of users with SUDO permissions to determine whether access to modify the process scheduler is restricted to authorized personnel.	No exceptions noted.

Data Transmission

Control Objective #8: *Controls provide reasonable assurance that data transmissions between the Company and external parties are secure, segregated and received from authorized sources.*

#	Control Activity	Test of Operating Effectiveness	Test Results
8.1	Customers access Virtual Local Area Networks (VLANs) to retrieve data files from L+G. Each customer has a secure, designated switch access list that manages the virtual LAN and blocks traffic between each of the customer's virtual LANs and prevents customers from accessing each other's data and the devices used to store and process data.	**Inspection** Inspected the Access Control List (ACL) that exists on the L+G switch for the population of customers to determine whether customers are restricted to their own production subnet, meaning logical access to the production networks is implicitly denied by the firewalls.	No exceptions noted.
		Observation Observed a customer's production subnet to determine whether the L+G switch that creates the virtual LAN contains an ACL that does not allow communication among any of the customer virtual LANs and logical, access is explicitly permitted by rules in the firewalls.	No exceptions noted.
8.2	Each customer is assigned a unique IP address and designated secure File Transfer Protocol (FTP) sites. A unique username and password are setup for each customer submitting transactions via FTP to ensure that data submitted is secure and segregated. Additionally, customers are blocked from accessing other segments of the L+G network from the secure FTP (SFTP) server.	**Observation** Observed the successful login of a customer to determine whether a unique user name and password are setup for each customer submitting transactions via FTP.	No exceptions noted.
		Observation Observed a failed login attempt to a customer's FTP site to determine whether customers are blocked from accessing other segments of the L+G network from the SFTP server.	No exceptions noted.
		Inspection Inspected the IP address for the entire population of customers to determine whether each customer has a unique IP address and designated FTP site.	No exceptions noted.

Data Recording

Control Objective #9: *Controls provide reasonable assurance that meter data is uniquely identifiable, recorded and processed completely and accurately.*

#	Control Activity	Test of Operating Effectiveness	Test Results
9.1	Meter readings are associated to customers via a database table. Each meter is assigned a unique "meter ID" and a utility identifier/meter serial number, which is utilized to prevent duplicates within the table.	**Observation** Observed the meter database table settings to determine whether each meter is assigned a unique meter ID and a utility identifier/ meter serial number, which is utilized to prevent duplicates within the table.	No exceptions noted.
		Observation Observed the creation of an existing meter ID to determine whether an error message was generated if the meter already exists in the database tale.	No exceptions noted.
9.2	Each customer has a file delivery time threshold which is configured in the system and is used to ensure delivery of the file within established parameters. If this threshold is not met, an alarm is raised to the Services Desk by the monitoring system. Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.	**Observation** Observed the file delivery time threshold configuration to determine whether a threshold is configured in the system and is used to ensure delivery of the file within established parameters.	No exceptions noted.
		Observation Observed the monitoring scripts that are configured to send alerts to the Service Desk upon system error to determine whether an alarm is raised by the monitoring system if the file delivery time is outside of the designated threshold.	No exceptions noted.
		Observation Observed the submission of an incoming file outside of the file delivery time threshold to determine whether an alarm was raised to the Service Desk by the monitoring system.	No exceptions noted.

Data Recording			
Control Objective #9: *Controls provide reasonable assurance that meter data is uniquely identifiable, recorded and processed completely and accurately.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
		Inspection Inspected CRM tickets and tasks related to a semi-annual file delivery time threshold review to determine whether Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.	No exceptions noted.
9.3	When a "fresh" reading for a meter is not available, the most recent field reading captured by the database is utilized. A threshold, or read window, is established that indicates a minimum timeframe prior to the billing information due date for meters to be read manually, if current readings are not available. Meters that have exceeded the threshold for reliable readings are marked by the system for a manual read ('M') to be performed by L+G field personnel, and the manual read is recorded in the customer's billing file. Changes to customer read windows are made following the standard change management process.	**Observation** Observed the customer read window configuration within the meter database to determine whether a read window has been established to indicate a minimum timeframe prior to the billing information due date for meters to be read manually, if current readings are not available.	No exceptions noted.
		Observation Observed the submission of a field reading that has exceeded the read window threshold to determine whether the meter was a marked for a manual read ('M') by the system, and the manual read is recorded in the customer's billing file.	No exceptions noted.
		Inspection Inspected RFC tickets for a sample of changes to customer read windows to determine whether changes to read windows follow the standard change management process.	No exceptions noted.

