CORELLIAN SOFTWARE

EPRLive System

Relevant to Security, Availability, and Confidentiality

For the period February 1, 2024 to January 31, 2025

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Corellian Software, Inc. (Corellian Software)

Scope

We have examined Corellian Software's accompanying assertion titled "Assertion of Corellian Software Management" (assertion) that the controls within Corellian Software's EPRLive System (system) were effective throughout the period February 1, 2024 to January 31, 2025, to provide reasonable assurance that Corellian Software's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria.*

Service Organization's Responsibilities

Corellian Software is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Corellian Software's service commitments and system requirements were achieved. Corellian Software has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Corellian Software is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve Corellian Software's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Corellian Software's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Corellian Software's EPRLive System were effective throughout the period February 1, 2024 to January 31, 2025, to provide reasonable assurance that Corellian Software's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Sensiba LLP

San Jose, California

June 10, 2025

2. Assertion of Corellian Software Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Corellian Software, Inc. (Corellian Software) EPRLive System (system) throughout the period February 1, 2024 to January 31, 2025, to provide reasonable assurance that Corellian Software's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Corellian Software's EPRLive System," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2024 to January 31, 2025, to provide reasonable assurance that Corellian Software's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA*, Trust Services Criteria.*

Corellian Software's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period February 1, 2024 to January 31, 2025, to provide reasonable assurance that Corellian Software's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Corellian Software Management

June 10, 2025

3. Description of Corellian Software's EPRLive System

Company Background

Corellian Software, located in Portland, OR, provides benefit remittance and processing services throughout the United States. The company was founded in 2014 and provides the ability to replace paper-based benefit reports with online entry, funding, and data extraction for multiple downstream organizations.

Services Provided

The EPRLive system provides benefit and contribution reporting for multi-employer trust funds. The system description in this section of the report details the EPRLive system. Any other Corellian Software services are not within the scope of this report.

Benefit remittance:

- Allows union employers to input employee hours and wages to calculate employee fringe benefits based on the rates in collective bargaining agreements to which they are signatory.
- Allows site sponsors (clients) to manage their employer list, create users, update agreements and their rates, and manage access to the data in their area.

Funding:

- Allows multiple collecting agents to apply payments to the benefits for which they collect.
- Creates National Automated Clearing House Association (NACHA) files to upload to banks for electronic ACH payments.

Data extraction:

- Allows collecting agents to download balancing reports.
- Allows fund administrators to download contribution and credit reports, as well as delinquency reports.
- Allows for read-only view for assigned third parties on reports.
- Allows customers to create custom reports.

Principal Service Commitments and System Requirements

Corellian Software, Inc. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Corellian Software, Inc. makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Corellian Software, Inc. has

established for the services. The system services are subject to the Security, Confidentiality, and Availability commitments established internally for its services.

Commitments are communicated via Master Services Agreement.

Security commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up time availability of production systems

Confidentiality commitments

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties
- Confidential information must be used only for the purposes explicitly stated in agreements between The Company and user entities

Availability commitments

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components
- Responding to customer requests in a reasonably timely manner
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities
- Operational procedures supporting the achievement of availability commitments to user entities

Components of the system

The System description is comprised of the following components:

- The System description is comprised of the following components:
- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Components of the System

