ESQUIRE
DEPOSITION SOLUTIONS

System and Organization Controls 3 (SOC 3) Report – SOC for Service Organizations: Trust Service Criteria for General Use Report

Report on Esquire Deposition Solutions' Description of its Court Reporting Service System Relevant to Security Throughout the Period January 1, 2021 to December 31, 2021

Bonadio & Co., LLP
Certified Public Accountants

REPORT ON ESQUIRE DEPOSITION SOLUTIONS' DESCRIPTION OF ITS COURT REPORTING SERVICE SYSTEM RELEVANT TO SECURITY THROUGHOUT THE PERIOD JANUARY 1, 2021 TO DECEMBER 31, 2021

Table of Contents

SECTION ONE

Independent Service Auditor’s Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Management of Esquire Deposition Solutions

Scope

We have examined Esquire Deposition Solutions' accompanying assertion, titled "Assertion of the Management of Esquire Deposition Solutions" (assertion), that controls within Esquire Deposition Solutions' Court Reporting Service System (the System) were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Esquire Deposition Solutions' service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)* and included as Attachment A.

Service Organization's Responsibilities

Esquire Deposition Solutions 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 Esquire Deposition Solutions' service commitments and system requirements were achieved. Esquire Deposition Solutions has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, Esquire Deposition Solutions is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the System.

Service Auditor's 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 American Institute of Certified Public Accountants. The nature, timing, and extent of the procedures selected depend on our judgement, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. 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.

Service Auditor’s Responsibilities (Continued)

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 Esquire Deposition Solutions′ 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 Esquire Deposition Solutions′ service commitments and system requirements based the applicable trust services criteria

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

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 Esquire Deposition Solutions’ Court Reporting Service System were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Esquire Deposition Solutions’ service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Bonadio & Co., LLP

Pittsford, New York
April 6, 2022

SECTION TWO

Assertion of the Management of Esquire Deposition Solutions

ESQUIRE
DEPOSITION SOLUTIONS

ASSERTION OF THE MANAGEMENT OF ESQUIRE DEPOSITION SOLUTIONS

April 6, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within Esquire Deposition Solutions' Court Reporting Service System (the System) throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Esquire Deposition Solutions' service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in Section 3 titled "Management's Description of Esquire Deposition Solutions' Court Reporting Service System Throughout the Period January 1, 2021 to December 31, 2021" 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 January 1, 2021 to December 31, 2021, to provide reasonable assurance that Esquire Deposition Solutions' 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)*. Esquire Deposition Solutions' 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 Attachment B.

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 January 1, 2021 to December 31, 2021, to provide reasonable assurance that Esquire Deposition Solutions' service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Terrie Campbell
Chief Executive Officer

/s/ Jim Ballowe

Chief Information Officer

SECTION THREE

Management's Description of Esquire Deposition Solutions' Court Reporting Service System Throughout the Period January 1, 2021 to December 31, 2021

INTRODUCTION

Company Background

Esquire Deposition Solutions, LLC (Esquire Deposition Solutions, Esquire or the Company) was established in 2011 with a principal place of business in East Point, Georgia. The Company provides deposition management and automated transcription services from 37 United States offices. These services are provided using Esquire Deposition Solutions' Court Reporting Service System, which has been developed and is maintained by Esquire Deposition Solutions.

Esquire Deposition Solutions conducts more than 140,000 depositions annually in its 37 offices and remotely by leveraging its extensive network of court reporters across the United States. Since inception, Esquire has facilitated scheduling and conducting depositions, regardless of location, by combining the best reporters with the latest in digital technology and training.

Esquire offers quality court reporting using cutting edge technology through an uncommon focus on personal interactions, worry-free service, and high professional standards. Esquire leadership values friendliness and fairness but is also tough and determined to tackle challenges in the marketplace. Ethics and integrity are considered the most important factors that guide the actions of all Esquire staff and its service partners.

Services Provided

Esquire is the voice of progress in the deposition management industry, introducing new practices and technologies, such as a groundbreaking remote depositions platform, that standardizes and optimizes remote depositions for attorneys and their staff through the use of integrated video conferencing, video capture, exhibit management, sidebar rooms, and testimony review tools, all with searchable, in-proceeding, speech–to-text streaming.

Esquire's line of services delivers secure customer interaction software and services via the web. Services provided as part of Esquire Deposition Solutions' Court Reporting Service System include the following (the Service or the System):

Deposition Management

As the industry's foremost expert in remote depositions, Esquire has developed reliable, easy-to-use services that allow clients to attend depositions or depose witnesses via computers or mobile devices from anywhere.