Data Recording

Control Objective #9: *Controls provide reasonable assurance that meter data is uniquely identifiable, recorded and processed completely and accurately.*

#	Control Activity	Test of Operating Effectiveness	Test Results
9.4	Customers provide files that indicate added meters, removed meters, or meters that have changed accounts for billing purposes. An automated check exists in the database to ensure the record counts of meters submitted by the customers agree to the record counts processed within the L+G database. Error messages are generated as a result of unsuccessful processing.	**Observation** Observed the scripts used to process customer meter update information onto L+G's meter table database to determine whether the database is configured to receive files from customers.	No exceptions noted.
		Observation Observed the submission of a customer file into L+G's database to determine whether an automated check exists in the database to ensure the record counts submitted by the customers agree to the record counts processed within the L+G database.	No exceptions noted.
		Observation Observed the submission of an unsuccessful customer file of meter account data into the meter database table to determine whether an error message was generated as a result of the unsuccessful submission.	No exceptions noted.
9.5	Each customer within the platform has a file size threshold which is configured in the system and used to determine successful processing and building of the data file extracts. If this threshold is not met, an alarm is raised to the Service Desk by the monitoring system. Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.	**Observation** Observed the file size threshold configuration to determine whether a threshold is configured in the system and is used to determine successful processing and building of the data file extracts.	No exceptions noted.
		Observation Observed the monitoring scripts that are configured to send alerts to the Service Desk upon system error to determine whether an alarm is raised by the monitoring system if the file size is outside of the designated threshold.	No exceptions noted.
		Observation Observed the submission of an incoming file outside of the file size threshold to determine whether an alarm was raised to the Service Desk by the monitoring system.	No exceptions noted.

Data Recording

Control Objective #9: *Controls provide reasonable assurance that meter data is uniquely identifiable, recorded and processed completely and accurately.*

#	Control Activity	Test of Operating Effectiveness	Test Results
		Inspection Inspected CRM tickets and tasks related to a semi-annual file size threshold review to determine whether Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.	No exceptions noted.
9.6	Meter reading counts are logged to confirm completeness with total meter readings expected. Customer Operations Center analysts use the existing incident management procedures to open CRM tickets, as applicable, for variances that are outside expected thresholds and cannot be explained and to engage the appropriate resources required to resolve the incident timely.	**Observation** Observed the submission of an out-of-threshold incoming file of field reading into the meter database table to determine whether an error message was generated as a result of the unsuccessful submission.	No exceptions noted.
		Inspection Inspected CRM tickets for a sample of incidents where variances between the reading counts and total meter readings expected cannot be explained to determine whether: • a Customer Operations Center analyst creates a CRM ticket to record the details of the problem identified, and • the CRM is escalated and resolved in a timely manner, following standard operating procedure documents.	No exceptions noted.
9.7	Statistics from the company are compiled monthly and a key performance indicator (KPI) report is created. This report is reviewed by operations management on a monthly basis, which entails follow up and resolution where KPI	**Inspection** Inspected evidence of review of KPI reports for a sample of months to determine whether statistics from the company are compiled monthly and the report is reviewed by operations management on a monthly basis.	No exceptions noted.

Data Recording			
Control Objective #9: *Controls provide reasonable assurance that meter data is uniquely identifiable, recorded and processed completely and accurately.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
	thresholds were not met, and focuses on performance indicators, such as: • incident/problem reporting; • SLA performance; • system availability and performance; • file delivery performance - Current month and annual performance trend; • OLA reporting; and • call volume reporting.	**Inspection** Inspected KPI reports for a sample of months to determine whether they include: • follow up and resolution where KPI thresholds were not met, and • performance indicators such as: o incident/ problem reporting, o SLA performance, o system availability and performance, o file delivery performance, o OLA reporting; and o call volume reporting.	No exceptions noted.

