Epilogue Systems, LLC
Type 1 SOC 2
2019

REPORT ON EPILOGUE SYSTEMS, LLC'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY

Pursuant to Reporting on Service Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

May 15, 2019

Table of Contents

SECTION 1 MANAGEMENT OF EPILOGUE SYSTEMS, LLC'S ASSERTION REGARDING ITS SYSTEM AS OF MAY 15, 2019 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 EPILOGUE SYSTEMS, LLC'S DESCRIPTION OF ITS SAAS - EPILOGUE OPUS SERVICES SYSTEM AS OF MAY 15, 2019 7

OVERVIEW OF OPERATIONS 8
Company Background 8
Description of Services Provided 8
Principal Service Commitments and System Requirements 8
Components of the System 8
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING 14
Control Environment 14
Risk Assessment Process 16
Information and Communications Systems 16
Monitoring Controls 17
Changes to the System in the Last 12 Months 17
Incidents in the Last 12 Months 17
Criteria Not Applicable to the System 17
Subservice Organizations 17
COMPLEMENTARY USER ENTITY CONTROLS 19
TRUST SERVICES CATEGORIES 20
In-Scope Trust Services Criteria 20
Control Environment 21
Information and Communication 24
Risk Assessment 26
Monitoring Activities 28
Control Activities 29
Logical and Physical Access Controls 31
System Operations 35
Change Management 38
Risk Mitigation 39

SECTION 4 INFORMATION PROVIDED BY THE SERVICE AUDITOR 40

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR 41

SECTION 1

MANAGEMENT OF EPILOGUE SYSTEMS, LLC'S ASSERTION REGARDING ITS SYSTEM AS OF MAY 15, 2019

MANAGEMENT OF EPILOGUE SYSTEMS, LLC'S ASSERTION REGARDING ITS SYSTEM AS OF MAY 15, 2019

May 20, 2019

We have prepared the accompanying description of Epilogue Systems, LLC's ('Epilogue' or 'the Company') Software as a Service (SaaS) - Epilogue Opus Services System titled "Epilogue Systems, LLC's Description of Its SaaS - Epilogue Opus Services System" as of May 15, 2019 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the SaaS - Epilogue Opus Services System that may be useful when assessing the risks arising from interactions with Epilogue's system, particularly information about system controls that Epilogue has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Epilogue uses Amazon Web Services ('AWS') to provide cloud hosting services and Twentyseven Global, LLC ('27Global') to provide development and IT managed services (collectively, 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Epilogue, to achieve Epilogue's service commitments and system requirements based on the applicable trust services criteria. The description presents Epilogue's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Epilogue's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at Epilogue, to achieve Epilogue's service commitments and system requirements based on the applicable trust services criteria. The description presents Epilogue's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Epilogue's controls.

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

a. the description presents Epilogue's SaaS - Epilogue Opus Services System that was designed and implemented as of May 15, 2019, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of May 15, 2019, to provide reasonable assurance that Epilogue's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Epilogue's controls as of that date.

Mike Graham
CEO
Epilogue Systems, LLC

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT EPILOGUE SYSTEMS, LLC RELEVANT TO SECURITY

To: Epilogue Systems, LLC

Scope

We have examined Epilogue's accompanying description of its SaaS - Epilogue Opus Services System titled "Epilogue Systems, LLC's Description of Its SaaS - Epilogue Opus Services System" as of May 15, 2019, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of May 15, 2019, to provide reasonable assurance that Epilogue's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Epilogue uses AWS to provide cloud hosting services and 27Global to provide development and IT managed services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Epilogue, to achieve Epilogue's service commitments and system requirements based on the applicable trust services criteria. The description presents Epilogue's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Epilogue's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Epilogue, to achieve Epilogue's service commitments and system requirements based on the applicable trust services criteria. The description presents Epilogue's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Epilogue's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Epilogue 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 Epilogue's service commitments and system requirements were achieved. Epilogue has provided the accompanying assertion titled "Management of Epilogue Systems, LLC's Assertion Regarding Its System as of May 15, 2019" (assertion) about the description and the suitability of the design of controls stated therein. Epilogue is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted 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 presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