Infrastructure

Corellian Software, Inc. maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram(s).
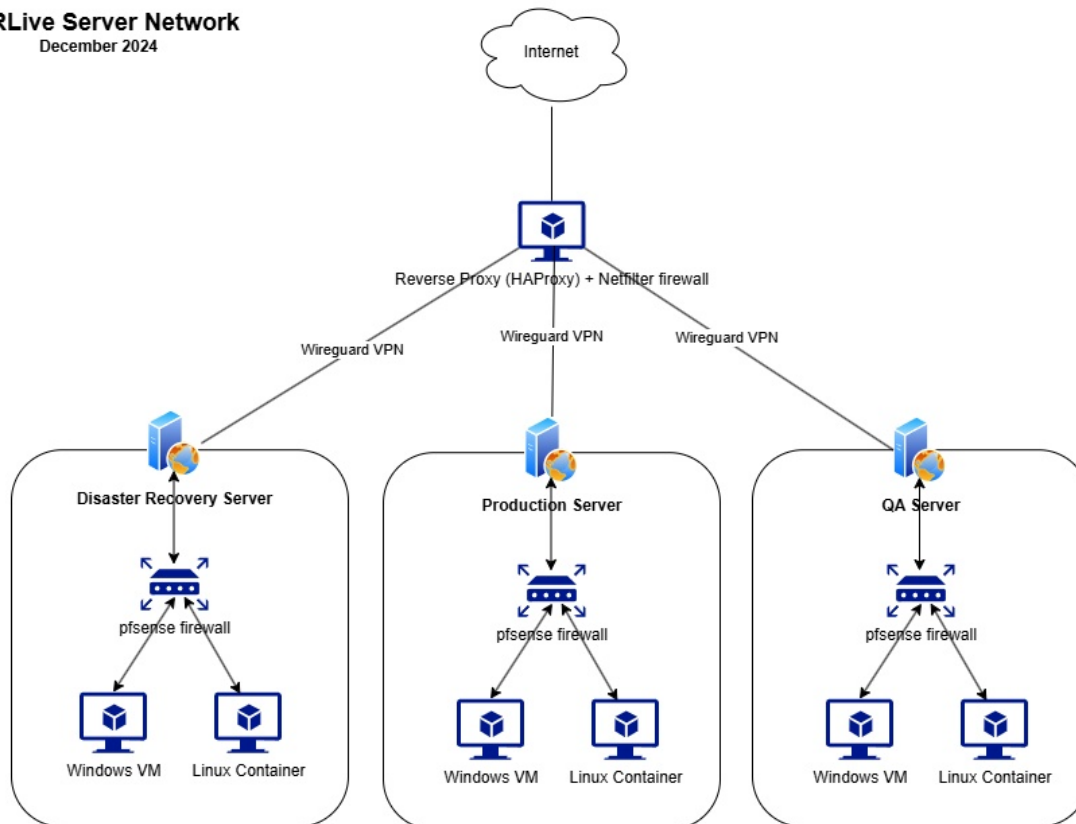
Hardware	Type	Purpose (optional)
Proxmox	Open source	Server virtualization platform to manage virtual machines (VMs) and Linux containers

Software

Corellian Software, Inc. is responsible for managing the development and operation of the EPRLive is a Software-as-a-Service (SaaS) system. system including infrastructure components such as servers, databases, and storage systems. The in-scope Corellian Software, Inc. infrastructure and software components are shown in the table provided below:

System/Application	Operating System	Purpose
Graphana	Graphana Proprietary	Infrastructure monitoring service.
Netbird	Netbird Proprietary	VPN for authentication to the Corellian private network. Connection through VPN is required to access underlying infrastructure of the EPRLive System.
pfSense	pfSense Proprietary	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.
GitHub	GitHub Proprietary	Source code repositories, version control systems, and build software.
Microsoft SQL Server	Microsoft Proprietary	Relational database management system used to securely store, manage, and retrieve structured data for the EPRLive application.

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Corellian Software, Inc. has a staff of approximately 9 organized in the following functional areas:

Management: Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives. Also responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. While overseeing human resources is the responsibility of the management team, Corellian users an outside vendor for HR operations.

Operations: Responsible for overseeing the day-to-day running of the company, including finance, accounting, sales, and marketing. Members of the Operations team are also part of the management team.

Engineering/IT: Responsible for the development, testing, deployment, and maintenance of the source code for the EPRLive system. Responsible for the product life cycle, including adding additional product functionality. Also responsible for incident management and response, access controls, and security of the production environment.

Client Success and Support: Responsible for implementations, account management, and customer support activities.

Information Security: Responsible for the oversight of internal controls, policy review, risk management, vulnerability management, and incident management, and includes members independent from control operators.

Data

Data as defined by Corellian Software, Inc., constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Corellian Software, Inc.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Corellian Software, Inc..	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Corellian Software, Inc.. Corellian Software, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer

Category	Description	Examples
Company data	Information collected and used by Corellian Software, Inc. to operate the business. Corellian Software, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Corellian Software, Inc. has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Processes, Policies and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

Corellian Software, Inc.'s production servers are maintained by OVHCloud. The physical and environmental security protections are the responsibility of OVHCloud. Corellian Software, Inc. reviews the attestation reports and performs a risk analysis of OVHCloud on at least an annual basis.