Court Reporting

Esquire's real-time reporting services allow clients to instantly read, search, and annotate testimony as it is collected. Esquire's experienced court stenographers handle all technical details during the deposition. Clients gain access to the real-time transcription during the deposition, as well as a full copy of the transcript at its completion.

Arbitration and Mediation

Every Esquire location is fully equipped to handle Alternative Dispute Resolution (ADR) services, including access to experienced court reporters, advanced technology, and concierge-level support in a modern, well-appointed, luxurious space.

Interpreters

Esquire's language translation services tap into a nationwide network of expert interpreters with fluency in a wide array of languages. Each interpreter is equipped with the training and expertise to navigate specialized legal, medical, and technological terminology.

Services Provided (Continued)

Legal Videography

Video deposition recordings are essential for capturing and preserving key aspects of testimony. Esquire Deposition Solutions' legal videographers offer a complete suite of professional video services that enable clients to leverage the full impact of deposition testimony. Video images depict important nonverbal components of the deponent, such as tone of voice, body language, and pauses in testimony. Video-recorded testimony can also be a valuable tool in the courtroom when presenting testimony of a non-appearing witness or to impeach the credibility of an adverse witness.

Client Support and Management

Esquire offers technical support through its center of excellence call center providing service 14 hours a day, Monday through Friday.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

Infrastructure

The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.

All workstations, laptops, and servers are encrypted. Employees are authenticated into the network via Active Directory (AD) and certificates issued to their workstations. Outbound access is monitored and controlled via Cisco and Meraki firewalls. Sophos endpoint protection guards against malware, limits access to known bad internet hosts, and enforces data leakage prevention policies for all employees. Beyond that, Cisco and Meraki network gear provides additional layers of protection against malware, botnets and bad actors online. Access logs are continuously monitored for unauthorized or unusual access via exception reporting. Privileged access to key applications is restricted and requires two-factor authentication. Offsite staff have the same protections in place and can only access Esquire infrastructure remotely via the Cisco Secure AnyConnect Mobility Client. Split tunneling is disabled so that all traffic over virtual private network (VPN) is subject to every security and traffic inspection mechanism for all remote connections to the network.

A combination of hardware and software-based tools have been deployed to protect the network and help control access to and maintain the integrity of data residing on its systems, including the use of redundant firewalls and security lists to filter incoming and outgoing traffic; host-based intrusion detection systems (HIDS) to monitor production servers for potential or actual security events; routers; switches; near real-time monitoring, and audit logging and reporting via a central security information and event management (SIEM) tool. Additionally, web applications provide the ability for clients to access reporting and make inquiries. The applications process within internet-based web services that utilize transport layer security (TLS) 1.2 or greater with 256-bit encryption and digital certificate security.

The production information systems are distributed across geographically separate, secure data center facilities. The secondary data center provides data mirroring, disaster recovery, and failover capabilities should the primary data center become non-operational. Data center facilities are operated by best-of-breed partner Quality Technology Services (QTS), a subservice organization who provides earthquake and fire protection, along with heating, cooling, and backup power.

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.

At the heart of Esquire's business operations lies the NetSuite Enterprise Resource Planning (ERP) Software as a Service (SaaS) solution (which is provided by Oracle America) that serves three (3) distinct audiences: Employees, Vendors, and Customers. Each set of constituents is provided with different access and role-based permissions appropriate to their function. Employee access is provided via the standard NetSuite User Interface (UI) with highly granular role-based controls designed around each employee's job function. Vendor access is provided via the Advanced Partner Center component of NetSuite ERP. Customers are able to access deliverables and schedule proceedings via the Client Portal at https://www.EsquireConnect.com, which is entirely housed in the SiteBuilder component of NetSuite ERP.

Software (Continued)

Amazon Web Services (AWS) is leveraged to index and store transcripts, exhibits, and other non-media deliverables in properly secured Simple Storage Service (S3) buckets. In turn, those files can be accessed by customers via the Client Portal. All such files are encrypted in transit via TLS 1.2 with the strongest commercially available ciphers and are encrypted at rest with AWS S3 server-side encryption using 256-bit Advanced Encryption Standard (AES-256). Esquire conducts scans weekly to ensure that its AWS environment remains in compliance with the Center for Internet Security (CIS) Amazon Web Services Foundations Benchmark, v1.2.0, Level 2. Esquire leverages malware protection for all files stored in S3 using the Sophos antivirus engine.