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

Opinion

In our opinion, in all material respects,

a. the description presents Epilogue's SaaS - Epilogue Opus Services System that was designed and implemented as of May 15, 2019, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of May 15, 2019, to provide reasonable assurance that Epilogue's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Epilogue's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Epilogue, user entities of Epilogue's SaaS - Epilogue Opus Services System as of May 15, 2019, business partners of Epilogue subject to risks arising from interactions with the SaaS - Epilogue Opus Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

_____

Tampa, Florida
May 20, 2019

SECTION 3

EPILOGUE SYSTEMS, LLC'S DESCRIPTION OF ITS SAAS - EPILOGUE OPUS SERVICES SYSTEM AS OF MAY 15, 2019

OVERVIEW OF OPERATIONS

Company Background

Epilogue was founded in May 2010 and launched its initial application performance support solution in January 2012. Epilogue's solution enabled customers to rapidly document their critical applications in order to provide training and guidance for the users of these applications. From 2012 - 2017, Epilogue sold its on-premises or hosted solution which also included a desktop component for application documentation, to predominantly medium to large companies. In June 2018, Epilogue launched its SaaS performance support solution which accomplishes the same outcomes but via a more efficient multi-tenant cloud technology which also enables a level of data collection and analytics not available in the predecessor technology.

Description of Services Provided

In addition to Epilogue's SaaS solution for application performance support, Epilogue provides services in support of its customers including, provisioning new accounts, on-boarding and training and product support.

Principal Service Commitments and System Requirements

Epilogue designs its processes and procedures related to Opus to meet its objectives for its digital performance support services. Those objectives are based on the service commitments that Epilogue makes to user entities, the laws and regulations that govern the provision of digital performance support services, and the financial, operational, and compliance requirements that Epilogue has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of Opus that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

Epilogue establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Epilogue’s policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of Opus.

Components of the System

Infrastructure

Primary infrastructure used to provide Epilogue’s SaaS - Epilogue Opus Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Router	AWS VPC	Provides the software defined network infrastructure needed to route traffic to and from the application, including subnets, route tables, access control lists and internet gateways.

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Firewall	Security Groups	Used as a firewall to govern traffic between the application, internal services and incoming traffic from the internet.
Hypervisor	AWS EC2	The hypervisor used to run the application and services.
Container orchestration system.	AWS EKS	EKS is the AWS variant of Kubernetes. It orchestrates containers of application services running on EC2 instances.
Container Registry	AWS ECR	Used as a repository of containers to be put on the EKS cluster.
Functions as a Service	AWS Lambda	Used to run event driven, “serverless” services.
Object Storage	S3	Used to store static assets for the application.
Database Services	AWS RDS	Hosts Microsoft SQL database for the application and Postgres databases for the internal services.
In-memory data store and cache service.	AWS ElastiCache	Used to cache activity on the application.
API Gateway	AWS API Gateway	AWS service for creating, publishing, maintaining, monitoring, and securing REST and WebSocket APIs.
CDN	Amazon CloudFront	Content delivery network distributes cached content such as images.
Identity Access Management	AWS IAM	Used to control who has what access to what components of the infrastructure.
DNS	Route 53	Routes DNS for the application.
Certificate Authority	AWS Certificate Manager	Manages and is the certificate authority for application domain names.

Software

Primary software used to provide Epilogue’s SaaS - Epilogue Opus Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Gitlab	Ubuntu 16.04	File system for the content engine of the application. When a user uploads content to the recording engine, this stores versions of the recordings.
Github	N/A	Application version control and source code management service.
Grafana	Ubuntu 16.04	Software that specializes in organizing metrics and dashboards.
AWS Glue	N/A	Used to perform ETL on a variety of data stores.

