GENERAL CONTROLS SUPPORTING THE ONLINE TIME MANAGEMENT SOLUTIONS

SOC 1 - SSAE 16 Type II Audit

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of the Controls

For the Period November 1, 2014 to October 31, 2015

INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

The Moore Group, CPA
SOC Audit Specialists

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

To: NOVAtime Technology, Inc.:

We have examined NOVAtime Technology, Inc.'s (NOVAtime) description of its online time management solutions and systems for processing user entities' transactions throughout the period November 1, 2014 to October 31, 2015 and the suitability of the design and operating effectiveness of 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 NOVAtime'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.

NOVAtime uses a third party data center to house its critical production computer servers, applications and networking equipment. The descriptions of controls within Section 4, the Testing Matrices, includes only the controls and related control objectives of NOVAtime and excludes the control objectives and related controls of the third party data center. NOVAtime has included a summary of the services utilized and related controls of the third party data center in Section 5, Other Information Provided by the Service Organization. Our examination did not extend to controls of the third party data center.

In Section 2, NOVAtime 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. NOVAtime 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 to achieve the related control objectives stated in the description.

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 November 1, 2014 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 Section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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.

In our opinion, in all material respects, based on the criteria described in NOVAtime's assertion in Section 2,

a. the description fairly presents the online time management solutions and systems that were designed and implemented throughout the period November 1, 2014 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 November 1, 2014 to October 31, 2015, and user entities applied the complementary user entity controls contemplated in the design of NOVAtime's controls throughout the period November 1, 2014 to October 31, 2015.

c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period November 1, 2014 to October 31, 2015.

The specific controls tested and the nature, timing, and results of those tests are listed in Section 4, the "Testing Matrices".

The information in Section 5 is presented by NOVAtime to provide additional information and is not a part of NOVAtime's description of controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements. Such information has not been subjected to the procedures applied in the examination of the description of the operations, and accordingly, we express no opinion on it.

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of NOVAtime and the user entities of NOVAtime's online time management solutions and systems during some or all of the period November 1, 2014 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.

The Moore Group CPA, LLC

November 24, 2015
Nashua, NH

SECTION 2

ASSERTIONS BY THE SERVICE ORGANIZATION'S MANAGEMENT

NOVATIME MANAGEMENT'S ASSERTION

We have prepared the description of NOVAtime's online time management solutions and systems ("description") for user entities of the services and systems during some or all of the period from November 1, 2014 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 misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the online time management solutions and systems made available to user entities of the services and systems during some or all of the period from November 1, 2014 to October 31, 2015. The criteria we used in making this assertion were that the description:

   i. presents how the services and systems made available to user entities of the services and systems were 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 reports and other information prepared for user entities.

      3) the related accounting records, if applicable, 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 and other information prepared for user entities.

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

      5) the process used to prepare reports and other information for user entities.

      6) the specified controls 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 services or systems, while acknowledging that the description is presented 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 services or systems that each individual user entity of the services and systems and its auditor may consider important in its own particular environment.

   iii. includes relevant details of changes to the service organization's services and systems during the period covered by the description when the description covers a review over time.

b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period from November 1, 2014 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 management;

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, and manual controls were applied by individuals who have the appropriate competence and authority.

SECTION 3

DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM PROVIDED BY MANAGEMENT OF NOVATIME

DESCRIPTION OF CONTROLS PLACED IN OPERATION

OVERVIEW OF OPERATIONS

Company Background

Founded in 1999, NOVAtime Technology, Inc. (NOVAtime) is a private C-corporation located in Diamond Bar, California, within the county of Los Angeles. NOVAtime provides an online SaaS (Software as a Service) application for time management. NOVAtime provides services and solutions to thousands of organizations, ranging from under 100 employees, to over 80,000 employees.

NOVAtime currently has over 80 employees and an employee turnover rate of less than 5%. Each member of the team has extensive knowledge in the industry, averaging over 10 years.

Major Milestones in NOVAtime history include:

- **1999** NOVAtime began building from the ground up, using a multi-tier design, OOPs, and UML, establishing a strong, scalable framework for future development.
- **2000** The first product release for NOVAtime 2000 brought an innovative and comprehensive solution to mid-sized companies of up to a thousand employees.
- **2003** Utilizing the Microsoft .NET Roadmap, NOVAtime continued to expand its product line with the release of NOVAtime 3000, a complete client/server, web-enabled solution for businesses of all sizes.
- **2004** Strategic alliance with the best intelligence staffing provider established NOVAtime as a frontrunner in the industry. NOVAtime also began distinguishing itself from the competition with true load balancing, architected to scale to meet client demands.
- **2006** NOVAtime became one of the first in the industry to utilize PUSH technology. This advancement gave NOVAtime the technology for full integration with NOVAtime Enterprise Web Services (NEWS).
- **2007** The release of the hosted NOVAtime 4000 SaaS model made the powerful Workforce Management solution 100% web-based.
- **2008** NOVAtime established a strategic alliance with an industry-leading HR solution provider, raising the bar and paving the way for company growth. NOVAtime earned Plynt™ Application Security Penetration Test Certification and became a Microsoft® Gold Certified Partner.
- **2009** Introduction of NOVAtime 4000 STAR provided a licensed option for clients to host the solution on-premise.
- **2011** NOVAtime accomplished 12 straight years of continued growth. Introduction of NOVAtime 4000 STARbox incorporated a turn-key 4000 platform and one-touch update capability.
- **2012** Expanded to a secondary data center on East Coast for SaaS clients. Hosted NOVAtime's inaugural user group and introduced the NT450 time clock – the most affordable and stable time clock in NOVAtime's history.
- **2013** NOVAtime achieved 14 years of continued overall growth. NOVAtime completed an independent audit and achieved SSAE16 Type II compliance. Introduced the NT7000 time clock – the most powerful and feature-rich clock to date, complete with multi-lingual support.

- **2014** Introduced the much optimized and scalable SaaS release, NOVAtime 5000, and successfully piloted with a sizeable health care client. NOVAtime 5000 also features the Advanced Schedule Manager (ASM) and support for rugged handheld NT65M that was successfully used by a prominent NFL franchise.

The NOVAtime SaaS Application

NOVAtime SaaS is an online time management service. NOVAtime provides innovative workforce management solutions that bring high efficiency and accuracy to labor processes. The offerings include a suite of Workforce Management solutions including Time & Attendance, Scheduling, Points, Labor Costing, Leave Management and Employee Self Service to the private and public sectors.

The NOVAtime solution was one of the first-to-market with "push" technology time clocks in the workforce management industry. It enables data collection through a variety of methods, and it provides interfaces to hundreds of payroll services and applications. This cost-effective solution platform supports flexible delivery methods, including an on-premise licensed web application, as well as a subscription-based hosted SaaS application with a secure, multi-tiered, multi-tenant infrastructure.

NOVAtime adopted and applied the latest technologies in the development of NOVAtime's solutions, including object oriented programming (OOP), unified modeling language (UML) framework, as well as .Net Workflow, Silverlight, and HTML5. Its baseline code is developed through the use of several programming languages, including ASP.NET, VB .NET, C/C++, C#.NET and javascript.

Facilities

For co-location of critical production servers, applications, and networking equipment, NOVAtime utilizes a secure third party data center provided by CenturyLink Technology Solutions (formerly Savvis, a CenturyLink Company). CenturyLink Technology Solutions' physical and environmental security controls are described in Section 5 of this report, as included in their SOC 1-SSAE 16 report for the period July 1, 2014 to June 30, 2015.

For co-location of disaster recovery and backup systems, NOVAtime utilizes a geographically redundant CenturyLink Technology Solutions data center on the east coast.

Development and QA testing tasks are performed at corporate headquarters in Diamond Bar, California. Updates to production are made via IPSec encrypted VPN connections to the production servers at the CenturyLink Technology Solutions data center in Irvine.

Processes and Data Flow

NOVAtime's production topology is set up in 3 Tiers:

- Web Farms (Front end)
- Application Clusters (Middle)
- SQL Servers (Backend).

The bulk of the NOVAtime SaaS data involves time records. All production devices are synchronized to a master NTP source in production which in turn is synchronized with a NIST Internet time server. The time clock devices at the customer site will also synchronize their time when communicating with NOVAtime servers.

The applications run on Windows Server 2008R2, 2012 R2 and Dell server platforms with SQL databases to support the applications. Best of breed monitoring tools provide alerts (i.e. temperature, voltage, server resources) if thresholds are exceeded, in addition to an enterprise monitoring application. Redundant architecture is in place, including:

- Redundant servers for critical systems
- Firewalls configured in an active-passive configuration
- Load balancers configured in primary-backup configuration
- Switches
- Network interface cards (NICs)
- Power supplies
- RAID storage.

Servers and workstations utilize anti-virus endpoint protection, which is kept properly updated and conducts routine scans. In addition, a perimeter firewall with deny by default policy provides a first line of defense. Patches for critical production servers are updated manually to ensure adequate testing and that no production interference will result. Other servers and workstations are automatically updated via WSUS (Windows Server Update Service), in which a central monitoring server pushes updates as discovered.

NOVAtime uses a multilevel backup strategy. For backups of critical internal company data, weekly full backups and daily incremental backups are taken utilizing Symantec Backup Exec. They are stored onsite in a NAS (Network Attached Storage). In addition, the backups are duplicated to external USB drives, which are taken offsite to secure storage and retained 8 weeks.

Customer databases are backed up utilizing SQL functionality. Disk-to-disk backups are made to redundant NAS devices at the primary production data center. Both SQL Studio scripts and internal proprietary scripts are utilized to define the schedule and scope of backups. The data is retained 2 years. For canceled clients, an archive is established at the end of service and will be retained for 7 years to allow retrieval when requested.

Customer data is also replicated utilizing SAN replication and de-duplication technologies to a secondary, geographically redundant CenturyLink Technology Solutions data center in New Jersey to protect against problems at the network or physical host level. Snapshots take place hourly (48 snapshot retention) and on a daily basis (retained 7 days.) Data transport takes place over the CenturyLink WAN (Wide Area Network, not the internet), and are further secured by NOVAtime utilizing IPSec encrypted VPN technology (Virtual Private Network).

In addition, another replication level takes place at the virtualization layer using MS HyperV technology, to protect against faults on virtual servers.

For inbound data, customers access the service from an internet browser, using HTTPS connections with 256-bit SSL encryption. Customers can only access the web cluster on the load balancers. Even the customers' time-punching clocks communicate via HTTPS to upload punches at job sites. (Straight HTTP is used for some customers' legacy clocks.)

