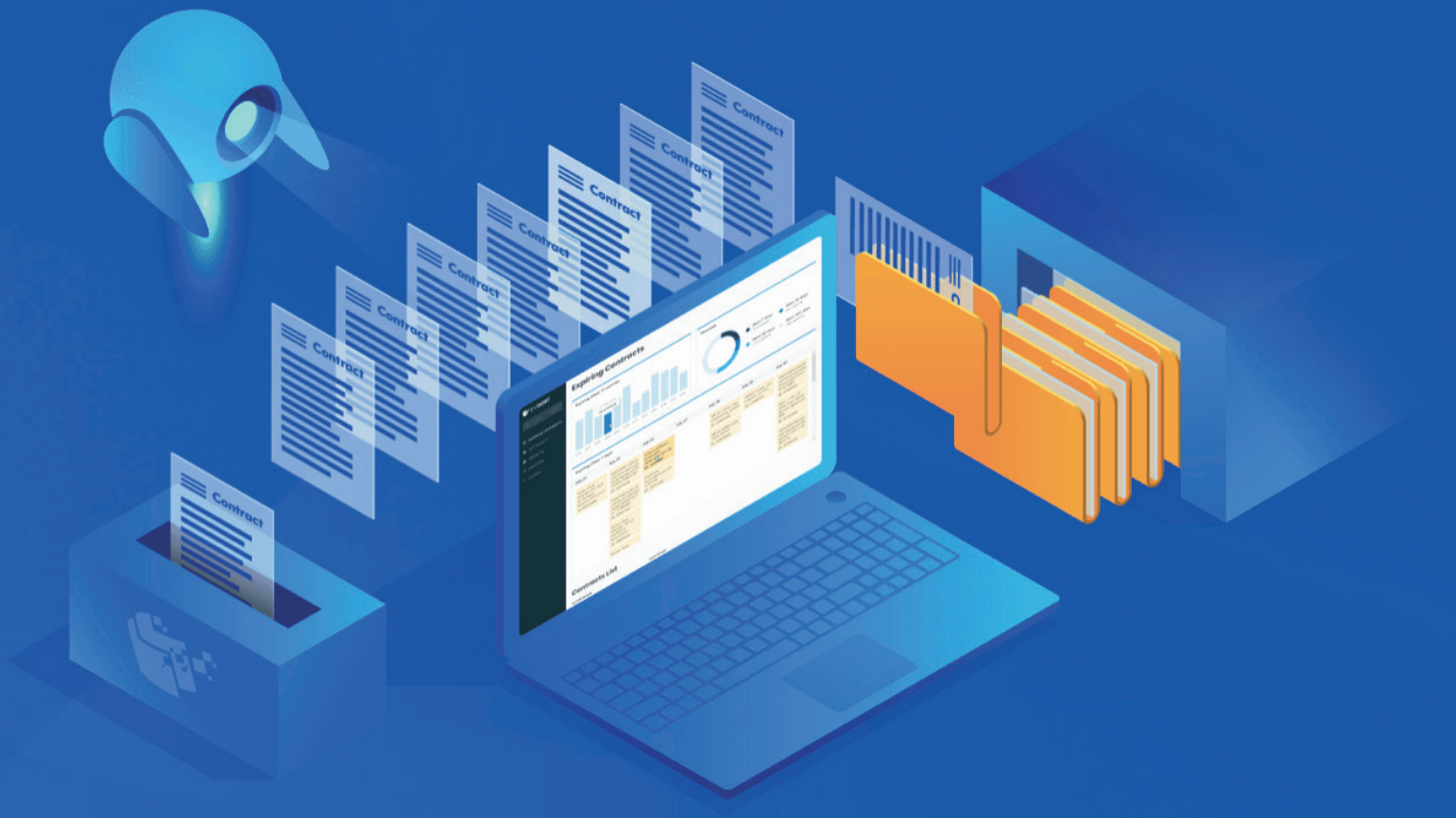
linford&co llp
cpa firm

EVISORT



SOC 3

REPORT ON CONTROLS RELEVANT TO SECURITY

OCTOBER 1, 2019 TO MARCH 31, 2020

linford&co llp
cpa firm

linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Independent Service Auditor's Report