Primary Software		
Software	**Operating System**	**Purpose**
Greylog	Ubuntu 16.04	Centralized log management for the application.
Uptime Robot	N/A	Checks services' APIs for status codes. If a bad code is returned, Uptime Robot sends alerts to system administrators.
Jenkins	Ubuntu 16.04	Jenkins is an automation server that performs software builds and checks during the application's development process.
Learning Locker	Amazon Linux 2	It is a conformant open source learning record store. It allows activities to be saved to its API and those activity can be later exported to other lockers. For example, if a user completes a lesson, they are rewarded a certificate which is stored in the Learning Locker. This certificate can be called upon for verification or exported to another learning locker.
Jira	N/A	Jira is a developer collaboration platform. It allows developers and stake holders to communicate user stories, tasks and bugs across the engineering team.
Zabbix	Ubuntu 16.04	Zabbix is a monitoring agent and interface that monitors host metrics of application servers and networks. It is used to measure the stability of the underlying system of the application.
CloudWatch	N/A	CloudWatch is a monitoring and management service provided by AWS that is used to alert system administrators of changes to the AWS infrastructure, host resources and billing.
CloudTrail	N/A	CloudTrail is an AWS managed service that records changes to the AWS infrastructure at a granular level.
VPC Flow Logs	N/A	VPC Flow Logs are logs of traffic across the VPC network.
Electron Release Server	N/A	The electron release server is a self-hosted release server for the application, which is an electron application.
ElasticSearch	N/A	ElasticSearch provides the search functions within the application.
Clam AV	N/A	ClamAV is an anti-virus solution which scans uploaded files to the service. When a customer uploads documents to the application, a scan is performed to make sure uploaded malware is not spread to the client's organization.
AWS Glue	N/A	AWS Glue is used to catalog datastores into a metadata catalog for further ETL'ing into other data formats or databases.

Primary Software		
Software	**Operating System**	**Purpose**
SQS	N/A	SQS is Amazon's Simple Queue Service. It facilitates messages between the applications internal services.
SES	N/A	SES is Amazon's Simple E-mail Service, it's an e-mail service that sends e-mails regarding defined topics and triggers.
SNS	N/A	Amazon Simple Notification Service is a fully managed publish/subscribe messaging service for microservices, and distributed systems and serverless applications.
PostgresDB	N/A	Postgres databases are used to store data for internal services that support the application.
Microsoft SQL Server Web Edition	N/A	Microsoft SQL databases serve as the application's main database.

People

Epilogue has a staff of 19 employees organized in the following functional areas:

- Corporate. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources, and transportation provider relations. These individuals use the Opus primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for Epilogue's user entities
- IT. Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support
    - The help desk group provides technical assistance to the Opus users
    - The infrastructure, networking, and systems administration staff typically has no direct use of Opus. Rather, it supports Epilogue's IT infrastructure, which is used by the software. A systems administrator will deploy the releases of Opus and other software into the production environment
    - The software development staff develops and maintains Opus for Epilogue. This includes the Opus, supporting utilities, and the external websites that interact supports Epilogue and their clients. The staff includes software developers, database administration, software quality assurance, and Dev-Ops
    - The information security staff supports Opus indirectly by monitoring internal and external security threats and maintaining current antivirus software
    - The information security staff maintains the inventory of IT assets

Data

Data, as defined by Epilogue, constitutes the following:

- Subscription Data
- Target Application usage data
- Electronic support content and metadata
- Content User support content usage data
- Audit logs
- System files
- Error logs

Subscription data is developed by the client that starts an account in the system. They define the target applications to be documented by Opus and provides that information through the creation of the Electronic support content and metadata to support the target applications usage. As the content is used by the client employees, the context user usage of the digital support content is maintained for analytical purposes. Through the usage of Opus, each client creates audio, system and error logs that are monitored for legal requirements and improvement processes.

Policies, Processes and Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Epilogue policies and procedures that define how services should be delivered. These are located on the Company's shared drive and can be accessed by any Epilogue team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by Amazon Web Services ("AWS"). As such, AWS is responsible for the physical security controls for the in-scope system , SaaS - Epilogue Opus services.

Logical Access

Epilogue Opus uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources.

All resources are managed in the asset inventory spreadsheet and ownership of these assists are assigned to the CTO. The CTO is responsible for approving access to the resource and for performing reviews of access by role.

Employees and approved vendor personnel sign on to the Epilogue Opus system and any supporting systems such as Salesforce, Jira and Discovery using a unique user ID and password. Passwords must conform to defined password standards and are enforced through parameter settings in the applications. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Customer employees' access Opus through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to Opus. Passwords must conform to password configuration requirements of the Opus solution or use a compatible SAML 2.0 server such as OKTA, ADFS or Login One for SSO or two-factor authentication.