Data Output			
Control Objective #10: *Controls provide reasonable assurance that data output is distributed in a timely manner to appropriate users.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
10.1	Each customer within the platform has a file delivery time threshold which is configured in the system and is used to ensure delivery of the file within established parameters. If this threshold is not met, an alarm is raised to the Services Desk by the monitoring system. Customer Operations performs a semi-annual review of each customer's thresholds to confirm they are still appropriately configured in the system.	**Observation** Observed the file delivery time threshold configuration to determine whether a threshold is configured in the system and is used to ensure delivery of the file within established parameters.	No exceptions noted.
		Observation Observed the monitoring scripts that are configured to send alerts to the Service Desk upon system error to determine whether an alarm is raised by the monitoring system if the file delivery time is outside of the designated threshold.	No exceptions noted.
		Observation Observed the submission of an incoming file outside of the file delivery time threshold to determine whether an alarm was raised to the Service Desk by the monitoring system.	No exceptions noted.
		Inspection Inspected CRM tickets and tasks related to a semi-annual file delivery time threshold review to determine whether Customer Operations performs a semi-annual review of each customer’s thresholds to confirm they are still appropriately configured in the system.	No exceptions noted.
10.2	Customers access virtual Local Area Networks (LANs) to retrieve data files from L+G. Each customer has a secure, designated switch access list that manages the virtual LAN and blocks traffic between each of the customer's virtual LANs and prevents customers from accessing each other's data and the devices used to store and process the data.	**Inspection** Inspected the Access Control List (ACL) that exists on the L+G switch for the population of customers to determine whether customers are restricted to their own production subnet and logical access to the production networks is implicitly denied by the firewalls.	No exceptions noted.

Data Output			
Control Objective #10: *Controls provide reasonable assurance that data output is distributed in a timely manner to appropriate users.*			
#	**Control Activity**	**Test of Operating Effectiveness**	**Test Results**
		Observation Observed a customer's production subnet to determine whether the L+G switch that creates the virtual LAN contains an ACL that does not allow communication among any of the customer virtual LANs and logical access is explicitly permitted by rules in the firewalls.	No exceptions noted.
10.3	Statistics from the company are compiled monthly and a key performance indicator (KPI) report is created. This report is reviewed by operations management on a monthly basis, which entails follow up and resolution where KPI thresholds were not met, and focuses on performance indicators, such as: • incident/problem reporting; • SLA performance; • system availability and performance; • file delivery performance - Current month and annual performance trend; • OLA reporting; and • call volume reporting.	**Inspection** Inspected evidence of review of KPI reports for a sample of months to determine whether statistics from the company are compiled monthly and the report is reviewed by operations management on a monthly basis.	No exceptions noted.
		Inspection Inspected KPI reports for a sample of months to determine whether they include: • follow up and resolution where KPI thresholds were not met, and • performance indicators such as: o incident/ problem reporting, o SLA performance, o system availability and performance, o file delivery performance, o OLA reporting; and o call volume reporting.	No exceptions noted.

V. Other Information Provided by Landis+Gyr Technology, Inc.

The information describing Landis+Gyr's management's response to the exception, environmental controls, physical security notifications, network monitoring, application changes, change management, logical access, data processing, and data recording, is presented by Landis+Gyr ("L+G") to provide additional information and is not a part of L+G's description of controls that may be relevant to customers' internal control as it relates to an audit of financial statements.

Management's Response to the Exception

As it relates to control activity 4.6, L+G acknowledges that system time stamped evidence confirming the completion of three reviews is not available, but asserts that the reviews did occur. L+G has implemented a solution which will retain system time stamped historical evidence of review completion for future audits.

Additionally, L+G reviewed the aforementioned reports a second time and no causes for concern were identified.

Environmental Controls

In the Lenexa, KS, data center, environmental safeguards such as raised floors, fire suppression, air conditioning, sprinkler systems and uninterruptible power supply (UPS) systems have been installed in order to protect computer equipment and data from environmental risks. This equipment is maintained by manufacturers or contracted vendors. The L+G facility in Lenexa, Kansas includes the production data center and test devices. The data center room is built on a raised floor and is monitored 24 x 7.

The overall facility is protected by a sprinkler system which is tested annually. The data center room is protected by a dry sprinkler system and an Inergen based fire suppressant which is tested semi-annually. The sprinkler has a dual trigger dry pipe, which requires either heat or smoke to activate the system.

In the event of a fire alarm within the facility, an audible alarm is activated in the data center and overall Customer Operations building. In addition, the fire and intrusion detection system is monitored by an offsite company. In the event of an alarm, this vendor contacts the Customer Operations facility to confirm if there is a fire or safety emergency. If there is an emergency, the offsite company contacts the respective fire and police authorities. Handheld fire extinguishers are located in the data center in the event of small emergencies.