To the Board of Directors of Evisort Inc.:

Scope

We have examined Evisort Inc.'s (Evisort or the Company) accompanying assertion titled "Assertion of Evisort's Management" (assertion) that the controls within Evisort's contract management platform (system) were effective throughout the period October 1, 2019 to March 31, 2020, to provide reasonable assurance that Evisort's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Evisort 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 Evisort's service commitments and system requirements were achieved. Evisort has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Evisort 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. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- ✓ Obtaining an understanding of the system and service organization's service commitments and system requirements.
- ✓ Assessing the risks that controls were not effective to achieve Evisort's service commitments and system requirements based on the applicable trust services criteria.
- ✓ Performing procedures to obtain evidence about whether controls within the system were effective to achieve Evisort's service commitments and system requirements based on the applicable trust services criteria.

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

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 Evisort's contract management platform were effective throughout the period October 1, 2019 to March 31, 2020 to provide reasonable assurance that Evisort's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

linford&co llp

April 1, 2020
Denver, Colorado

Section II –Assertion of Evisort's Management

April 1, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within Evisort Inc.'s (Evisort or the company) contract management platform throughout the period October 1, 2019 to March 31, 2020, to provide reasonable assurance that Evisort's services commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in Section III, and identifies the aspects of the system covered by our assertion.

We have prepared an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2019 to March 31, 2020 to provide reasonable assurance that Evisort's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Evisort's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III.

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 October 1, 2019 to March 31, 2020, to provide reasonable assurance that Evisort's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Jake Sussman
Chief Operating Officer

Section III – Evisort's Description of Its Contract Management Platform

Overview of Operations

Evisort Inc. is an advanced contract analytics solution, allowing end-to-end contract management through a single platform. Evisort streamlines contract workflow using advanced AI to extract, classify, and track key provisions in documents, all delivered through a cloud-based platform. Evisort provides the ability to upload, access, search, monitor, deliver results, and run reports seamlessly across all lines of business. Evisort facilitates the entire contracting process, from contract generation to benchmarking and analytics.

Principal Service Commitments and System Requirements

Evisort designs its processes and procedures to meet objectives for its contract management platform. Those objectives are based on the service commitments that Evisort makes to user entities and the compliance requirements that Evisort has established for their services.

Security commitments to user entities are documented and communicated in their 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 design of the contract management platform are implemented 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.
- Controlled access to the production environment and the supporting infrastructure.
- Segregation of client data.
- Monitoring of system performance metrics and critical application services.

Evisort establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Evisort 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 networks are managed, and how employees are hired and trained.

Subservice Organizations: Evisort uses subservice organizations to achieve operating efficiency and to obtain specific expertise. The following are the principal subservice organizations used by Evisort:

- ✓ **Amazon Web Services (AWS)** – AWS hosts Evisort's production IT environment and provides certain managed services including firewall management and data backup services. AWS undergoes an annual Type II SOC 2 examination and the report may be obtained directly from them. Evisort obtains and reviews the SOC 2 report provided by AWS related to their hosting

operations to determine whether controls are designed and operating effectively AWS. Additionally, any listed complementary user entity controls in the AWS SOC reports are also reviewed and addressed by Evisort.

- ✓ **Vanta, Inc.** – Vanta is an automated continuous compliance monitoring software used by Evisort. Vanta provides ongoing monitoring of controls in place at Evisort to provide alerts if any control is out of compliance. Vanta has a security information page as part of their client site, and Evisort reviews the security information and inquires of Vanta if additional information is needed.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities for the Security Criteria

A company's control environment reflects the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. The control environment is not specific to any individual transaction but applies to the company as a whole. These types of controls are necessary to facilitate the proper functioning of activity-level controls supporting Evisort's contract management platform. Throughout this section, a description of the five components of internal control (control environment, risk assessment, information and communication, monitoring, and control activities) as they relate to the services Evisort provides to its clients.