For data import, NOVAtime connects to client's SFTP server to retrieve the data over SSH encrypted connections. Each customer has a separate database, stored on the SAN (Storage Area Network).

For outbound data back to customers, a Task Scheduler feature allows each customer to schedule reports to be generated to be automatically emailed, or generated and picked up by the customer from their report repository. There is no need for pre-defined/scheduled data transmission to and from the customer.

The NOVAtime functionality re-calculates and reposts data when discrepancies due to pay policy or rule setup are detected. Punches can be over-written by Supervisors to adjust the timesheets to correctness.

NOVAtime utilizes the underlying transmission protocol's data integrity check to detect discrepancies in transit.

Certain IT engineers access production network equipment and data stored at the third party data center remotely, via secure VPN tunnels protected by IPsec encryption.

CONTROL ENVIRONMENT

Integrity and Ethical Values

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

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

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

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

Commitment to Competence

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

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into **written position requirements**.
- Management utilizes **skills assessment testing** for certain position s during the hiring process, including programmer, tech support and QA, and lead generation specialists.
- Management has developed an initial **training and development program** with peers and supervisors, as well as ongoing training to maintain and enhance the skill level of personnel on an as-needed basis.
- For NOVAtime employees not directly engaged in application development, management provides **ongoing employee training** related to system and application enhancements and version modifications, to maintain and enhance the skill level of personnel.
- Management encourages employees to complete and continue **formal education** and technical certification programs.
- Management-approved **professional development expenses** incurred by the employees are paid by NOVAtime.
- Each new employee undergoes an **initial 90 day probationary period and performance review** to evaluate performance.
- Each employee undergoes a **semi-annual performance review** each year. During these reviews, management reinforces and updates professional development plans for each employee.

Board of Directors' Participation

NOVAtime's control consciousness is influenced significantly by its Board of Directors participation. The Board of Directors oversees management activities and meets annually to discuss strategic, operational, and compliance issues.

Management's Philosophy and Operating Style

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

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

- NOVAtime uses an external law firm to keep updated with the latest employment law, regulatory and industry changes as needed.
- Management regularly attends **trade shows,** utilizes **trade and regulatory publications, journals, online news feeds and government sites**, and belongs to **industry associations** to stay current on any regulatory compliance or operational trends affecting the services provided.
- **Management meetings** are held on a regular basis to discuss operational planning and budgeting, human resource planning and hiring, and customer related issues. Meeting agendas and meeting minutes are recorded and communicated to relevant personnel.
- Management engages an **independent CPA firm** to audit NOVAtime's financial statements on an annual basis.

Organizational Structure and Assignment of Authority and Responsibility

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

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

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

- **Organizational charts** are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and are updated as needed.
- **Workflow charts** are in place to communicate information about the roles of different employees. These charts are communicated to employees and are updated as needed.
- NOVAtime's **operating goals and objectives are communicated** to the entire organization during regular staff meetings, employee performance reviews, and other written communications.
- NOVAtime provides an **employee orientation program** that communicates organizational structure and responsibility, company and departmental objectives, and relationships between departments and personnel.
- NOVAtime has established a **segregation of duties process**, which is based upon changes and recommendations from management.

Human Resource Policies and Practices

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

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

- Management has established **hiring guidelines and procedures** that guide the hiring process to ensure that specific elements of the hiring process are consistently executed.
- Human Resources management utilizes a **new hire checklist** to ensure that specific elements of the hiring process are consistently executed. A copy of the new hire checklist is maintained in the employee file.
- Comprehensive **background checks** are performed by an independent third party for all employees as a component of the hiring process. Management has developed a detailed **employee handbook** that communicates human resource policies and practices.
- NOVAtime utilizes a **formal training program** for each new employee. Ongoing training is also utilized for each employee on an as-needed basis beyond the initial hiring training period.
- Management conducts **performance evaluations** and career development discussions with each employee on an initial 90 day, and thereafter, semi-annual basis. A formal evaluation form is prepared, and is maintained in employee's HR file.
- Management has established **employee termination procedures** that guide the termination process.
- Human Resources management utilizes a **termination checklist** to ensure that specific elements of the termination process are consistently executed. This includes but is not limited to the terminated employee's physical and logical access to company facilities and computer systems. The checklist is retained in the employee files.

RISK ASSESSMENT

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

Objective Setting

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

NOVAtime has established certain broad categories including:

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

Risks Identification

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

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

External Factors

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

Internal Factors

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

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

Risks Analysis

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

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

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

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

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

Selection and Development of Control Activities

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

NOVAtime's control objectives and related control activities are included in Section 4 (the "Testing Matrices") of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in the Testing Matrices. Although the control objectives and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of NOVAtime's description of controls.

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

MONITORING

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

Ongoing and Separate Evaluations of the Control Environment

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

Ongoing Monitoring

Examples of NOVAtime's ongoing monitoring activities include the following:

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

Separate Evaluations

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

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

Reporting Deficiencies

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

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

A combination of custom developed and commercial applications are utilized to support the online time management solutions provided to user organizations. The applications run on Windows Server 2008 R2, 2012 R2 and Dell server platforms with SQL databases to support the applications.

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

Communication Systems

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

DISCLOSURES OF RELEVANT INFORMATION

Significant Changes During the Review Period

There were no significant changes to the control environment during the review period.

Subsequent Events

No material events occurred subsequent to the period covered by management's description of the service organization's system up to the date of the service auditor's report that could have a significant effect on management's assertion.

Using the Work of the Internal Audit Function

The service auditor did not utilize any work of the internal audit function in preparing this report.

COMPLEMENTARY CONTROLS AT USER ORGANIZATIONS

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

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

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

SECTION 4

TESTING MATRICES

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Integrity and Ethical Values		
1.1	The **employee handbook** contains organizational policy statements, and codes of conduct and benefits and practices to which all employees are required to adhere.	Inspected the employee handbook to determine that it contains organizational policy statements, benefits and practices to which all employees are required to adhere.	No exceptions noted.
1.2	**Codes of conduct**, organizational policy statements, and disciplinary policies are documented and communicate entity values and behavioral standards to personnel.	Inspected the codes of conduct, policy statements, and disciplinary policies to determine that these are documented and communicate entity values and behavioral standards to personnel.	No exceptions noted.
1.3	Policies and procedures require that new employees sign an **employee handbook acknowledgment form** indicating that they have been given access to it, and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook. The signed form is kept in the employee personnel file.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee handbook and understand their responsibility for adhering to the standards, policies and procedures contained within the handbook.	No exceptions noted.
1.4	Employees must sign a **confidentiality and non-disclosure agreement** to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
1.5	Comprehensive **background checks** are performed by an independent third party for all employees as a component of the hiring process. These background checks include but are not limited to: • Criminal records (federal and county) • Credit report • E-Verify (Homeland Security).	Inspected completed background checks for a judgmental sample of employees hired during the review period to determine that background checks are performed by an independent third party, and that they include: • Criminal records (federal and county) • Credit report • E-Verify (Homeland Security).	No exceptions noted.
1.6	Management personnel perform **reference checks** on all candidates being considered for positions within NOVAtime, including: • Personal reference checks • Verification of past employment • Verification of professional certifications for programmers.	Inquired of management to determine that management personnel perform reference checks on all candidates being considered for positions within NOVAtime.	No exceptions noted.
1.7	Management maintains a commercial **insurance policy** which includes professional errors and omissions coverage.	Inspected insurance coverage policy declarations page to determine that management maintained a commercial insurance policy which includes professional errors and omissions coverage.	No exceptions noted.
1.8	Periodic **meetings with staff** are conducted whereby the core values and mission of NOVAtime are discussed as well as ways to reinforce and improve the components of NOVAtime's related core functions.	Inquired of management to determine that periodic meetings with staff are conducted whereby the core values and mission of NOVAtime are discussed as well as ways to reinforce and improve the components of NOVAtime's related core functions.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Commitment to Competence		
1.9	Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into **written position requirements**.	Inspected a judgmental sample of written job descriptions to determine that management had considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.	No exceptions noted.
1.10	Management utilizes **skills assessment testing** for certain position s during the hiring process, including programmer, tech support and QA, and lead generation specialists.	Inspected a sample of skills assessment test templates utilized during the review period to determine that management utilizes skills assessment testing for certain positions during the hiring process.	No exceptions noted.
1.11	Management has developed an initial **training and development program** with peers and supervisors, as well as ongoing training to maintain and enhance the skill level of personnel on an as-needed basis. This includes five types of training: • New employee orientation • On the job training • Annual product training • Ad hoc HR training regarding company policies • Offsite seminars as needed	Inquired of management into initial and ongoing training and development program for employees.	No exceptions noted.
		Inspected a judgmental sample of company documentation (meeting agendas, assignments) of initial and ongoing training and development.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
1.12	For NOVAtime employees not directly engaged in application development, management provides **ongoing employee training** related to system and application enhancements and version modifications, to maintain and enhance the skill level of personnel.	Inquired of management into ongoing training and development program for employees.	No exceptions noted.
1.13	Management encourages employees to complete and continue **formal education** and technical certification programs.	Inquired of management into encouragement of employees to pursue formal education and technical certification programs to determine that management encourages employees to complete and continue formal education and technical certification programs. .	No exceptions noted.
1.14	Management-approved **professional development expenses** incurred by the employees are paid by NOVAtime.	Inquired of management to determine that management-approved professional development expenses incurred by the employees are paid by NOVAtime.	No exceptions noted.
1.15	Each new employee undergoes an **initial 90 day probationary period and performance review** to evaluate performance.	Inspected a judgmental sample of initial 90 day reviews of new employees hired during the review period to determine that each new employee undergoes an initial 90 day probationary period and review to evaluate performance.	No exceptions noted.
1.16	Each employee undergoes a **semi-annual performance review** each year. During these reviews, management reinforces and updates professional development plans for each employee.	Inspected a judgmental sample of semi-annual reviews for employees, to determine that managers discuss job objectives, goals, and career development plans for each employee.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Board of Directors Participation		
1.17	A board of directors **oversees management activities**.	Inquired of management regarding the board of directors to determine that a board of directors was in place to oversee company performance and direction.	No exceptions noted.
		Inspected the listing of the board of director members to determine that a board of directors was in place.	No exceptions noted.
1.18	The board of directors **meets on an annual basis**.	Inquired of management to determine that a board of directors meets annually.	No exceptions noted.
1.19	NOVAtime utilizes a **third party financial auditor** to audit its financial statements.	Inquired of management to determine that NOVAtime utilizes a third party financial auditor to audit its financial statements.	No exceptions noted.
	Management Philosophy and Operating Style		
1.20	NOVAtime uses an external **law firm** to keep updated with the latest employment law, **regulatory and industry changes** as needed.	Inquired of management to determine that NOVAtime uses an external law firm to keep updated with the latest employment law, regulatory and industry changes	No exceptions noted.
1.21	Management regularly attends **trade shows,** utilizes **trade and regulatory publications, journals, online news feeds and government sites**, and belongs to **industry associations** to stay current on any regulatory compliance or operational trends affecting the services provided.	Inspected a judgmental sample of trade show agendas, online sites utilized and publications, and association membership literature to determine that management is periodically briefed on regulatory and industry changes affecting services provided.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
1.22	**Management meetings** are held on a regular basis to discuss operational planning and budgeting, human resource planning and hiring, and customer related issues. Meeting agendas and meeting minutes are recorded and communicated to relevant personnel.	Inquired of management to determine that management meetings were held on a regular basis to discuss operational and customer related issues.	No exceptions noted.
1.23	Management engages an **independent CPA firm** to audit NOVAtime's financial statements on an annual basis.	Inquired of management to determine that management engages an independent CPA firm to audit NOVAtime's financial statements on an annual basis.	No exceptions noted.
		Inspected the most recent engagement letter reflecting the engagement of an independent CPA to determine that Management engages an independent CPA firm.	No exceptions noted.
	Organizational Structure, and Assignment of Authority and Responsibility		
1.24	**Organizational charts** are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to employees and are updated as needed.	Inquired of management regarding communication of organizational charts to determine that the charts are communicated to employees and updated as needed.	No exceptions noted.
		Inspected organizational charts to determine that organizational charts are in place to communicate key areas of authority and responsibility and are updated.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
1.25	**Workflow charts** are in place to communicate information about the roles of different employees. These charts are communicated to employees and are updated as needed.	Inspected workflow charts to determine that workflow charts are in place to communicate key areas of authority and responsibility and are updated as needed.	No exceptions noted.
1.26	NOVAtime's **operating goals and objectives are communicated** to the entire organization during regular staff meetings, employee performance reviews, and other written communications.	Inquired of management regarding communication of NOVAtime's operating goals and objectives to employees of organization to determine that they are communicated to the entire organization.	No exceptions noted.
		Inspected a judgmental sample of written company communications to determine that NOVAtime's operating goals and objectives are communicated to the entire organization.	No exceptions noted.
1.27	NOVAtime provides an **employee orientation program** that communicates organizational structure and responsibility, company and departmental objectives, and relationships between departments and personnel.	Inquired of management regarding the employee orientation program to determine that organizational structure, responsibility, company and departmental objectives and relationships between departments are communicated to employees during the orientation.	No exceptions noted.
		Inspected employee orientation documentation to determine that organizational structure, responsibility, company and departmental objectives and relationships between departments are communicated to employees during the orientation.	No exceptions noted.
1.28	NOVAtime has established a **segregation of duties process**, which is based upon changes and recommendations from management.	Inquired of management regarding segregation of duties process.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected the organization chart to determine that NOVAtime has established a segregation of duties process	No exceptions noted.
	Human Resource Policies and Practices		
1.29	Management has established **hiring guidelines and procedures** that guide the hiring process to ensure that specific elements of the hiring process are consistently executed.	Inspected the hiring guidelines and procedures to determine that such documentation guides the hiring process.	No exceptions noted.
1.30	Human Resources management utilizes a **new hire checklist** to ensure that specific elements of the hiring process are consistently executed. A copy of the new hire checklist is maintained in the employee file.	Inspected a judgmental sample of new hire checklists used for employees hired during the review period to determine that Human Resources management utilizes a new hire checklist for the employees and that the checklist is retained in the employee files.	No exceptions noted.
1.31	Comprehensive **background checks** are performed by an independent third party for all employees as a component of the hiring process. These background checks include but are not limited to: • Criminal records (federal and county) • Credit report.	Inspected completed background checks for a judgmental sample of employees hired during the review period to determine that background checks are performed by an independent third party, and that they include: • Criminal records (federal and county) • Credit report.	No exceptions noted.
1.32	Management has developed a detailed **employee handbook** that communicates human resource policies and practices.	Inspected employee handbook that communicates human resource policies and practices.	No exceptions noted.