The data center is supported by a UPS system and a diesel generator, which will sustain computer operations in the event of a commercial power loss. The UPS system protects the data center during an initial power loss and provides "conditioned" power to the systems within the data center. The UPS system is located in a secure area within the data center, which requires authorized card access for entry. There is an automated switch that turns the diesel generator on after ten seconds in the event of a loss of commercial power. The generator is located in a secured area adjacent to the loading dock. There are weekly test runs performed on the generator. Results from the tests are monitored for trends or discrepancies. If there are abnormalities in the UPS system readings, a vendor is under contract to perform necessary maintenance. This vendor also performs regular preventive maintenance and inspection of the UPS system. Another vendor provides maintenance on the diesel generator including routine maintenance and servicing of any malfunctions identified during regularly scheduled testing.

The manufacturers and contracted vendors maintaining the environmental equipment perform semi-annual and annual monitoring and tests of the fire suppressant, data center air conditioning, and UPS system.

A dedicated environmental system provides proper air, temperature, and humidity controls for the data center. There is a flood detection system installed under the raised floors. The system consists of a cord, which wraps under the raised floor cooling units. If water touches any part of the cord, it immediately sends an alarm notification via e-mail to Customer Operations personnel and indicates the location of the potential leak. The data center is monitored by vendor environmental sensors, which display a warning to the Customer Operations personnel if problems arise. Vendor maintenance logs and monitoring reports are maintained as evidence of vendor monitoring.

Physical Security Notifications

Electronic card access is required for entry into the main facility. All visitors to the Lenexa L+G facility, including visiting L+G employees, are required to obtain and use a visitor's badge in order to access the building via the card reader system. Automated notifications are sent to responsible personnel the morning of the scheduled return date. Should a badge become overdue for return, the badge is deactivated and automated notifications are sent daily to ensure visibility to the current badge status.

Network Monitoring

General information

Network infrastructure is monitored to increase the assurance of continuous operations and to identify potential issues. The L+G Customer Operations Center is monitored 24 x 7 by a team that monitors the network for issues, including weather and power problems that may cause outages on different areas of the network, such as meters and collectors. The Customer Operations Center utilizes an automated solution for network monitoring, which includes polling network devices and systems. This polling is performed with SNMP, Ping, SSH and Telnet. Performance data is collected and automated alerts are generated to notify Customer Operations in the event of a monitoring issue.

Incidents are initiated by a customer, L+G personnel or via automated monitoring alerts which are sent to Customer Operations Center staff. A Customer Operations Center staff member creates a CRM ticket, as applicable, to record the details of the problem identified, which is escalated and resolved following standard operating procedure documents. Refer to control objective #1 – Incident Management above for additional details.

The monitoring application receives simple network management protocol (SNMP) traps sent by network devices which allows a large footprint of monitoring capabilities and provides performance monitoring of several devices from storage, to system controller, to universal resource locator (URL) availability. The Customer Operations Center team updates the "shift brief" log for each daily shift change to track issues and duties that are transferred for resolution between shifts.

LAN/WAN monitoring

The Network Engineering team monitors network utilization, latency, distribution, and packet loss. The Network Engineering team reviews the output from the Cacti server (round robin database (RRD) based graphic tool), which displays the traffic load on network links, and allows the team to isolate network segments or devices that may be overloaded by traffic as necessary.

L+G utilizes syslog servers. One is used by the Manager of Infrastructure Engineering, or designee for forensic purposes. The syslog servers are administered by the Network Engineering group. The routers, switches, and firewalls are configured to log to the syslog servers. The network devices are set to log exceptions such as failed login attempts and interface resets. The logs are retained for the maximum amount of time possible based on disk space requirements. Logs are collected from the network devices and accessed through a syslog server. If the Operation Support team notifies the Network Engineering team of an issue, the syslog server is one of the tools used to research the problem. If there are issues that are discovered "after the fact", the logs can be utilized by Network Engineering to research the issue.

L+G management tracks issues with network devices to prevent problems from remaining unresolved for extended periods of time. Performance reports are reviewed by operations management on a regular basis for issues designated as high or of critical importance to ensure issues are resolved in a timely manner. Monthly, statistics from the company are compiled and a KPI report is created which is reviewed by management on a monthly basis.