The controls supporting the control objectives identified by Evisort were used to evaluate the suitability of the design and operating effectiveness of controls stated in the description. Control objectives and controls designed and implemented to meet them ensure that the system is protected against unauthorized access (both physical and logical). Entity-level controls and specific control activities supporting the applicable trust services criteria are provided in the descriptions of this section of the report.

Control Environment

A board of directors exercises independent oversight of Evisort's strategic direction, operational performance, and internal control. Evisort's board of directors is made up of internal executives as well as external leadership. The board of directors sets the tone at the top of the organization that is followed by all employees. The tone is demonstrated through their directives, actions, and behavior and highlights the importance of integrity and ethical values to support the functioning of the system of internal control. The board of directors meeting occurs at least once a quarter. To help ensure expectations are understood by employees, executive management has established a code of conduct. The primary goal of Evisort's code of conduct is to foster inclusive, collaborative, and safe working conditions for all Evisort staff.

Evisort is committed to providing a friendly, safe, and welcoming environment for all staff, regardless of gender, sexual orientation, ability, ethnicity, socioeconomic status, and religion. The code of conduct applies to all Evisort full-time, part-time, and contractor staff and includes the following sections: culture and citizenship, accepted and expected behavior, unacceptable behavior, weapons policy, sanctions for non-compliance, and reporting violations.

Continuous Independent Compliance and Security Monitoring: Evisort uses a tool called Vanta which objectively and continuously monitors the Evisort control environment and alerts management when many types of internal control and security issues arise.

Organizational Structure: Management has established structures, reporting lines, and appropriate authorities in the pursuit of Evisort's business objectives. The structures, reporting lines, and authority are clearly communicated through management's operational style, the organizational structure, policies and procedures, and employee job descriptions. Evisort's organizational structure is organized into several departments including: Engineering, Sales, Data, and Operations. The role of Security Officer has been assigned and communicated throughout the organization. The Security Officer is responsible for the security of Evisort's systems.

Hiring: When a position is open at Evisort, a job description and listing will be posted on Evisort's website, as well as on other job forums. Additionally, Evisort sources candidates via referrals, and external recruiting agencies. Resumes of applicants are received and reviewed by the hiring manager. An initial phone screening is performed, followed by a video/phone in-depth interview or take-home test. Lastly, there is a final round interview on-site with team members. The interview process is tailored to match the position being hired. Candidates are managed in an applicant tracking system to help interviewers assess the right skills, traits and qualifications with data-driven hiring decisions. Reference checks are performed after the final round interview before a final decision on the candidate is made. Following the in-person interview and the reference checks, candidates with most or all of the desired attributes are extended an offer for employment. Once an applicant is selected internally, an offer letter is sent to the selected applicant, which states that the applicant will be hired pending a successful background check. Applicants for full-time Evisort employment that may have access to client data are required to complete a successful background check, which includes a social security verification, federal and state criminal check, global watchlist, national search, county searches, and sex offender database check.

New Hires: Onboarding consists of completing the employment documentation and reviewing and acknowledging all policies and procedures. Employees are required to complete Evisort security awareness training within 30 days of hire, and annually thereafter.

Performance and Feedback: Evisort evaluates competence across the entity in relation to established policies and practices and acts as necessary to address shortcomings. Evisort has a procedure for evaluating employee performance and feedback on an annual basis. Evisort believes feedback is forward-looking and is information that someone can use to grow and develop. Performance assessments, however, look to the past to discover how an individual performed over the last year. Feedback is also provided informally on an ongoing basis.

Employment-at-Will: All new hires sign an employment agreement with the Company that includes "at-will" employment language. As part of the terms of the employment agreement with individuals, Evisort maintains the right to discipline or terminate individuals based on a pattern of poor job performance. Additionally, under at-will employment law, employees can be terminated at any time for any reason.