MATRIX 1 CONTROL ENVIRONMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that discipline and structure are an essential part of the culture and operations within the organization and also influence the control awareness of its management and employees.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
1.33	NOVAtime utilizes a **formal training program** for each new employee. Ongoing training is also utilized for each employee on an as-needed basis beyond the initial hiring training period.	Inspected a judgmental sample of documented training programs for new and tenured employees to determine that ongoing training is utilized for each employee on an as-needed basis beyond the initial hiring training period.	No exceptions noted.
1.34	Management conducts **performance evaluations** and career development discussions with each employee on an initial 90 day, and thereafter, semi-annual basis. A formal evaluation form is prepared, and is maintained in employee's HR file.	Inspected the evaluation forms for a judgmental sample of employees to determine that management performed evaluations after 90 days for new hires, and semi-annually for each employee.	No exceptions noted.
1.35	Management has established **employee termination procedures** that guide the termination process.	Inspected the employee termination procedures, to determine that they are used to guide the termination process.	No exceptions noted.
1.36	Human Resources management utilizes a **termination checklist** to ensure that specific elements of the termination process are consistently executed. This includes but is not limited to the terminated employee's physical and logical access to company facilities and computer systems. The checklist is retained in the employee files.	Inspected a judgmental sample of termination checklists utilized during the review period, to determine that Human Resources management utilizes a termination checklist to ensure that specific elements of the termination process including access removal are consistently executed, and that the checklists are retained in the employee files.	No exceptions noted.

MATRIX 2 PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	THIRD PARTY COLOCATION FACILITY		
2.1	NOVAtime utilizes the services and controls of CenturyLink Technology Solutions for housing critical production computer servers, applications, and networking equipment.	Inspected Service Level Agreement to determine that NOVAtime utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking equipment.	No exceptions noted.
	CenturyLink's summarized physical and environmental security controls are described in Section 5, as included in their SOC 1-SSAE 16 Type II report for the period July 1, 2014 to June 30, 2015.	Inspected the SOC 1-SSAE 16 report for CenturyLink for the review period July 1, 2014 to June 30, 2015.	No exceptions noted.
	PRIMARY CORPORATE LOCATION		
	Facility Access		
2.2	After-hours employee **access into the building** housing the corporate suite and elevators to suite is restricted by a **proximity card** access system managed by the building owner.	Observed the access system at the facility to determine that access into the facility is restricted by a proximity card access system.	No exceptions noted.
2.3	Employee **access into the corporate suite** is restricted by a **proximity card** access system managed by NOVAtime, with variable access rights granted by management. All accesses are **logged** by the system, and stored in digital format for ad hoc review. All employees are required to carry their badges while in the Corporate facility.	Observed the access system for the corporate suite to determine that access into the suite is restricted by a proximity card access system.	No exceptions noted.

MATRIX 2 PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected a judgmental sample of printouts of logged accesses to determine that all accesses are logged and stored in digital format for ad hoc review.	No exceptions noted.
		Inspected the access rights listing to determine that access into and within the facility is restricted, with variable access rights granted by management.	No exceptions noted.
		Observed attempt to access restricted area with a proximity card not authorized to access that area to determine that variable rights are in effect.	No exceptions noted.
		Inquired of management to determine that access rights are granted based on a “least privilege” basis.	No exceptions noted.
		Inquired of management to determine that all employees are required to carry their badges while in the Corporate facility.	No exceptions noted.
2.4	The **employee termination process** includes the removal of the terminated personnel’s ability to gain access to the facility, including deactivation and retrieval of all electronic access means. This process is documented in the termination checklist.	Inquired of management to determine that electronic access is deactivated and proximity cards and physical keys are retrieved where possible.	No exceptions noted.
		Inspected the proximity card access control list to determine that management deactivated electronic access privileges to a judgmental sample of previously terminated employees as a component of the termination process.	No exceptions noted.

MATRIX 2 PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected a judgmental sample of termination checklists for any employees terminated during the review period to determine that this process is documented in the checklist.	No exceptions noted.
	Visitor Access		
2.5	**Visitors** to the company facility may only enter through the main entrance, where access is monitored at the **manned reception desk**. Visitors cannot gain access via other entrances. A remote entry button allows non-employees to be allowed entry through the front door once they have identified themselves.	Observed the manned front reception desk to determine that access to the facility through the main entrance is monitored and controlled.	No exceptions noted.
		Observed other entrances to determine that they are kept locked during business and after hours.	No exceptions noted.
		Observed remote entry button to determine that a remote entry button allows non-employees to enter through the front door once they have identified themselves.	No exceptions noted.
	Server Room Access		
2.6	The server room is equipped with an access security system requiring a **proximity card** for entry, with a physical key override for power outages.	Observed access into the server room to determine that access to the server room was equipped with an access security system requiring a proximity card for entry, with a physical key override for power outages.	No exceptions noted.

MATRIX 2 PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
2.7	**Access privilege** to the server room is granted to approved management and support personnel only. ***Security in Corporate Suite***	Inspected the server room access privileges to determine that access is granted to approved management and support personnel only.	No exceptions noted.
2.8	**CCTV surveillance cameras** are in place to monitor the interior and exterior premises of the facilities on a 24x7x365 basis. • Video data is recorded and archived for future use. • The system is tied into **motion sensors**, which triggers event driven recording. • Some of the surveillance cameras have **night vision capability**, where necessary.	Observed the surveillance cameras utilized on the interior and exterior of the facilities to determine that surveillance cameras are utilized within the facilities.	No exceptions noted.
		Inspected a judgmental sample of video data from the facility to determine that it is recorded and stored for future use, and that motion sensors trigger event-driven recording.	No exceptions noted.
		Inspected a judgmental sample of video data to determine that some of the surveillance cameras have night vision capability, where necessary.	No exceptions noted.
2.9	Video images from the surveillance cameras are **stored** to DVR for approximately two weeks. By policy, video related to any incident would be stored indefinitely.	Inspected a judgmental sample of video data from the office and data center facility to determine that it is recorded and stored for future use DVR for approximately two weeks.	No exceptions noted.