Logical Access

Corellian Software, Inc. provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems are split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access.

Management is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Corellian Software, Inc.'s policies, completing security training. These steps must be completed within 30 days of hire.

When an employee is terminated, Management is responsible for deprovisioning access to all in scope systems within 3 business days for that employee's termination.

Computer Operations – Backups

Customer data is backed up and monitored by the Development for completion and exceptions. If there is an exception, Development will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in OVHCloud with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations – Availability

Corellian Software, Inc. maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Corellian Software, Inc. internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Corellian Software, Inc. utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

Change Control

Corellian Software, Inc. maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Corellian Software, Inc. has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Corellian Software, Inc. application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Annual Penetration test. Microsoft 365 Defender to track Vulnerabilities. Scans are automatic by agent and report to Microsoft 365 when a vulnerability is detected.

Boundaries of the System

The boundaries of the EPRLive is a Software-as-a-Service (SaaS) system. are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the EPRLive is a Software-as-a-Service (SaaS) system.

The applicable trust services criteria and the related controls:

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- **Security**: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.

- **Availability**: Information and systems are available for operation and use to meet the entity's objectives.

- **Confidentiality**: Information designated as confidential is protected to meet the entity's objectives.

Control Environment

<u>Integrity and Ethical Values</u>

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 Corellian Software, Inc.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Corellian Software, Inc.'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They 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, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

<u>Commitment to Competence</u>

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

Specific control activities that the service organization 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.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The Corellian Software, Inc. management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Corellian Software, Inc. can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Corellian Software, Inc. to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Corellian Software, Inc.'s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities. Corellian Software, Inc.'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 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 the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.

- Organizational charts are communicated to employees and updated as needed.

<u>Human Resource Policies and Practices</u>

Corellian Software, Inc.'s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Corellian Software, Inc.'s human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

Corellian Software, Inc.'s risk assessment process identifies and manages risks that could potentially affect Corellian Software, Inc.'s ability to provide reliable and secure services to our customers. As part of this process, Corellian Software, Inc. maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Corellian Software, Inc. product development process so they can be dealt with predictably and iteratively.

<u>Integration with risk assessment</u>

The environment in which the system operates; the commitments, agreements, and responsibilities of Corellian Software, Inc.'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Corellian Software, Inc. addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Corellian Software, Inc.'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of Corellian Software, Inc.'s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Corellian Software, Inc. uses several information and communication channels internally to share information with management, employees, contractors, and customers. Corellian Software, Inc. uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Corellian Software, Inc. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Corellian Software, Inc.'s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going monitoring

Corellian Software, Inc.'s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Corellian Software, Inc.'s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Corellian Software, Inc.'s personnel.

Reporting deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal

tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Corellian Software's EPRLive System.

Subservice Organizations

Corellian Software's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Corellian Software's services to be solely achieved by Corellian Software's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Corellian Software.

The following subservice organization controls should be implemented by OVHCloud to provide additional assurance that the trust services criteria described within this report are met.

Security Category	
Criteria	*Controls expected to be in place*
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	OVHCloud is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	OVHCloud is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

Availability Category	
Criteria	*Controls expected to be in place*
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	OVHCloud is responsible for managing environmental protections within the data centers that house network, virtualization management, and storage devices for its cloud hosting services where the entity's system resides.

Corellian Software management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Corellian Software performs monitoring of the subservice organization controls, including the following procedures

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Complementary User Entity Controls

Corellian Software's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to Corellian Software's services to be solely achieved by Corellian Software's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Corellian Software's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Corellian Software.
2. User entities are responsible for notifying Corellian Software of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.

4.   User entities are responsible for ensuring the supervision, management, and control of the use of Corellian Software services by their personnel.

5.   User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Corellian Software services.

6.   User entities are responsible for providing Corellian Software with a list of approvers for security and system configuration changes for data transmission.

7.   User entities are responsible for immediately notifying Corellian Software of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.