Communication and Information

Internal Control Monitoring: Evisort obtains or generates and uses relevant, quality information to support the functioning of internal control. Evisort uses a variety of methods to monitor production systems and internal controls. The methods include the Vanta tool for monitoring internal controls relevant to SOC 2 compliance, as well as application and infrastructure monitoring tools and penetration testing.

Internal Communication: Evisort maintains security policies to communicate security responsibilities to Evisort personnel. The policies include objectives and responsibilities for internal control necessary to support the functioning of internal control. Policies are reviewed at least annually and updated as necessary. In addition to policies and procedures, Evisort uses an internal communication tool that is used for collaboration and communication including responsibilities related to security. The communication tool is used by entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls to communicate about responsibilities, including changes in responsibilities.

Annual Security Awareness Training: To assist with Evisort's commitments to security, Evisort management provides annual security awareness training for all employees that covers information security, data protection, and confidentiality of client information.

External Communication: Evisort has also created a high-level overview of the Evisort system used to describe the services provided to the clients that Evisort serves. Evisort and their clients' responsibilities and commitments regarding the acceptable use of the Evisort system are included within the Evisort Master Services Agreement (MSA), which clients must agree to before using the Evisort system. The Evisort site https://status.evisort.com communicates changes and status to the application and the impact on users.

Incident Reporting: Evisort has provided information to clients and employees on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by Evisort in the event there are problems. Clients may contact Evisort support at via the Evisort support email at support@evisort.com or the customer service phone number at 1-888-Evisort. There is also a training center site for customers with instructions on different features in the Evisort platform (https://www.notion.so/Training-Center-6f7f7a2659bc4f189937760341676fb1). Evisort personnel may contact their supervisor to report important matters requiring attention.

Risk Management

Evisort Risk Assessment and Management Program: Evisort's Risk Assessment and Management Program policy describes the processes Evisort has in place to identify new business and technical risks and how frequently those risks are mitigated. The policy designates responsibility for risk management at Evisort and outlines the process for identifying and addressing risks to the confidentiality, integrity, and availability of client data that Evisort accesses, stores, and transmits. The policy is made available to all employees through the Company's Vanta tool.

Principles: Evisort specifies risk management objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. Evisort is proactive in its approach to risk management, balancing the cost of managing risk with anticipated benefits, and undertaking contingency planning in the event that critical risks are realized. Evisort's primary duty is to ensure the security, availability, and confidentiality of critical systems and customer data. The duty to ensure a secure and available infrastructure requires Evisort to identify and manage risks.

Evisort believes that effective risk management involves:

1. A commitment to the security, availability, and confidentiality of Evisort infrastructure and services from senior management;
2. The involvement, cooperation, and insight of all Evisort staff;
3. A commitment to initiating risk assessments, starting with discovery and identification of risks;
4. A commitment to the thorough analysis of identified risks;
5. A commitment to the strategy and treatment of identified risks;
6. A commitment to communicate all identified risks to the company;
7. A commitment to encourage the reporting of risks and threat vectors from all Evisort staff.

Evisort believes that the following events should trigger a risk assessment to occur:

1. A significant and major change to existing infrastructure, product, or business practices;
2. A significant amount of time (e.g., a year) has passed since the last risk assessment.

Scope: The Risk Assessment and Management program applies to all systems and data on the Evisort network, owned by Evisort or its customers, or operated on behalf of the organization. Evisort risk assessments evaluate infrastructure such as computer infrastructure containing networks, instances, databases, systems, storage, and services. Evisort risk assessments also include an analysis of business practices, procedures, and physical office spaces as needed.

Risk assessments may be high level or detailed to a specific organizational or technical change as Evisort stakeholders and technologists see fit. Risk assessments must be conducted by unbiased and qualified parties such as security consultancies or qualified internal staff.

Risk Management Oversight: Overall, the execution, development, and implementation of risk assessments and remediation programs is the joint responsibility of Evisort's Security team and the department or individuals responsible for the area being assessed. All staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible.
Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Commitments

- Evisort performs at least one risk assessment annually using qualified internal staff and/or external third parties who have experience performing risk assessments.
- A risk assessment should be performed or reviewed on critical systems and applications no less than every two years.