MATRIX 2 PHYSICAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage, and interference.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inquired of the facilities specialist to determine that video images from the surveillance cameras related to any incident would be stored indefinitely.	No exceptions noted.
	Server Room Security		
2.10	Server room **walls** extend from the physical floor to the physical ceiling structure.	Observed server room walls to determine they extend from the physical floor to the physical ceiling structure.	No exceptions noted.
2.11	All walls surrounding the server room are **fire rated walls**.	Inquired of facilities personnel to determine that all walls surrounding the server room are fire rated.	No exceptions noted.
2.12	The server room **doors are self-closing**.	Observed the server room doors to determine that they were self-closing.	No exceptions noted.
2.13	No **windows** to the exterior exist within the server room.	Observed server room to determine that no windows to the exterior exist.	No exceptions noted.

MATRIX 3 ENVIRONMENTAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	THIRD PARTY COLOCATION FACILITY		
3.1	NOVAtime utilizes the services and controls of CenturyLink Technology Solutions for housing critical production computer servers, applications, and networking equipment.	Inspected Service Level Agreement to determine that NOVAtime utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking equipment.	No exceptions noted.
	CenturyLink's summarized physical and environmental security controls are described in Section 5, as included in their SOC 1-SSAE 16 Type II report for the period July 1, 2014 to June 30, 2015.	Inspected the SOC 1-SSAE 16 report for CenturyLink for the review period July 1, 2014 to June 30, 2015.	No exceptions noted.
	PRIMARY CORPORATE LOCATION		
	Fire Control Systems		
3.2	The primary corporate facility is protected by **fire detection and suppression controls** that include • High sensitivity smoke sensors • Heat sensors • Fire alarms (horn and strobe enunciators) • Water-based wet pipe sprinkler system in the office area • Hand-held fire extinguishers in the office facility.	Observed the fire detection and suppression controls to determine that the primary corporate facility is protected by • High sensitivity smoke sensors • Heat sensors • Fire alarms (horn and strobe enunciators) • Water-based wet pipe sprinkler system in the office area • Hand-held fire extinguishers in the office facility.	No exceptions noted.

MATRIX 3 ENVIRONMENTAL SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that critical information technology infrastructure is protected from certain environmental threats.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
3.3	A **third party inspects** the hand-held fire extinguishers on an annual basis.	Inspected the most recent inspection results to determine that a third party provider inspects the hand-held fire extinguishers on an annual basis.	No exceptions noted.
	Climate Control		
3.4	For **climate control**, the server room is equipped with dedicated redundant air conditioning units to control temperature and humidity. Both are monitored within the server room.	Observed the climate control and temperature and humidity monitoring units to determine that the server room is equipped with dedicated redundant climate control units.	No exceptions noted.
	UPS and Battery Backup Systems		
3.5	Equipment in the server room is connected to **UPS systems** to provide temporary electricity in the event of short term power outages, and to mitigate the risk of power fluctuations impacting infrastructure in the server room.	Observed the UPS systems to determine that the equipment in the server room was connected to UPS systems to provide temporary electricity in the event of a power outage and mitigate the risk of power fluctuations impacting infrastructure in the server room.	No exceptions noted.
3.6	The UPS system provides approximately **three hours of backup power**.	Inquired of management to determine that the UPS system provides approximately three hours of backup power.	No exceptions noted.

MATRIX 4 COMPUTER OPERATIONS I – BACKUP AND STORAGE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of NOVAtime's and customers' critical files, storage of NOVAtime's and contracted customer's data, and retention of NOVAtime's and contracted customer backup files.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
4.1	Documented **backup procedures** are in place for company systems deemed critical by management, to guide personnel in performing backup system tasks. **Disk-to-Disk Backup of NOVAtime Internal Systems and Customer Data**	Inspected documented backup procedures on the company intranet to determine that documented backup procedures are in place for critical NOVAtime systems.	No exceptions noted.
4.2	Using **in-house SQL scripts, automated backup jobs** are utilized to perform scheduled system backups.	Inspected the SQL automated backup scripts to determine that automated backup systems are utilized to perform scheduled system backups.	No exceptions noted.
4.3	**Weekly full backups** are performed of all critical company data such as critical application and database components. Logs are used to record backup activity.	Inspected a judgmental sample of backup software logs to determine that weekly full data backups are performed of all critical NOVAtime data such as critical application and database components.	No exceptions noted.
4.4	**Differential daily backups** of all critical NOVAtime application components and databases are performed by the automated backup applications. Logs are used to record daily backup activity.	Inspected a judgmental sample of daily backup logs to determine that automated backup applications perform differential daily backup tasks of NOVAtime application components and databases.	No exceptions noted.
4.5	Production data is backed up to a **NAS** (Network Attached Storage) at the primary data center.	Inspected Configuration Management System backup storage control panel to determine that backups are made to a NAS, and that snapshots are also available directly from the NAS.	No exceptions noted.
4.6	The **retention period** for backup data is three years. Multiple NAS devices are utilized for long term archiving.	Inspected a judgmental sample of daily and weekly backup data files on NASs to determine that the retention period is three years.	No exceptions noted.

MATRIX 4 COMPUTER OPERATIONS I – BACKUP AND STORAGE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of NOVAtime's and customers' critical files, storage of NOVAtime's and contracted customer's data, and retention of NOVAtime's and contracted customer backup files.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Backup Monitoring		
4.7	**Failure notifications** of the backup process are communicated by the backup application to management and the IT Operations manager by automated email.	Inquired of management to determine that failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.	No exceptions noted.
		Inspected a judgmental sample of emailed notifications to determine that failure notifications of the backup process are communicated by the backup application to management and appropriate IT personnel by automated email.	No exceptions noted.
4.8	In addition to failure notifications, the built-in SQL Job Notification functionality is utilized to provide **backup status email notifications to the Exchange public folder.**	Inspected a judgmental sample of emailed notifications to determine that backup status notifications are emailed to the Exchange public folder.	No exceptions noted.
4.9	The backup applications generate and maintain **logs**, which specify the data backup processes are completed, and success/failure status of each process.	Inspected the backup application logs to determine that backup applications maintain logs which specify the data backup processes are completed, and success/failure status of each process.	No exceptions noted.
4.10	Management performs **systematic reviews** of the backup applications and logs to detect abnormalities in the backup process.	Inquired of management to determine that management performs systematic reviews of the backup application and logs to detect abnormalities in the backup process.	No exceptions noted.

MATRIX 4 COMPUTER OPERATIONS I – BACKUP AND STORAGE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of NOVAtime's and customers' critical files, storage of NOVAtime's and contracted customer's data, and retention of NOVAtime's and contracted customer backup files.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected a judgmental sample of backup application logs or reports to determine that management performs systematic reviews of the backup applications and logs to detect abnormalities in the backup process.	No exceptions noted.
4.11	Management periodically performs **restorations of backup data** at customer request, which also serves to verify the success of backup processes and employee readiness.	Inquired of management to determine that management periodically performs restorations of backup data at customers' request, which also serves to verify the success of backup processes and employee readiness.	No exceptions noted.
		Inspected a judgmental sample of restoration logs to determine that management periodically performs restorations of backup data at customer request, which serves to verify the success of backup processes and employee readiness.	No exceptions noted.
	Replication / Mirroring		
4.12	Certain production servers are **replicated** for redundancy. Because NOVAtime utilizes redundant web application servers in the DR site which are maintained to the current stable release, the only critical data to be replicated is the **database tier.**	Inspected the server Dell AppAssure and Tegile configurations to determine that certain database production servers are replicated for redundancy.	No exceptions noted.
4.13	**1st Generation SAN** uses a third party replication tool (Replay, by AppAssure, now owned by Dell), is utilized to perform scheduled system replication. **2nd Generation SAN** (hybrid with SSD) introduced in Dec 2013 uses Tegile's (manufacturer) built-in replication tool.	Inspected the Dell AppAssure and Tegile control panel to determine that NOVAtime utilizes a third party application for scheduled system replication.	No exceptions noted.

MATRIX 4 COMPUTER OPERATIONS I – BACKUP AND STORAGE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of NOVAtime's and customers' critical files, storage of NOVAtime's and contracted customer's data, and retention of NOVAtime's and contracted customer backup files.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
4.14	Replication of databases is made to **offsite storage for geographic redundancy**, utilizing SAN-to-SAN replication from the primary data center to the secondary (DR site) data center.	Inquired of management to determine that replication of database data is made to offsite storage for geographic redundancy, utilizing SAN-to-SAN replication.	No exceptions noted.
		Inspected the replication tool to determine that replication of database data is made to offsite storage for geographic redundancy, utilizing SAN-to-SAN replication.	No exceptions noted.
4.15	**Offsite transport** of replication data is secured at two levels: • Transport is over the private CenturyLink WAN, not over the internet. • A secure site-to-site VPN tunnel within the WAN pipe utilizes IPsec encryption to further segregate and protect data in transit.	Inspected the VPN methodology to determine that backups are performed via VPN to the offsite backup location.	No exceptions noted.
		Inspected the VPN encryption configurations to determine that the site-to-site connection utilizes IPsec encryption.	No exceptions noted.
4.16	Production data is replicated to a **SAN** (Storage Area Network). The backups are asynchronous, with point-in-time **snapshots** (recovery points) as frequently as **every 60 minutes**. These snapshots are combined with the initial full replication image to create a continuous "synthetic full" image. The snapshot images themselves are retained in the system for 12 hours.	Inspected backup storage control panel to determine that replication is made to a SAN, and that recovery points have been configured as needed, and that they are retained for 12 hours.	No exceptions noted.