Box.com houses Esquire's Construction Defect Repository as well as interim working media files and final video deliverables. The files are all encrypted in transit via TLS 1.2 and at rest with AES-256. Esquire maintains Box Enterprise Plus subscription with Box Shield implemented to provide sophisticated threat detection and protection as well as controls for data loss prevention.

The Atlassian suite of products are leveraged extensively by Esquire for management of internal operations. Confluence houses all internal policy, documentation, and spaces for departmental collaboration. Jira provides helpdesk support capabilities via Service Desk and full software development lifecycle management capabilities and transparency via Jira's project management, issue-tracking, and roadmap features.

People

The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

All employees are subject to background checks, must affirm that they agree to abide by Esquire's Code of Ethics upon hire, and are required to participate in ongoing security awareness training as well as annual evaluation via simulated phishing exercises while employed at Esquire. Beyond that, Esquire periodically provides security awareness briefings during All-Employee meetings.

The personnel supporting the Court Reporting System includes, but is not limited to, the following:

Executive management — responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives and the risk assessment.
Operations — responsible for managing, monitoring, and supporting user entities' systems and information to maintain integrity and availability. Operations also includes the 24/7 support desk.
Security — responsible for safeguarding systems and information through application, operations, and corporate security.
Development — responsible for development of new functionality and assistance with release management and responsible for testing and verification of new application functionality as well as regression testing.
Reservations — responsible for scheduling proceedings based on requests from customers received via telephone, email, or the Client Portal.
Service Delivery Coordinator — responsible for managing multiple local and remote depositions associated with their assigned local office.
Resource Manager — responsible for booking and managing Court Reporters, Videographers, and any other resources necessary to ensure successful proceedings.
Court Reporter — responsible for capturing the record, collecting and labelling exhibits, and for acting as an officer of the court to manage attendees and interactions during the proceeding. Following the proceeding, the Court Reporter produce the raw ASCII transcript and turns it in using the secure Service Partner portal for production.

People (Continued)

Videographer — responsible for capturing the record on video when that service is ordered.
Production — responsible for processing raw ASCII transcripts along with all relevant exhibits to produce the final transcript. If synced video is ordered, Production is also responsible for syncing video to the transcript as an additional deliverable.

Third Party Vendors

Third party vendors are assessed via the vendor risk analysis process with respect to the risks their services introduce to Esquire systems. All vendors are tracked in a vendor inventory which is regularly reviewed.

Vendor access accounts are limited in function, controlled and monitored in the same manner as production, corporate, and user accounts.

Data

The types of data used by the system, such as transaction streams, files, databases, tables, and other output used or processed by the system.

Media is stored in secure production facilities in either Esquire's primary location in Atlanta, GA or in its secondary location in Chicago, IL.

The data held by Esquire in its production environment consists of actual video and audio recordings of court and legal proceedings, and the various processed and collateral forms of this data including verbatim transcripts, video captures, etc.

Production files fall into one of three main categories: transcripts, exhibits, and video. Files are subcategorized by original file type accepted by the client or reporter and work product created by Esquire Deposition Solutions.

Esquire restricts access to client data in NetSuite based on the role of any given end-user. Production employees are allowed to use intermediate files provided by court reporters to create final deliverables that are stored in the cloud solutions so that they are then available via the secure client portal online at www.EsquireConnect.com.

All access and changes to meta-data or data is logged within NetSuite, providing a comprehensive audit trail of information access. The logs are retained for at least a year inside of NetSuite. Active Directory logging for file system stored intermediate files is logged for 90 days inside each server and aggregated along with other on-premise systems by AlertLogic. Amazon Web Services Simple Storage Service file access is logged within CloudTrail for over a year and Box.com access is also logged with logs being retained a minimum of at least one year.

Digital data is stored in the following locations and are accessible via secure client portal.

- **Transcripts & Exhibits:** Stored in Amazon Web Services S3 with files encrypted in transit via TLS 1.2 and at rest with AWS S3 server-side encryption using 256-bit Advanced Encryption Standard (AES-256). AWS environment undergoes a weekly third-party evaluation to ensure that it is in compliance with CIS Amazon Web Services Foundations Benchmark, v1.2.0, Level 2.
- **Video Files:** Stored using Box.com with files encrypted in transit and at rest using 256-bit Advanced Encryption Standard (AES-256).

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES (CONTINUED)

Data (Continued)

- **Production workstations and laptops:** Whole disk encryption is implemented on all end-user systems with access logged and limited to authorized personnel only. No local administrative access is granted on these systems.
- **Intermediate files/final deliverable creation:** Stored on encrypted windows file servers running as Virtual Machines (VMs) on encrypted storage area network (SAN) storage. These file servers are located in Esquire's primary (Atlanta) and secondary (Chicago) data centers and are secured 24x7 in a controlled-access environment.
- **NetSuite:** Contains no files, but rather has fields that reference customer records indicating where files are stored per customer in AWS S3 and Box.com.