- Risk assessments should be used to assess all risks to the organization.
- All staff involved in a risk assessment must fully cooperate with the risk assessment project lead conducting the assessment and developing a remediation strategy.
- Any staff members or external consultants who perform Evisort risk assessments are required to be familiar with computer technology and computer security in use by Evisort. The risk assessment project leader should be the security officer or a staff member the security officer designates to conduct the risk assessment.
- Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks. The action plan may be included with the risk assessment report, or separately. The action plan will be an action plan for implementing additional controls and solutions to mitigate or manage the risk. The action plan may define participants and actions to be taken during the implementation of the action plan.
- The risk assessment process and methodology will be updated as required due to results of audits and incidents.
- All identified vulnerabilities are assessed for impact and criticality. Vulnerabilities must be remediated as soon as possible as mandated by the Evisort Vulnerability Management & Patch Program.

Risk Assessment Process: Evisort's risk assessment methodology is based off *NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments*. Management defines the scope of the risk assessment and creates the risk assessment team with a point person to guide the process (risk assessment project lead). If risk assessment procedures are not defined, the team must define them. The proper time and method of communicating the selected risk treatment options to the affected IT and business management should be included.

- Determine if the system is critical to the organization's business processes and determine the data classification and security needs of the data on the system according to the Evisort Data Classification Policy, considering security, availability, and confidentiality needs.
- List possible threat sources such as an exploitation of a vulnerability.
- Identify vulnerabilities.
- Evaluate potential security controls already in place to assess if they adequately address the risk.
- Identify probability of exploitation. Additional security controls may need to be in place before the probability of exploitation is lowered.
- Categorize the damage (impact) and possibly place a dollar amount on the damage where possible.
- Use (likelihood * impact) to quantify the amount of risk.
- List specific vulnerabilities and threats to the system and identify mitigating controls.
- Identify existing controls and those that may further mitigate specific vulnerabilities.
- Create the risk assessment report.
- Communicate the selected risk treatment options to the affected IT and business management staff.
- Take recommended risk mitigation actions. Record such actions as changes per the Evisort Change Management program.
- Monitor the effectiveness of risk mitigation actions and document the results.

Vendor Risk Management: Evisort relies on vendors to perform a variety of services, some of which are critical for operations. Evisort aims to manage its relationship with vendors and minimize the risk associated with engaging third parties to perform services. The Vendor Risk Management policy provides a framework for managing the lifecycle of vendor relationships. Risk assessments for vendors are covered under Evisort's Vendor Management Program, which includes a thorough risk assessment targeted at a particular vendor's security, business practices, and legal commitments.

Fraud Risk: Evisort has considered the potential for fraud when assessing risks to the achievement of objectives. There is low risk of fraud since the Evisort application is used for purposes that does not allow the transfer of money.

Change Identification and Risk Assessment Evisort's risk identification process considers changes to the existing infrastructure, product or business practices in which the entity operates.

Logging and Monitoring

Application Logging and Monitoring: Evisort uses monitoring tools to monitor application health and these monitoring tools alert system administrators when the application in not operating within defined boundaries. When alerts from the tools are received, they are followed up on until they are resolved.

Infrastructure Logging and Monitoring: Evisort also logs authentication, availability, and error events and uses tools for infrastructure monitoring.

Audit Reduction, Review, and Analysis: Audit logs must be managed and protected to ensure they accurately reflect the activities conducted on organizational systems; however, if audit logs are not reviewed and analyzed, they will be of little use to an organization to detect an intrusion, actual or attempted. If audit logs are not managed, protected, and analyzed, attackers can erase their tracks, hide more efficiently, and persist their presence in corporate environments.

Evisort Vulnerability Management and Patch Program: Evisort's Vulnerability Management policies and procedures describe what is in place to monitor for new vulnerabilities, how often vulnerabilities are addressed, and the way in which those new vulnerabilities are addressed.