MATRIX 4 COMPUTER OPERATIONS I – BACKUP AND STORAGE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of timely system backups of NOVAtime's and customers' critical files, storage of NOVAtime's and contracted customer's data, and retention of NOVAtime's and contracted customer backup files.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
4.17	NOVAtime employs **block level replication**, allowing for operating system and data restoration of any production server. Servers can be quickly rolled back to a previous virtual instance of that server environment in the event of patch related or other issues.	Inspected a judgmental sample of snapshot configurations on the backup server to determine that any production server could be quickly rolled back to a previous virtual instance of that server environment in the event of patch related or other issues.	No exceptions noted.
4.18	**Windows 2012 R2 HyperV replication** technology was introduced this year to further enhance system recoverability via manual failover.	Inspected HyperV control panel to determine that Windows 2012 R2 HyperV replication technology was introduced this year to further enhance system recoverability via manual failover.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.1	**Policies and procedures** are in place to govern critical computer operations activities.	Inspected the policies and procedures to determine that policies and procedures are in place to govern critical computer operations activities.	No exceptions noted.
5.2	NOVAtime has a documented **disaster recovery plan.**	Inspected documented disaster recovery plan.	No exceptions noted.
5.3	A **computer incident response plan** is in place to ensure that required resources are obtained in an organized and timely manner.	Inspected the SaaS escalation incident response plan to determine that a policy is in place to ensure that required resources are obtained in an organized and timely manner.	No exceptions noted.
5.4	NOVAtime maintains **two geographically redundant data center facilities** provided by CenturyLink. The primary data center hosts NOVAtime's production network and systems, and the secondary acts as a disaster recovery (DR) site.	Inquired of management to determine that NOVAtime maintains two distinct data center facilities and that the secondary acts as a disaster recovery site for the primary data center.	No exceptions noted.
		Inspected Service Level Agreement from CenturyLink to determine that NOVAtime utilizes the services and controls of third party data centers for housing critical production computer servers, applications, and networking equipment as well as disaster recovery systems.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	System Monitoring and Response		
5.5	Management has developed NOVAtime's **definition of system downtime** and determined acceptance level criteria.	Inspected policies and procedures to determine management has developed NOVAtime's definition of system downtime and acceptance level criteria.	No exceptions noted.
5.6	**System downtime and operations issues** are monitored to help ensure that system downtime does not exceed predefined levels.	Inspected a judgmental sample of monthly metrics tracking reports to determine that system downtime and operations issues were monitored.	No exceptions noted.
5.7	As a general rule, when NOVAtime resources reach a nominal load of 50% capacity, or when there are frequent spikes above 70% of capacity, the IT department will start planning to **add more resources**.	Inquired of management to determine that resources are added when they exceed certain capacity thresholds.	No exceptions noted.
		Inspected documented Server Farm Expansion Logistics procedures to determine that a methodology is followed for server expansion.	No exceptions noted.
5.8	Third party **enterprise monitoring applications** are used to monitor and record performance criteria for critical NOVAtime server and network equipment.	Inspected the enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical NOVAtime server and network equipment.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.9	The enterprise monitoring applications functionality includes **server and port monitoring features** that provide monitoring services for critical server and network components, including: • Resource utilization • Server availability • Services availability • .NET-IIS healthiness • NOVA-specific exceptions.	Inspected the Microsoft SCOM (System Center Operations Manager) server and port monitoring applications to determine that network administrators utilize server and port monitoring applications that provide monitoring services for critical server and network components.	No exceptions noted.
5.10	Customer database **SQL behavior is also monitored** via in-house SQL agent jobs to ensure data are being processed normally.	Inspected a judgmental sample of SQL scripts to determine that customer database SQL behavior is also monitored via in-house SQL agent jobs.	No exceptions noted.
5.11	The enterprise monitoring applications and scripts are configured to send **alert notifications** to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via email or SMS text.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
5.12	All NOVAtime IT personnel are **equipped with smart phones** for use in the network and server monitoring alert process.	Observed smart phones of IT personnel to determine that network operations center personnel are equipped with smart phones for use in the network and server monitoring alert process.	No exceptions noted.
5.13	NOVAtime provides on call IT **personnel** on a 24/7/365 basis for server and network performance monitoring.	Inquired of management to determine that NOVAtime IT personnel are provided on an on-call basis for server and network performance monitoring.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Hardware and Maintenance		
5.14	A helpdesk **ticketing system** is utilized to manage systems **infrastructure issues**. Tickets are assigned to support personnel based on the nature of the ticket.	Inspected a judgmental sample of logs from the SpiceWorks ticketing system showing closed tickets to determine that a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on the nature of the ticket.	No exceptions noted.
5.15	**Routine network maintenance** is scheduled by the third party data center at early morning weekend hours, and email ticketing notification is automatically generated to NOVAtime IT personnel.	Inspected a judgmental sample emails from the third party data center ticketing system to determine that routine network maintenance is scheduled by the third party data center at early morning weekend hours, and email ticketing notification is automatically generated to NOVAtime's IT personnel.	No exceptions noted.
5.16	A **standard hardware build** is utilized for installation and maintenance of certain critical NOVAtime servers.	Inspected the standard hardware build procedures on the company intranet for certain NOVAtime servers to determine that a standard hardware build is utilized for certain critical NOVAtime servers.	No exceptions noted.
5.17	A **standard virtualization template** for virtualized environments is utilized for installation and maintenance of certain critical NOVAtime virtual machines.	Inspected the Hyper V configurations to determine that a standard template is used for installation and maintenance of certain critical NOVAtime virtual machines.	No exceptions noted.
		Inspected the internal configuration management utility to determine that templates and methodologies are in place for quick spin up of new virtual machines.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected virtualization spin up methodology in Server Build From Image in Sharepoint to determine that procedures are in place for quick spin up of new virtual machines.	No exceptions noted.
5.18	NOVAtime maintains **redundant servers** for critical production applications.	Inquired of management to determine that NOVAtime maintains redundant servers for critical production applications.	No exceptions noted.
		Observed redundant system infrastructure in network diagram and the network configuration documentation to confirm server redundancy for critical production applications.	No exceptions noted.
5.19	**Redundant architecture** is built into the *network systems* infrastructure, including, but not limited to the: • Routers and switches, all in active-standby pairs • Firewalls • Load balancers.	Observed the redundant system infrastructure components to determine that redundant architecture was built into certain aspects of the systems infrastructure.	No exceptions noted.
5.20	**Redundant architecture** is built into the individual physical server infrastructure, including, but not limited to the: • Network interface cards (NICs) • Power supplies • RAID storage • Dual storage controllers on the SAN for SQL devices.	Inspected a judgmental sample of server build quotes to determine that redundant architecture was built into certain aspects of the systems infrastructure.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.21	All servers feature hardware **RAID (1, 5, or 10)** allowing for hard disk drive failure without a server outage. Hot swap technology is also utilized to provide zero downtime operation for the most common type of hardware failure.	Inspected a judgmental sample of servers to determine the use of RAID drives and hot swap technology.	No exceptions noted.
5.22	NOVAtime utilizes **load balancers** configured in an active-active mode to not only minimize system down time, but also improve performance.	Inspected A10 Networks load balancer monitoring application to determine that NOVAtime utilizes load balancers to not only minimize system down time, and that automatic failover is configured.	No exceptions noted.
5.23	**Redundant internet connections** are in place through multiple providers into the data center, and multiple routers and switches are utilized.	Inspected network diagram to determine that redundant internet connections are in place, through multiple providers with separate entrances into the physical building, and that multiple routers and switches are used.	No exceptions noted.
5.24	Multiple **internet** connections provide **fail over redundancy,** set up in an active-passive configuration. In the event of failover, the enterprise monitoring system sends alert notifications.	Inspected the in the firewall control panel configurations to determine that multiple internet connections provide failover redundancy, and that in the event of fail over, the enterprise monitoring system sends alert notifications.	No exceptions noted.
5.25	NOVAtime subscribes to a third party **service that checks its Web application and services** with agents from different parts of the country, and provides alerts when response time exceeds predefined thresholds.	Inspected the Webmetrics application monitoring control panel to determine that NOVAtime subscribes to a third party service that checks its Web application and services with agents from different parts of the country	No exceptions noted.
		Inspected a judgmental sample of alerts to determine that they are sent by the monitoring application when response time exceeds predefined thresholds.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.26	Critical production equipment is maintained under **warranty** and maintenance or Service Level Agreements (SLAs) with 3rd party vendors.	Inquired of management to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.	No exceptions noted.
		Inspected a judgmental sample of agreements with third party vendors to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.	No exceptions noted.
	OS and Software Patches: (NOVAtime Servers)		
5.27	An automated methodology is utilized to **monitor patch releases**, distribute patches to relevant devices and apply the patches to the device. WSUS (Windows Server Update Services) is managed through a central server, which pushes patch updates to individual servers pending evaluation before manual application to the servers.	Inquired of management to determine that a methodology is utilized to monitor patch releases, distribute patches to relevant devices and apply the patches to the device.	No exceptions noted.
5.28	Infrastructure changes, patches and upgrades to critical services are **tested** by the Quality Assurance and IT departments before being applied to a production server.	Inquired of management to determine that infrastructure changes, patches and upgrades to critical services are tested by the Quality Assurance and IT departments after hours before being introduced to a production server.	No exceptions noted.
		Inspected hardware update logs to determine that patches and upgrades to critical services are tested by the Quality Assurance and IT departments before being introduced to a production server.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
5.29	A **test environment** at the corporate office is utilized on secondary servers, to ensure that patches and upgrades to critical services can be tested before being introduced to a production server.	Inquired of management to determine that a test environment is utilized on secondary servers, to ensure that patches and upgrades to critical services can be tested before being introduced to a production server.	No exceptions noted.
		Observed test servers at the corporate office and network diagram to determine that a server test environment is utilized before patch introduction to production servers.	No exceptions noted.
	Anti-virus Software: (NOVAtime Internal Domain Servers)		
5.30	Third party **antivirus software** is installed on all pertinent external facing NOVAtime servers **(endpoint protection).**	Inquired of management to determine that third party antivirus software is installed on all pertinent external facing NOVAtime servers.	No exceptions noted.
		Inspected Trend Micro antivirus software installed on judgmental sample of NOVAtime servers to determine that antivirus software is installed on all external facing NOVAtime servers.	No exceptions noted.
5.31	Antivirus applications are **managed by a central antivirus server** on a daily basis. Updates are pushed to specific production servers on a daily basis.	Inspected the antivirus system's update settings to determine that a central server monitored for updates to antivirus definitions on a daily basis.	No exceptions noted.
		Inspected the list of servers configured to receive updates from the central antivirus server to determine that antivirus software was installed on specific production servers.	No exceptions noted.