Legal vs. Business Obligations Regarding Data

Esquire fulfills certain mandated duties on behalf of the deposition officer; acting as an extension of the officer.

Esquire currently stores hold-notes (no write) rough drafts on behalf of the reporters. The read and sign and/or witness come-in process, and some court filing duties are also handled by Esquire, even though certain state rules are very clear that it is the reporter's responsibility.

The Company undertakes best efforts to store the official record (e.g. transcript or video) indefinitely because it may be reasonably held accountable to rules applying to a "deposition officer" or reporter.

Because there is no alternative data warehousing structure in place nor logical record access method for determining state or reporter, Esquire assumes the greatest length of file retention by state law for all records. Federal Courts and many state courts mandate that the court reporter must retain notes – without an explicit timeframe, as such an indefinite retention of all original files received by Esquire Deposition Solutions is presumed for court notes.

The requirements regarding retention of data differ throughout the many jurisdictions served by Esquire. To address this, Esquire data retention standards are uniformly handled with respect to the standards of the most restrictive or severe of the jurisdictions.

Original Files

• Reporter's Original ASCII Transcript (.TXT)	7 Years
• Original Paper Exhibits	90 Days
• Master File – media containing original video deposition	7 Years

Work Product

• Errata Pages	7 Years
• Summary (.PDF, .DOCX)	7 Years
• Exhibit Images	7 Years
• Video Product Files	7 Years
• Interim Remote Reporter Videos	21 Days

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES (CONTINUED)

Data (Continued)

Video Surveillance

• Production facility ingress/egress footage	90 Days+

Logs

• NetSuite System Information (logs of record access)	7 Years

Data and Document Transfer

Esquire can send transcripts via its secure mail gateway, but the most secure and preferred method for providing access to transcripts, exhibits, and video is via the secure online client portal located at www.EsquireConnect.com which is fully indexed, searchable, and available around the clock for access to all transcript documents.

Esquire leverages the subservice organizations NetSuite, AWS S3, and Box.com for document management and product delivery. The Esquire ecosystem leverages each platform's native auditing capabilities in conjunction with role-based access control to ensure the principle of least privilege is enforced and demonstrable for access to all customer data.

Data Destruction and Removal

Electronic and physical documents stored by Esquire can only be destroyed after Esquire receives a signed order from a judge or similarly authoritative document demonstrating consent from all parties affirming that the documents should be destroyed along with a copy of the confidentiality order/provision.

The destruction process can take up to 14 days to complete after the appropriate documentation is received and validated. Documentation of the request is then kept on file by Esquire General Counsel and in the Esquire ticketing system. Certificates of Destruction are kept on file by the Esquire IT Department.

Destruction of Unused/Discarded Physical Copies

Esquire disposes of superfluous overprints or scrap copies of non-client information that are discarded due to issues with printing or formatting. Such documents are disposed of in secure bins which are managed by Iron Mountain. Iron Mountain picks up the bins on a regular basis and provides a certificate of destruction for any media provided in those bins by Esquire.

Third Party Access

Vendors, business partners, and others (third parties) often store, process, and transmit sensitive data or otherwise access a service organization's system. These third parties may provide components of the system. Service organization management may need to describe the components of the system provided by such third parties. Such disclosures may include, for example, the nature of the third parties' access and connectivity to the service organization's system.

Processes and 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.

Esquire has established a set of policies and procedures which includes a set of Information Security Standards (the Standards) that govern the operation, maintenance, and management of Esquire systems. The Information Security Standards are reviewed no less frequently than annually to assess their continued efficacy in light of the ever-evolving threat landscape. Changes to the Standards and all policy documents within the library are approved by Esquire management via the Change Management Policy. The Information Security Standards establish the framework of a security program that defines minimum logical security controls for platforms used to support operations and applications in both the corporate environment and the production environment. Esquire's Information Security Policy Library details the System's security settings and related logical access controls. The Library includes the following:

- Information Security Policy
- Information Security Standards
- Encryption Policy
- Data and Systems Acceptable Use Policy
- Non-Production Data and Records Retention Policy
- System Logging Policy
- Change Management Policy
- Employee Onboarding, Offboarding, & Auditing
- Destruction and Disposal of Electronic Equipment and Data
- Information Technology Procurement Policy
- Application Inventory Policy
- Cloud Computing Policy
- Virtual Machine Build Standards and Template
- Network Access Control Policy
- Access Management & Auditing
- IT Service Level Agreements
- Email Retention Policy
- Backup Policy
- Patch Management Policy
- Audit Policy
- Software Development Life Cycle
- Data Governance
- Security Incident Monitoring Policy
- Incident Response Plan

During periodic security training and awareness programs, management ensures the latest security policies as well as current security best practices are communicated.