Upon hire, employees are provided access to the systems consistent with their role based on the job description. The access is reviewed annually at a minimum or when there is a position or responsibility change to ensure access is correct.

Termination requires all access for that individual be removed and is verified by the CTO.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Backup infrastructure is the ASW backup service using their 11 9's S3 storage as described in the Backup and Recovery Policy and Procedure. Backups are performed daily, weekly and monthly to ensure the ability to recover from any disaster.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify, and respond to incidents on the network.

Epilogue monitors the capacity utilization of physical and computing infrastructure of Opus to ensure that service delivery matches service level agreements. Epilogue evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Disk storage
- CPU Utilization
- Memory Utilization
- Container Health
- Network bandwidth

Epilogue has implemented a patch management process to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches. Epilogue owners review proposed operating system patches to determine whether the patches are applied. Epilogue is responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems. Epilogue staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Epilogue 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 Opus implementation of new changes. Quality assurance testing 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.

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.

Epilogue has implemented a patch management process to ensure Opus and infrastructure systems are patched in accordance with vendor recommended operating system patches. Epilogue owners review proposed operating system patches to determine whether the patches are applied. Epilogue is responsible for determining the risk of applying or not applying patches based upon the security and availability impact of Opus. Epilogue staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Epilogue. The third-party vendor's approach begins with a vulnerability analysis of Opus to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the network and application, and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with Epilogue policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Epilogue. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Boundaries of the System

The scope of this report includes the SaaS - Epilogue Opus Services System performed in the Ambler, Pennsylvania facilities.

This report does not include the cloud hosting services provided by AWS or the development and IT managed services provided by 27Global.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

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 Epilogue's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Epilogue'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

Commitment to Competence

Epilogue'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 particular 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 encouraged to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Epilogue's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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

- Management is 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 as a whole

Organizational Structure and Assignment of Authority and Responsibility

Epilogue'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.

Epilogue'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

Human Resources Policies and Practices

Epilogue'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. Epilogue'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 acknowledgement 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
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Epilogue's risk assessment process identifies and manages risks that could potentially affect Epilogue's ability to provide reliable services to Opus Users. This ongoing process requires that management identify significant risks inherent in Opus or services as they oversee their areas of responsibility. Epilogue identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Epilogue, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Epilogue has identified a team of executives responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organization with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Epilogue attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with all employees.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Epilogue's Opus system ; as well as the nature of the components of the system result in risks that the criteria will not be met. Epilogue addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because Opus 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 Opus, Epilogue'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 is an integral component of Epilogue'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. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Epilogue, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Epilogue personnel via e-mail messages.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Epilogue'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

Epilogue'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 Epilogue'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 Epilogue's personnel.

Reporting Deficiencies

An internal 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. 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 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 review date.

Criteria Not Applicable to the System

All Common criteria was applicable to the Epilogue SaaS - Epilogue Opus Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS or the development and IT managed services provided by 27Global.

Complementary Subservice Organization Controls

Epilogue'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 Epilogue's services to be solely achieved by Epilogue control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Epilogue.

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems (IDS) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

The following subservice organization controls should be implemented by 27Global to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - 27Global		
Category	**Criteria**	**Control**
Common Criteria / Security	CC4.1, CC6.6, CC6.7, CC7.1, CC7.2	An IDS is utilized to analyze network events and report possible or actual network security breaches.
	CC4.1, CC6.6, CC6.7, CC7.1, CC7.2	The IDS is configured to notify personnel upon intrusion detection via e-mail.
	CC4.1, CC6.6, CC6.7, CC7.1, CC7.2	A firewall is in place to filter unauthorized inbound network traffic from the internet.
	CC4.1, CC6.6, CC6.7, CC7.1, CC7.2	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
	CC6.8, CC7.2	Antivirus software is installed to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.
	CC6.8, CC7.2	The antivirus software provider pushes updates to the installed antivirus software each time there is an upload of a file.