MATRIX 5 COMPUTER OPERATIONS II – SYSTEM UPTIME AND MAINTENANCE

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the computer systems are maintained in a manner that helps ensure customer system availability.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected the antivirus settings for frequency that updates are pushed to production servers to determine that updates were pushed to specific production servers on a daily basis.	No exceptions noted.
5.32	Antivirus **definition updates** are performed by the perimeter antivirus application on a daily basis.	Inspected AV software configuration to determine that antivirus definition updates are performed on a daily basis.	No exceptions noted.
	Company Workstations and Laptops		
5.33	An **automated methodology** is utilized for managing workstations, using a dedicated WSUS server (Windows Server Update Service).	Inspected WSUS configurations to determine that an automated methodology is utilized to roll out workstation updates.	No exceptions noted.
5.34	Third party **antivirus software** is installed on all NOVAtime workstations and laptops **(endpoint protection).** The software is currently licensed.	Inquired of management to determine that third party antivirus software is installed on all NOVAtime servers.	No exceptions noted.
		Inspected Trend Micro antivirus software installed on judgmental sample of NOVAtime workstations and laptops to determine that antivirus software is installed on all NOVAtime workstations and laptops and is currently licensed.	No exceptions noted.

MATRIX 6 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion. Procedures are also in place to keep authentication and access mechanisms effective.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	General Access Controls		
6.1	Management has **documented information security policies and procedures** to communicate corporate security standards to employees.	Inspected the information security policies to determine that management documented information security policies to communicate corporate security standards to employees.	No exceptions noted.
6.2	Management has **segregated specific duties** within the production environment for administering critical areas such as: • Network administration • Systems administration (including Active Directory) • Database administration • Development.	Inspected access rights listing to determine that management has segregated specific duties within the production environment for administering critical areas.	No exceptions noted.
6.3	**Network diagrams** are in place and communicated to appropriate personnel.	Inspected network diagrams to determine that network diagrams are in place and communicated to appropriate personnel.	No exceptions noted.
6.4	Management utilizes **vulnerability assessment tools (VAT)** to help determine vulnerability risks.	Inspected the Pscan vulnerability assessment tools, configurations and test reports generated to determine that management utilizes vulnerability assessment tools to help determine vulnerability risks.	No exceptions noted.
6.5	Management periodically performs **internal security assessments,** including reviews of server logs and other critical items. All servers have Security Audit functionality turned on.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.	No exceptions noted.

MATRIX 6 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion. Procedures are also in place to keep authentication and access mechanisms effective.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected active directory default domain policy to determine that all servers have this functionality turned on.	No exceptions noted.
6.6	NOVAtime periodically utilizes an external provider to perform system **third party security audits.**	Inspected the most recent results from the Plynt Security Certification audit performed during the review period to determine that NOVAtime periodically utilizes an external provider to perform system third party security audits.	No exceptions noted.
6.7	The production network is **logically and physically segregated** from the internal corporate network.	Inspected network diagram topology to determine that the production network was logically and physically segregated from the internal corporate network.	No exceptions noted.
6.8	NOVAtime provides **no wireless access points** or support within the production environments. Only physical access when visiting the data center or remote VPN access is allowed.	Inquired of management and inspected the network diagram to determine that NOVAtime provides no wireless access points or support within the production environments, and that only physical access when visiting the data center or remote VPN access is allowed.	No exceptions noted.
	Production Network Domain – Network Authentication Controls Via Windows Active Directory		
6.9	Users are required to authenticate via a unique user **ID and password** before being granted access to NOVAtime production network domain. No shared accounts are currently in use. Passwords are masked upon entry.	Inspected the production network domain (NOVASAAS) authentication process to determine that users are required to authenticate via a unique user ID and password before being granted access to NOVAtime production network domain, and that passwords are masked upon entry.	No exceptions noted.

MATRIX 6 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion. Procedures are also in place to keep authentication and access mechanisms effective.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inquired of management to determine that no shared accounts are currently in use.	No exceptions noted.
6.10	Internal network domain (default domain in production) **passwords must conform** to the following requirements: • Enforce password history • Maximum password age • Minimum password age • Minimum password length • Complexity requirement enabled. **Production Network Domain – Network Access and Monitoring Controls**	Inspected the network authentication configurations to determine that network domain (NOVASAAS) passwords must conform to stated requirements.	No exceptions noted.
6.11	• Production database and application server **operating system account policies** are controlled by the production domain group policy. • A separate Active Directory domain is used for non-production, internal corporate servers and applications.	Inquired of the network administrator regarding operating system account policies to determine that database and application server operating system account policies were controlled by the production domain group policy.	No exceptions noted.
		Inspected a judgmental sample of application and database server configurations to determine that the database and application server operating system account policies were controlled by the production domain group policy.	No exceptions noted.

MATRIX 6 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion. Procedures are also in place to keep authentication and access mechanisms effective.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected internal domain access and authentication policies to determine that a separate Active Directory domain is used for non-production, internal corporate servers and applications.	No exceptions noted.
6.12	There is no direct access to production servers. Authenticated **VPN sessions can only access IT Ops Management consoles**, which are on a separate VLAN from the production servers themselves. Further access to the servers themselves is controlled via Active Directory.	Observed the process of accessing production servers to determine that VPN sessions can only access IT consoles, and that further access to the servers themselves is controlled via Active Directory.	No exceptions noted.
		Inspected network diagram to determine that the IT consoles are on a separate VLAN from the production servers.	No exceptions noted.
6.13	Management has **segregated specific duties** within the production environment for administering critical areas such as network administration and database management.	Inquired of management to determine that management has authorized specific personnel to administer information security within the production environment, and has segregated duties.	No exceptions noted.
		Inspected the administrative access rights listing to confirm that management has authorized specific personnel to administer information security within the production environment, and has segregated specific duties within the production environment for administering critical areas such as network administration, and database management.	No exceptions noted.

MATRIX 6 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion. Procedures are also in place to keep authentication and access mechanisms effective.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
6.14	Users are assigned to **pre-defined roles and access rights** within all NOVAtime systems. • **Access** to sensitive production server directories and files is restricted based on job responsibilities. • Users are granted **variable access rights** according to a rights authorization methodology. • Access to systems is granted on a **"least privilege"** basis, with employees acquiring access only to those systems necessary to perform their job functions.	Inquired of management to determine that users are assigned to pre-defined roles and access rights within all NOVAtime production systems and that variable rights are assigned based on job responsibilities and least privilege.	No exceptions noted.
		Inspected the access rights listing to determine that users are assigned to pre-defined roles and access rights within all NOVAtime production systems.	No exceptions noted.
6.15	Management **revokes** server access privileges assigned to terminated employees as a component of the employee termination process. If there is a need to maintain the account, the password will be changed for the direct supervisor and left active.	Inquired of management to determine that management revokes server access privileges assigned to terminated employees as a component of the employee termination process. If there is a need to maintain the account, the password will be changed for the direct supervisor and left active.	No exceptions noted.
		Inspected the production server access rights listing to determine that management revoked server access privileges assigned to previously terminated employees as a component of the employee termination process.	No exceptions noted.
6.16	The servers **log certain server-level events** for ad hoc auditing and review purposes.	Inquired of management to determine that the server logs certain server-level events for ad hoc auditing and review purposes.	No exceptions noted.