WAN redundancy

L+G utilizes redundant architecture to increase the assurance that connectivity is maintained with customers and with the meters and devices in the field. The Customer Operations campus has a synchronous optical networking (SONET) ring architecture which utilizes multiple carriers, providing protection against the loss of local circuits in Lenexa. L+G also utilizes redundant architecture in connecting collectors to the Customer Operations Data Center. Certain collectors have both an A-side and a B-side connection from the collector to the portmaster terminal server. L+G uses redundant routers, switches, and dual connections to transmit data to the cell manager located at Customer Operations.

Application Changes

Release Management

L+G conducts regular meetings of the Release Architecture Team to discuss changes and enhancements that have come from Product Management via the New Product Introduction (NPI) process. This process provides approval, budget review, requirements gathering, etc. Requests may also originate through L+G's business life cycle where defects and enhancements come from user organizations. The Release Architecture Team membership consists of management personnel from key areas of the organization including product management, software development, quality assurance, service delivery, and customer operations, if applicable.

Change Management

On-site parts inventory levels provide for sufficient standbys for critical systems based on an analysis of the installed servers, operating system baseline(s), and vendor provided mean time between failure information. If an outage resolution is beyond the capabilities of L+G, support from third-party external vendors would be an option. L+G receives e-mail alerts from vendors notifying L+G of upcoming patches. L+G performs patch implementations to production devices as required.

Pre-authorized Changes

L+G has implemented a process for pre-authorizing certain routine maintenance tasks. Pre-authorized changes are a controlled subset of common change types and are considered to be routine maintenance tasks that require pre-authorized CAB approval. Pre-authorized changes are categorized into two groups: 1) tasks that do not require RFC's, such as backup jobs and 2) changes that require RFC's for documentation and tracking purposes, such as replacement of redundant hot swappable components. In order for a change to be considered as pre-authorized, the change must not be expected to cause any "downtime" to the system, or impact system functionality, user interaction with the system, or other required elements of system availability or operation and must be transparent to the end users of the system.

Change types submitted for inclusion in the pre-authorized change list require an initial review and approval by the CAB, or a subset of CAB members as applicable. Once an item or change type is approved, it is added to the "Pre-Authorized/Non-Change Control Board (CCB) Required Activities Form". The list of pre-authorized changes is reviewed annually by the CAB. Changes to the Pre-Authorized/Non-CCB Required Activities Form (additions, deletions or other modifications), may be performed throughout the year as necessary, but require approval as outlined above.

Pre-authorized changes must be reviewed and approved by the Change Manager prior to implementation in the production environment. The Change Manager may, at his/her discretion, approve an RFC of this nature without formal CAB review, or may elect to bring the request to the CAB for consideration and approval.

L+G maintains the list of pre-authorized changes on L+G's intranet.

Standard Changes

Approval is obtained from the program office and/or customer if downtime to the system is required. This approval may be provided via email, phone or other method and includes scheduling the change for implementation.

Logical Access

The L+G network devices (routers, switches, firewalls) at the Lenexa facility are maintained by the Network Engineering team. Least-privileged access is provided to members of the Operations Support team for investigative purposes, but privileges to change device configurations are limited to the Network Engineering team. Configurations for network devices are backed up as changes occur or on a weekly basis. The Network Engineering team uses a script to compare the current configuration to the backup configuration at the end of each day. Any changes to the network device configuration are tracked in a log. If the change was not expected, an investigation begins and the Network Engineering team restores the backup configuration for the device if necessary. In order to access any of the L+G switches, routers, or local accounts, users must authenticate through a Terminal Access Controller Access-Control System (TACACs+) server. The ability to modify network device configurations is restricted via TACACs+ to Network Engineering personnel.

Data Processing

Command Center system

L+G analysts perform checks within the Command Center system to validate loading, and processing of data. The Command Center system provides alerts and notifications via the dashboard views for L+G technicians to investigate. When issues are discovered, a CRM ticket is created to resolve the issue, as necessary.

Data Recording

Data received and recorded from the field utilizes a standardized and uniform format. Field data that is collected from the network is loaded directly into the database without transformations to maintain data integrity and increase the assurance of accurate representation of the meter readings.

Firewalls also protect the L+G internal network from unauthorized access when retrieving field data. The cell manager servers at L+G Customer Operations control the data collected from the field and determine where the data is loaded. The cell manager on each customer's virtual LAN contains logic to increase the assurance that it only retrieves and inputs data from appropriate customer meters. Each head-end system retrieves information from certain collectors in the field based on routing information. The routing information received details which collectors have collected readings corresponding to individual L+G customers.