Subservice Organization - 27Global		
Category	**Criteria**	**Control**
	CC6.8, CC7.2	The antivirus software is configured to scan workstations on a daily basis.
	CC6.8, CC8.1	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.
	CC8.1	Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.
	CC8.1	Development and test environments are physically and logically separated from the production environment.

Epilogue 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, Epilogue performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding discussions with vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Epilogue'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 of the Trust Services Criteria related to Epilogue's services to be solely achieved by Epilogue control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Epilogue's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services 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 Epilogue.
2. User entities are responsible for notifying Epilogue of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Epilogue 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 Epilogue services.
6. User entities are responsible for providing Epilogue with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Epilogue of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Criteria

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Control Activities Specified by the Service Organization

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook. An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Upon hire, personnel are required to complete a background check. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Performance and conduct evaluations are performed for personnel on an annual basis. The employee handbook, which includes sanctions such as suspension and termination, are in place for employee misconduct. Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually. Executive management defines and documents the skills and expertise needed among its members. Executive management maintains independence from those that operate the key controls within the environment. Executive management assesses the effectiveness and performance of internal controls within the environment. Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive. Upon hire, personnel are required to sign an offer letter which requires adherence to the personnel's job role and responsibilities. Executive management has established proper segregations of duties for key job functions and roles within the organization.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Performance and conduct evaluations are performed for personnel on an annual basis. The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities. Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process. The entity works with an outside vendor to attract individuals with competencies and experience that align with the entity's goals and objectives. Executive management uses an outside vendor to assist with its continued training of employees. Upon hire, personnel are required to complete a background check.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Upon hire, personnel are required to sign an offer letter which requires adherence to the personnel's job role and responsibilities. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Performance and conduct evaluations are performed for personnel on an annual basis. The employee handbook, which includes sanctions such as suspension and termination, are in place for employee misconduct.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive. Edit checks are in place to prevent incomplete or incorrect data from being entered into the system. Data flow diagrams and process flowcharts are documented and maintained by management to identify the relevant internal and external information sources of the system. Data that entered into the system , processed by the system and output from the system is protected from unauthorized access.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive. The entity's policies and procedures, code of conduct, and employee handbook are made available to employees through the entity's shared drive. Upon hire, employees are required to complete information security and awareness training. Current employees are required to complete information security and awareness training on an annual basis. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis. Upon hire, personnel are required to acknowledge the employee handbook and code of conduct. Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner. Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's shared drive.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's shared drive and all team meetings. The entity's third-party agreement delineates the boundaries of the system and describes relevant system components. The entity's third-party agreement communicates the system commitments and requirements of third parties. The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system. Customer commitments, requirements and responsibilities are outlined and communicated to customers upon agreement to use the service. Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties. Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics. Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART). Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved. Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure. Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies. Business plans and budgets align with the entity's strategies and objectives. Entity strategies, objectives and budgets are assessed on an annual basis.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are approved by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process. For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impact security. On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations, including risks such as unauthorized access. As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impact security. Changes to legal, regulatory, and contractual requirements are considered and evaluated as part of the annual comprehensive risk assessment. Changes in job roles and responsibilities are considered and evaluated as part of the annual comprehensive risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. Backup restoration tests are performed at least annually. Logical access reviews are performed on a monthly basis. Penetration tests and vulnerability scans are performed at least annually on the environment to identify control gaps and vulnerabilities. Performance and conduct evaluations are performed for personnel on an annual basis. Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Additional controls are implemented by the subservice organizations. Refer to the Subservice Organizations section for controls managed by the subservice organizations.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Vulnerabilities, deviations and control gaps identified from the control and risk assessments are communicated to those parties responsible for taking corrective actions. Vulnerabilities, deviations, and control gaps identified from the control and risk assessments are documented, investigated, and addressed.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations (e.g. risk assessments, vulnerability scans) performed. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Management has documented the relevant controls in place for each key business or operational process. Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. A disaster recovery plan is developed and updated on an annual basis. The disaster recovery plan is tested on an annual basis.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive. Management has documented the controls implemented around the entity's technology infrastructure. The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive. Management has implemented controls that are built into the organizational and information security policies and procedures.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Executive management assesses the effectiveness and performance of internal controls within the environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	An inventory of system assets and components is maintained to classify and manage the information assets. Privileged access to sensitive resources is restricted to authorized personnel. Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	VPC	
		VPC user access is restricted via role based security privileges defined within the access control system. VPC administrative access is restricted to user accounts accessible by appropriate personnel. VPC users are authenticated via individually-assigned user accounts and passwords. The VPC is configured to enforce password requirements that include: • One uppercase letter • One lowercase letter • One number • One non-alphanumeric character • Maximum password age • Password history VPC flow logs are in place that track and capture information about the IP traffic going to and from the network interfaces in the VPC.
	Database	
		Database user access is restricted via role based security privileges defined within the access control system. Database administrative access is restricted to user accounts accessible by appropriate personnel. Database users are authenticated via individually-assigned user accounts and passwords. The database is configured to enforce password requirements that include: • Minimum password length • Complexity