MATRIX 6 INFORMATION SECURITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion. Procedures are also in place to keep authentication and access mechanisms effective.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected a judgmental sample of server logs to determine that the server logs certain server-level events for ad hoc auditing and review purposes.	No exceptions noted.
	Hosted User Application - Application Authentication and Access Controls		
6.17	Application users are required to **authenticate** via an authorized unique user ID and password before being granted access to the production environment. No shared accounts are currently in use. Passwords are masked upon entry.	Inspected logon screens to determine that application users were required to authenticate via an authorized unique user ID and password before being granted access to the production environment, and that passwords are masked upon entry.	No exceptions noted.
		Inquired of management to determine that no shared accounts are currently in use.	No exceptions noted.
6.18	Within the application, **client's designated application Administrator** can configure for standard or strong password.	Inspected the hosted user application authentication configurations to determine that passwords are configured by client's administrators.	No exceptions noted.
6.19	**Security groups** are utilized to manage access privileges within the hosted user application.	Inspected a judgmental sample of security groups and access privileges to determine that security groups were utilized to manage access privileges within the hosted user application.	No exceptions noted.
6.20	Certain **application events are logged** by the application and maintained for management review.	Inspected application logs to determine that certain system/configuration change events were logged and maintained for management review.	No exceptions noted.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to NOVAtime's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
7.1	Documented **policies and procedures** are in place, which govern critical data communication activities.	Inspected policies and procedures which govern critical data communication activities to determine that documented policies and procedures are in place, which govern critical data communication activities.	No exceptions noted.
7.2	IT personnel subscribe to **informational services** and are notified of recent attacks and vulnerabilities.	Inspected a sample of SANS and Microsoft Security Advisory informational services communications to determine that IT personnel subscribe to informational services and are notified of recent attacks and vulnerabilities.	No exceptions noted.
	Data Transfer Methodology and Encryption Between NOVAtime and Customers		
7.3	Customers access the NOVAtime service from an internet browser, using HTTPS connections (**SHA-2 SSL certificates with RSA 2048 encryption key)**. Customers can only access the web cluster on the load balancers.	Observed the customer access process to determine that HTTPS connections are utilized.	No exceptions noted.
		Inspected the web application SHA-2 SSL certificates to determine that transaction processing performed on web-based applications is secured through the use of the Secure Socket Layer (SSL) protocol, and that licensing is current.	No exceptions noted.
		Observed the NAT topology in the production firewalls to determine that customers can only access the web cluster on the load balancers.	No exceptions noted.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to NOVAtime's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
7.4	Even **time keeping data** (configuration, schedules etc.) from the customers' time-punching clocks communicate via HTTPS to upload punches at job sites. (Straight HTTP is used for some customers' legacy clocks.)	Inspected the production firewall ACLs to determine that time data transport is made over HTTPS ports unless a customer legacy system requires the use of HTTP.	No exceptions noted.
7.5	For **data import** (such as employee rosters), NOVAtime connects to client's **SFTP** server to retrieve the data over encrypted connections. Each customer has a separate database, stored on the SAN (Storage Area Network).	Inspected the SAN virtualization configurations to determine that each customer has a separate database on the SAN.	No exceptions noted.
		Inspected the SFTP configuration to determine that remote import file access by NOVAtime is secured by SFTP connection to file servers.	No exceptions noted.
7.6	For **outbound** data back to customers, an application **Task Scheduler feature** allows each customer to schedule reports to be generated to be automatically emailed, or generated and picked up by the customer from their report repository. There is no need for pre-defined/scheduled data transmission to and from the customer.	Inspected the Task Scheduler feature and configurations to determine that customers can utilize a Task Scheduler feature, and that reports can be scheduled for automatic email or deposit in the customer's folder in the Report Repository.	No exceptions noted.
7.7	The NOVAtime functionality includes the ability to re-calculate and re-post data when **discrepancies** due to pay policy or rule setup are detected. Punches can be over-written by Supervisors to adjust the timesheets to correctness.	Inspected the NOVAtime functionality to determine that discrepancies lead to re-calculation and re-posting.	No exceptions noted.
		Observed the over-writing process to determine that application functionality includes this ability.	No exceptions noted.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to NOVAtime's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
7.8	NOVAtime utilizes the underlying transmission protocol's data **integrity check** to detect discrepancies in transit. ***Firewall*** *systems are in place to screen data flow between external parties and the NOVAtime network. Firewalls are comprised of commercial software products that utilize stateful packet inspection technologies. All inbound and outbound data packets on all interfaces are intercepted and inspected. Packets that are not explicitly permitted by the security policy definition are rejected.* **Production Firewall System Administration**	Inquired of management to determine that NOVAtime utilizes the underlying transmission protocol's data integrity check to detect discrepancies in transit.	No exceptions noted.
7.9	The firewall requires **two levels of authentication** before administrative access to the firewall system is allowed.	Observed the network engineer log into the firewall system to determine that the firewall required two levels of authentication before administrative ("enabled") access to the firewall system was allowed.	No exceptions noted.
7.10	All firewall administrator accounts have been **changed from their default IDs.**	Inspected the administrator account ID configurations to determine that all firewall administrator accounts have been changed from their default IDs	No exceptions noted.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to NOVAtime's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
7.11	The **ability to modify** the firewall system software, configurations or rule sets is **restricted** based on job responsibility, and is limited to approved positions only.	Inspected firewall system access documentation to determine that the ability to modify the firewall system software, configuration or rule sets is restricted based on job responsibility and is limited to approved positions only.	No exceptions noted.
7.12	Firewall **modifications** to rule sets and configurations are **saved to archive** for forensic comparison to current configurations if necessary, and are available for ad hoc review by security personnel.	Inquired of management to determine that all modifications to the firewall system software, configurations or rule sets are saved and available for ad hoc review by security personnel.	No exceptions noted.
		Inspected a judgmental sample of logs of modifications to the firewall system software, configurations or rule sets to determine that they are stored	No exceptions noted.
7.13	Firewalls are configured to **log all potentially malicious activity**, and logs are available for ad hoc review by security personnel.	Inspected the firewall system configuration and sample syslog server logs to determine that firewalls are configured to log all malicious activity.	No exceptions noted.
	Firewall Utilization		
7.14	Hardware based **firewalls and routers** are placed at all network perimeter and third-party entry points to NOVAtime networks.	Inspected the network diagram, router security policy, and firewall system rule sets to determine that hardware based firewalls and routers are placed at all network perimeter and third party entry points to NOVAtime networks.	No exceptions noted.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to NOVAtime's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected firewall configurations to determine that hardware-based firewalls and routers are placed at all network perimeter and third-party entry points to NOVAtime networks	No exceptions noted.
7.15	**Multiple firewalls** are utilized for **redundancy.** The firewalls are set up in an **active/passive** configuration with automatic failover in the event of failure of the primary.	Inspected the network diagram to determine that multiple firewalls are setup for redundancy.	No exceptions noted.
		Inspected the firewall rule sets and failover configurations to determine that they are set up in a failover configuration.	No exceptions noted.
7.16	Firewall configurations **filter internet traffic** based on content and destination site address. The configurations include: • The firewall performs **stateful packet inspection.** • **Network Address Translation (NAT) and PAT** services are enabled on all network firewalls to hide internal servers. • Firewall **ports are configured** to allow only specific types of traffic between certain destinations. All unused ports on the firewall are blocked. • The firewall is **configured to deny** all traffic that is not specifically authorized in the rule set.	Inspected firewall configurations to determine that firewall configurations filter internet traffic based on content and destination site address, and that the firewall performs stateful packet inspection.	No exceptions noted.
		Inspected the firewall configuration to determine that the NAT and PAT services are enabled on all network firewalls.	No exceptions noted.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to NOVAtime's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected the firewall system configuration to determine that firewalls are configured to allow only specific types of traffic between certain destinations, and that unused ports are disabled.	No exceptions noted.
		Inspected the firewall rule sets to determine that the firewall was configured to deny traffic that was not specifically authorized in the rule set.	No exceptions noted.
7.17	Firewall **Access Control Lists** (ACLs) are set up to limit access. These include: • **IP address filtering** (IP white listing) is used in the firewall to restrict network access from outside of the network to only known personal computers. • Firewalls are programmed with **anti-spoofing** access lists to prevent spoof attacks by blocking incoming traffic pretending to originate from internal IPs.	Inspected the firewall access lists to determine that firewall access lists (IP white lists) are utilized for filtering traffic into the network.	No exceptions noted.
		Inspected a firewall access control list to determine that routers were programmed with anti-spoofing access lists to prevent spoof attacks.	No exceptions noted.
7.18	Protection against **network attacks like DDOS** were enabled at the **load balancers** where Internet traffic terminates.	Inspected load balancer configurations to determine that protection against network attacks like DDOS were enabled at the load balancers where Internet traffic terminates.	No exceptions noted.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to NOVAtime's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
7.19	**VLAN**s (Virtual Local Area Networks) have been established through the use of switches / firewalls, segregating the following networks from each other: • Internal Network (Management, Backup and Monitoring) • Production Servers • Production SAN	Inspected network diagram to determine that VLANs have been established through the use of firewalls, segregating the following networks from each other: • Internal Network (Management, Backup and Monitoring) • Production Servers • Production SAN	No exceptions noted.
	Remote Access and Remote PC Emulation		
7.20	A **secure VPN** (Virtual Private Network) connection is used for remote external access to the internal network by authorized NOVAtime employees and consultants.	Inquired of management to determine that a secure VPN is used for remote connection to the network by authorized NOVAtime employees and consultants.	No exceptions noted.
7.21	VPN tunnels utilize the **IPsec** network layer **encryption protocol** to protect customer and NOVAtime data in transit.	Inspected the VPN encryption certificates to determine that VPN tunnels utilize the IPsec network layer encryption protocol to protect customer and NOVAtime data in transit.	No exceptions noted.
7.22	**Virtual Private Network (VPN)** remote access requires a valid user ID and password for authentication.	Observed the VPN login process to determine that the VPN remote access required a user ID and password for authentication.	No exceptions noted.
7.23	There is no direct access to production servers. Authenticated **VPN sessions can only access IT consoles**, which are on a separate VLAN from the production servers themselves. Further access to the servers themselves is controlled via Active Directory.	Observed the process of accessing production servers to determine that VPN sessions can only access IT consoles, and that further access to the servers themselves is controlled via Active Directory.	No exceptions noted.

MATRIX 7 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the security infrastructure and practices secure against unauthorized access to NOVAtime's internal network and threats from connections to external networks are limited.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
		Inspected network diagram to determine that the IT consoles are on a separate VLAN from the production servers.	No exceptions noted.
7.24	An **RDP connection** (Microsoft's Remote Desktop Protocol) connection is used for remote connection to the network by authorized NOVAtime employees.	Inquired of management to determine that a RDP connection is used for remote connection to the network by authorized NOVAtime employees.	No exceptions noted.
		Observed logon process to determine that connection to the production network must first be made through an AES-encrypted VPN connection.	No exceptions noted.
7.25	NOVAtime provides **no wireless access points** or support **within the production environment**. Only physical access when visiting the data center or remote VPN access is allowed.	Inquired of management and inspected the network diagram to determine that NOVAtime provides no wireless access points or support within the production environments, and that only physical access when visiting the data center or remote VPN access is allowed.	No exceptions noted.
7.26	Onsite employees, customers and visitors can utilize a **corporate office wireless access point** (WAP) located on a stand-alone network. This WAP only allows access to the internet, with no direct access to the internal company network. The WAP utilizes WPA2 encryption.	Inquired of management regarding the corporate office wireless access point to determine that it is located on a stand-alone network, and that access is limited to the internet.	No exceptions noted.
		Inspected the network diagram to determine that the WAP only allows access to the internet, with no direct access to the internal company network.	No exceptions noted.
		Inspected the WAP configuration settings and encryption certificates to determine that the WAP utilizes WPA2 encryption.	No exceptions noted.

MATRIX 8 APPLICATION DEVELOPMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to production application code and systems are properly authorized, tested, approved, implemented and documented.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
	Change Request Initiation and Control *NOVAtime provides an online SaaS (Software as a Service) application for time management. The application is NOVAtime SaaS. Its baseline code is developed through the use of several programming languages, including ASP.NET, VB .NET, C/C++, C#.NET and javascript.* *Development and QA testing tasks are performed at corporate headquarters in Diamond Bar, California. Updates to production are made via IPSec encrypted VPN connections with servers at the production facility at the CenturyLink Technology Solutions data center in Irvine, California.*		
8.1	Documented **policies and procedures** are in place to centrally maintain, manage and monitor application development, maintenance and documentation activities.	Inspected the Change Management documentation and flowcharts to determine that a documented process is utilized to centrally maintain, manage and monitor application development and maintenance activities.	No exceptions noted.
8.2	A **change management form** is completed by an R&D member (Requestor) before submission for management approval, utilizing the in-house CRM to document: • Risk assessment for the change • Change description • Reason for change • Test plan and • Backout procedure.	Inspected a judgmental sample of Change Control forms from the review period to determine that a change management form is completed before submission for management approval.	No exceptions noted.

MATRIX 8 APPLICATION DEVELOPMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to production application code and systems are properly authorized, tested, approved, implemented and documented.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
8.3	Change Control proposals must be reviewed, prioritized and **properly approved** by the Change Control Board based on business needs and resource availability, and assigned to personnel for action before core changes are made to production application code. **Application Development**	Inspected a judgmental sample of Change Control forms from the review period to determine that they are approved before the change was applied to production code.	No exceptions noted.
8.4	Program development is performed in a distinct development environment that is **physically and logically separated from the production environment.** Development takes place on developers' **local machines**.	Inspected the location of the servers for each environment to determine that development environment is physically separated from the production environment.	No exceptions noted.
		Inspected network diagram to determine that development and test environments are logically separated from the production environment.	No exceptions noted.
		Inspected the checkout process from the version control software and a judgmental sample of local development machines to determine that development takes place on developers' local machines.	No exceptions noted.
8.5	NOVAtime **classifies 3 major types of changes** for the SaaS application; • Bug Fixes • Enhancements • New Features.	Inquired of management to determine that NOVAtime classifies 3 major types of changes for the SaaS application.	No exceptions noted.