ATTACHMENT A

AICPA Trust Services Categories and Criteria

AICPA TRUST SERVICES CATEGORIES AND CRITERIA

This attachment includes the Trust Services Criteria (TSC) included in the scope of the engagement relevant to the security category set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

CC1.0 – Common Criteria Related to Control Environment	
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.0 – Common Criteria Related to Communication and Information	
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
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.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.0 – Common Criteria Related to Risk Assessment	
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
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.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.0 – Common Criteria Related to Monitoring Activities	
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.
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.
CC5.0 – Common Criteria Related to Control Activities	
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.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
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.

AICPA TRUST SERVICES CATEGORIES AND CRITERIA (CONTINUED)

CC6.0 – Common Criteria Related to Logical and Physical Access Controls	
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.
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.
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.
CC6.4	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.
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.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.
CC7.0 – Common Criteria Related to System Operations	
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.
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.
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.
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.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.0 – Common Criteria Related to Change Management	
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.
CC9.0 – Common Criteria Related to Risk Mitigation	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.

ATTACHMENT B

Principal Service Commitments and System Requirements

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Esquire designs its processes and procedures related to court reporting to meet its objectives for its services. Those objectives are based on the service commitments that Esquire makes to user entities; the laws and regulations that govern the provision of its services; and the financial, operational, and compliance requirements that Esquire has established for the services. Esquire services are subject to the legal requirements governing the creation, storage, availability, and retention in each of the jurisdictions in which it operates. Where standards and requirements that cross these jurisdictions, Esquire builds its processes and procedures to meet or exceed the standards of the most restrictive jurisdiction.

Security commitments to user entities are documented and communicated in customer agreements as well as in the description of the service offerings provided online. Security commitments are standardized and include, but are not limited to, the following:

The Information Security team will ensure that security commitments are standardized and include the following:

- Maintain administrative, physical, and technical safeguards designed to ensure the confidentiality and integrity of corporate and customer data.
- Corporate and customer information will be protected against any unauthorized access.
- Business requirements for the availability of information and systems will be met, and an availability service level agreement (SLA) of 99.5% uptime per quarter shall be maintained.
- Develop, maintain, and evaluate detailed Security Policies and Standards consistent with industry standards and review them on at least an annual basis.
- Physical and logical controls will be defined and reviewed on at least an annual basis.
- Security Tools will be deployed, maintained, and used including antivirus (AV), endpoint monitoring, and event/log correlation.
- Risk management protocols will be defined and followed to identify and manage potential areas of risk associated with Esquire systems for Esquire and its clients.
- Comprehensive inventory & configuration management
- Information architecture and data flows must be maintained and reviewed at least annually
- Applications will be inventoried and documented on an ongoing basis
- Asset inventory will be updated continuously and reviewed on at least an annual basis.
- Build standards must be maintained and evaluated for efficacy across all systems
- Develop, maintain and evaluate, and rehearse its Incident Response Plan (IRP) at least annually.
- Maintain multiple geographically, physically and logically separate data centers providing data mirroring disaster recovery (DR) and failover capabilities.
- Develop, maintain and evaluate its Disaster Recovery Plan (DRP), which will be tested at least annually.

Esquire takes seriously its responsibility to adequately safeguard its clients' data. Esquire’s Global Security Model is a layered physical, digital, and procedural risk management framework designed to protect the network, safeguard all client data and support compliance obligations. Client data is encrypted end-to-end: workstations, laptops, servers, mobile devices, video and audio streams, including transcript processing and delivery.

Esquire establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Esquire’s system 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 the Court Reporting Service System.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS (CONTINUED)

Esquire periodically reviews, and updates as deemed appropriate, the policies to address new and evolving security technologies, changes to industry standard practices, and changing security threats. Esquire considers updates to its policies in the context that any such updates do not materially reduce the commitments, protections, or overall level of service provided to customers as described within the customer contracts. Esquire's policies are readily available for employees to review and understand their responsibility for adhering to the associated organizational standards and security requirements.

In accordance with the assertion and the description criteria, the service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and, therefore, may not fully address the specific service commitments and requirements made to all system users.