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Database account lockout settings are in place that include: • PH timeout • Remote login timeout • Remote query timeout Database audit logging settings are in place that include: • Completed patching • Delayed patching • Table numbers • Database numbers • TDE key rotation • Database activity
	Application	
		Application user access is restricted via role based security privileges defined within the access control system. Application administrative access is restricted to user accounts accessible by appropriate personnel. Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include: • One uppercase letter • One special letter • Minimum password length Application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold Application audit policy settings are in place that include: • Logon events • Process tracking • System events Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process. Logical access reviews are performed on a monthly basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process. Logical access reviews are performed on a monthly basis. Privileged access to sensitive resources is restricted to authorized personnel.
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is granted to an employee as a component of the hiring process. Logical access to systems is revoked as a component of the termination process. Logical access reviews are performed on a monthly basis. Privileged access to sensitive resources is restricted to authorized personnel.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organizations. Refer to the Subservice Organizations section for controls managed by the subservice organizations.
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.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. Backups are automatically disposed of once the retention policy has been met. Data that is no longer required for business purposes is rendered unreadable.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network address translation (NAT) functionality is utilized to manage internal IP addresses.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. Logical access to stored data is restricted to authorized personnel. Additional controls are implemented by the subservice organizations. Refer to the Subservice Organizations section for controls managed by the subservice organizations.
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.	Logical access to stored data is restricted to authorized personnel. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. NAT functionality is utilized to manage internal IP addresses. Data is stored in encrypted format using software supporting the AES. Backups are stored in an encrypted format. Additional controls are implemented by the subservice organizations. Refer to the Subservice Organizations section for controls managed by the subservice organizations.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	When downloading an application or software that is potentially malicious, a warning message is prompted. Additional controls are implemented by the subservice organizations. Refer to the Subservice Organizations section for controls managed by the subservice organizations.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. Penetration tests and vulnerability scans are performed at least annually on the environment to identify control gaps and vulnerabilities. Additional controls are implemented by the subservice organizations. Refer to the Subservice Organizations section for controls managed by the subservice organizations.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. Additional controls are implemented by the subservice organizations. Refer to the Subservice Organizations section for controls managed by the subservice organizations.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. The incident response and escalation procedures are reviewed at least annually for effectiveness.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The incident response policies and procedures define the classification of incidents based on its severity. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Identified incidents are reviewed, monitored and investigated by appropriate personnel. Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy. The incident response and escalation procedures are reviewed at least annually for effectiveness.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes. Data backup and restore procedures are in place to guide personnel in performing backup activities. Backup restoration tests are performed at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		A disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The disaster recovery plan is tested on an annual basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process. The change management process has defined the following roles and assignments: • Authorization of change requests • Verification of system stability prior to release • Development - change design and support • Staging - Change approval • QA - Ensure change is working properly • Testing-quality assurance department • Change implementation • After action review System changes are communicated to both affected internal and external users. System changes are authorized and approved by management prior to implementation. System change requests are documented and tracked in a ticketing system. System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation. Additional controls are implemented by the subservice organizations. Refer to the Subservice Organizations section for controls managed by the subservice organizations.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are approved by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. Identified third-party risks are rated using a risk evaluation process and ratings are approved by management. Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment. A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements. The entity has documented procedures for terminating third-party relationships.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of Epilogue was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Epilogue and did not encompass all aspects of Epilogue's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.