MATRIX 8 APPLICATION DEVELOPMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to production application code and systems are properly authorized, tested, approved, implemented and documented.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
8.6	Management has **documented coding standards** and procedures and a data dictionary to guide coding activities throughout the code development process. Developers are required to adhere to these documented coding standards.	Inspected the documented coding standards to determine that coding standards are documented and utilized to guide coding activities.	No exceptions noted.
8.7	**Version control software** (Microsoft Team Foundation Server, "TFS") is utilized to maintain and control access to current and prior versions of application source code, and the associated reporting and logging functions.	Inspected and observed the version control software to determine that version control software is utilized to maintain and control access to current and prior versions of application code.	No exceptions noted.
8.8	**Logs** are utilized to maintain and record changes to manage and monitor development and maintenance activities.	Inspected a sampling of logs to determine that logs are utilized to maintain and record changes to manage and monitor development and maintenance activities.	No exceptions noted.
8.9	Changes to source code results in the creation of a new version of the application code. If necessary, changes **can be rolled back to prior versions** of the application code.	Inspected a judgmental sample of versioning history to determine that changes to source code resulted in the creation of a new version of the application code.	No exceptions noted.
8.10	**Administrative access to the application code** and directories where application executables are stored (i.e. other than read-only) is restricted within the version control software. Administrative responsibilities are limited to the following positions: • R&D Manager • Team Foundation Administrator • System Architect.	Inspected the version control software user access list to determine that management restricts access (other than read-only) to the application code within the version control software, based on Project assignment	No exceptions noted.

MATRIX 8 APPLICATION DEVELOPMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to production application code and systems are properly authorized, tested, approved, implemented and documented.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
8.11	In-house proprietary **change management software** (NOVAtime CRM CC [Change Control] Module) is utilized to manage application changes, and the associated reporting and logging functions.	Inspected and observed the CC application to determine that change management software is utilized to manage application changes, and the associated reporting and logging functions.	No exceptions noted.
8.12	Custom developed tools and reports are utilized to manage and **document development and maintenance activities** through the development and test stages.	Inspected custom developed tools (in-house CRM application) and reports to determine that tools and reports were utilized to manage and document development and maintenance activities through the development and test stages.	No exceptions noted.
8.13	Management utilizes application development **project status reports** to communicate project status to all relevant personnel.	Inspected a sampling of project status reports to determine that project status reports are in place to communicate to all relevant personnel the status of application development projects.	No exceptions noted.
8.14	The development team lead performs **code reviews** to verify developers' compliance with documented coding standards for development and maintenance activity.	Inspected a sample of code reviews during the control period to determine that the development team lead performs code reviews to verify developers' compliance with documented coding standards for development and maintenance activity.	No exceptions noted.
	Applications Quality Assurance / Testing		
8.15	The quality assurance and testing efforts are performed in a distinct QA staging environment that is **physically and logically separated from the production environment.**	Observed the location of the servers for each environment to determine that quality assurance and test environments are physically separated from the production environment.	No exceptions noted.

MATRIX 8 APPLICATION DEVELOPMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to production application code and systems are properly authorized, tested, approved, implemented and documented.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
8.16	Management requires that the **development and testing** of application changes be **performed by separate personnel**.	Inspected a judgmental sample of application change tickets from the review period to determine that management required that the development and testing of application changes be performed by separate personnel.	No exceptions noted.
8.17	**Access to the quality assurance testing environment** is restricted based upon job responsibilities.	Inspected access rights to determine that access to the quality assurance testing environment is restricted based upon job responsibilities.	No exceptions noted.
8.18	**Application testing** takes place at several different phases of the development cycle: • Unit Testing during development • QA Testing, including regression testing/staging • Concise confirmation testing after migration to the production environment.	Inquired of management to determine that application testing takes place at different phases of the development cycle.	No exceptions noted.
8.19	There are **two main categories of testing**: • Basic testing, in which fundamental features are verified via an automated test environment • QA Engineers' direct testing for more advanced and new changes requiring more specialized testing before automated testing.	Inspected a judgmental sample of testing logs from the review period to determine that NOVAtime utilizes two main categories of testing.	No exceptions noted.
8.20	A **regression test plan** is developed by the quality assurance team for system enhancements.	Inspected a judgmental sample of major releases from the review period for regression test plans to determine that a regression test plan was developed by the quality assurance team for system enhancements.	No exceptions noted.

MATRIX 8 APPLICATION DEVELOPMENT

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to production application code and systems are properly authorized, tested, approved, implemented and documented.

Control Point	Control Activity Described by the Service Organization	Test of Control Activity by the Service Auditor	Test Results Determined by the Service Auditor
8.21	Quality assurance personnel perform **quality assurance testing for application changes** and update the change request ticket history to indicate approval of the test results prior to migration to the production environment.	Inspected change request forms and internal release notices for changes promoted to production during the review period to determine that quality assurance personnel perform quality assurance testing for application changes and update the change request ticket history to indicate approval of the test results prior to migration to the production environment.	No exceptions noted.
8.22	For updates to production, the CC Form for each change serves as a roll-out **log**, and is updated with the status (including time stamp) for tracking purposes.	Inspected a judgmental sample of CC forms from the review period to determine that they are updated to serve as a roll-out log.	No exceptions noted.
8.23	NOVAtime **roll-out schedules** are based on the classification of the change: • For emergency changes (e.g. changes that affect payroll), an 'unscheduled' live update is performed. • Other changes are scheduled to be included in the next Maintenance Window, which is reserved for the first Friday night of every month.	Inspected rollout logs to determine that major changes are rolled to production during scheduled maintenance windows, while emergency changes take place immediately.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MATRIX 9 SERVICES AND CONTROLS PROVIDED BY THE THIRD PARTY DATA CENTER

NOVAtime utilizes the services and controls of a third party data center, CenturyLink Technology Solutions, for housing critical production computer servers, applications, and networking equipment. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data center Described by the Service Organization	Resources Utilized by the Service Organization to provide this Description
	CenturyLink Technology Solutions Data Center	
9.1	Physical security policies and procedures are in place to guide personnel in the following areas: • Data center access for employees, contractors, and visitors • Security Monitoring • Security assessments and access reviews	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.2	Site authorizers are utilized to approve all permanent access to the data centers.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.3	Security access controls (i.e. physical barriers and doors, card controlled entry points, biometric scanning, video surveillance and/or manned reception desks) are utilized to protect areas that contain information and information processing facilities.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.4	Control mechanisms are in place to limit physical access to restricted data center areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.5	Data center badge access requests for CenturyLink employees and contractors require a completed badge access request approved by site authorizers. Badge access requests for customers require a completed badge access request approved by an authorized customer representative.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.6	Data center security personnel undergo an annual certification process to maintain awareness and help ensure adherence to current physical security policies and procedures.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.

MATRIX 9 SERVICES AND CONTROLS PROVIDED BY THE THIRD PARTY DATA CENTER

NOVAtime utilizes the services and controls of a third party data center, CenturyLink Technology Solutions, for housing critical production computer servers, applications, and networking equipment. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data center Described by the Service Organization	Resources Utilized by the Service Organization to provide this Description
9.7	Data center access for CenturyLink personnel is revoked as a component of the employee termination process.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.8	Temporary access to the data centers for CenturyLink contractors must be pre-approved by work order or ticket. Temporary access to data centers for customers require prior authorization by the authorized customer representative.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.9	Customer-maintained access lists are utilized to identify customer representatives authorized to request permanent or temporary access to the data center(s) where the customer colocation space resides.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.10	Visitor logs are maintained for at least 90 days to document visitor activity at the data centers.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.11	Visitors are required to be escorted by an authorized CenturyLink employee or authorized customer representative at all times while in the data centers.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.12	All persons entering the data centers must present valid government-issued photo ID, or display and use a valid CenturyLink photo access badge prior to entering the facility.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.13	CCTV surveillance video and/or ACS activity logs are retained for a minimum of 90 calendar days.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.

MATRIX 9 SERVICES AND CONTROLS PROVIDED BY THE THIRD PARTY DATA CENTER

NOVAtime utilizes the services and controls of a third party data center, CenturyLink Technology Solutions, for housing critical production computer servers, applications, and networking equipment. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data center Described by the Service Organization	Resources Utilized by the Service Organization to provide this Description
9.14	Data center security personnel and the CSOC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms and CCTV video surveillance systems	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.15	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and, where applicable, are isolated from information processing facilities to avoid unauthorized access.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.16	An inventory of access badges and metal keys designated for loan to employees, customers, or contractors, as applicable by location, is performed at least once per day to account for all badges and metal keys.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.17	All shipments received at the data centers are stored in a physically secured location.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.18	Access to the shipping and receiving areas at the data centers is restricted to authorized personnel.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.20	Environmental security policies and procedures are in place to guide personnel in the following areas: • Equipment specifications and operating instructions • Equipment inspections • Preventive maintenance schedules	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.

MATRIX 9 SERVICES AND CONTROLS PROVIDED BY THE THIRD PARTY DATA CENTER

NOVAtime utilizes the services and controls of a third party data center, CenturyLink Technology Solutions, for housing critical production computer servers, applications, and networking equipment. The information within the table below describes some, but not all, of these utilized services and controls.

Control Point	Control Activity of Third Party Data center Described by the Service Organization	Resources Utilized by the Service Organization to provide this Description
9.21	A BMS is configured to monitor data center equipment including, but not limited to, the following: • Fire detection and suppression systems, as applicable • HVAC units • Generators, as applicable • Electrical systems, as applicable	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.22	The BMS is configured to notify data center staff either via onscreen alert or e-mail alert when predefined thresholds are exceeded on monitored devices.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.23	Power management equipment is in place at each data center.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.24	Third party specialists inspect power management systems on an annual basis.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.25	Fire detection and suppression equipment is in place at each data center.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.26	Third party specialists inspect fire detection and suppression systems on an annual basis.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.
9.27	HVAC systems are in place at each data center. Third party specialists inspect HVAC systems and water detection sensors, as applicable, on an annual basis.	SOC 1-SSAE 16 report for CenturyLink Technology Solutions for the period July 1, 2014 to June 30, 2015.

END OF REPORT