On average, 20-30 new vulnerabilities are released into the wild every day. Evisort's internal vulnerability monitoring and external vulnerability scanning are in place to keep up with new threats while validating security controls put in place so that Evisort's security posture is maintained.

Vulnerability Management and Patch Policy: Evisort performs internal vulnerability scanning and package monitoring on a continuous basis using Cloudcheckr, AWS Inspector, Pen testers, a Bug Bounty Program (CESPPA), and the Vanta Continuous Security and Compliance Monitoring tool. The security team is responsible for communicating detected vulnerabilities and package updates needed to the appropriate engineering staff for resolution. Engineering staff are responsible for various infrastructure

components are responsible for resolving detected vulnerabilities in a timely manner as defined by Evisort's timing standards. Evisort has automated OS updates and security patching performed bi-weekly on the production environment.

Severity and Timing: Evisort defines the severity of an issue via industry-recognized Common Vulnerability Scoring System (CVSS) scores, which all modern scanning and continuous monitoring mechanisms utilize. The CVSS provides a way to capture the characteristics of a vulnerability, and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Vulnerability and Patch Management Process Flow:

1. A new vulnerability or a new patch is detected from the various monitoring and scanning Evisort has in place.
2. The security team enters vulnerability or patch details and instructions into Evisort's change management system, which is JIRA, and assigns the ticket to the appropriate team member to address.
3. The ticket assignee follows the change management process to implement the necessary change to apply the patch or address the new vulnerability.
4. The ticket is updated with results from the applied change, detailing any exceptions into the Evisort risk register.
5. The security team checks the source from which the vulnerability originated to ensure that the change performed has addressed the vulnerability detected. The ticket is updated with the results and closed out.

Responsible Disclosure Program: In addition to monitoring for vulnerabilities using scans and tools, Evisort has implemented a responsible disclosure program for users to report issues and vulnerabilities associated with their use of the Evisort application.

SOC 2 Common Criteria/Security: Evisort has a SOC 2 performed annually covering the Common Criteria which includes Security. During the examination, a number of Evisort's internal controls are tested and issues with design and operating effectiveness are brought to management's attention for remediation.

Penetration Testing: Evisort periodically has a third-party application penetration test performed. Issues identified during the tests are remediated as necessary.

Control Activities

Evisort selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. Control activities include a variety of controls and may include a balance

of approaches to mitigate risks, considering both manual and automated controls as well as preventive and detective controls. Management has established and implemented policies and procedures to ensure periodic assessments and evaluations are performed that consider all elements of security as it applies to the AICPA Trust Services Criteria. The policies include control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats. Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary. In addition, management takes corrective action when issues are identified with control activities.

Logical and Physical Access

Evisort System Access and Authorization Control Policy: Each Evisort employee, contractor, and associate has limited access to Evisort systems and applications. Access is always provisioned on a minimum-necessary (least-privilege) basis. Evisort's System Access and Authorization Control Policy documents the requirements for registering and authorizing employees prior to being issued system credentials and granted the ability to access the system.

Employee Access to Evisort Systems: Access to Evisort systems and third-party accounts owned by Evisort are only granted on a need-to-use basis, as defined by the responsibilities of the position held and the duties of the position. Access control and management is divided into multiple phases of the account lifecycle which include creation, privilege management, authorization, password management, audit, and revocation.

Authorization - Role Based Access Control: In most cases, Evisort employees are granted access to Evisort systems according to their role and/or team. The executive team and team managers are jointly responsible for maintaining a list of roles and associated access scope for team members. If an Evisort employee requires access outside of the standard for their role or team, either they or their managers may initiate an access request, following the policy outlined in "Creation - Access Requests," as follows.

Creation - Access Requests: Access requests for Evisort employees are made by authorized employees. An onboarding checklist is used for initial access provisioning of new hires. Access requests should be made to the Evisort employee or employees who manage the relevant resource(s). Those employees will not grant access unless they are satisfied the additional access is necessary for the grantee to complete a necessary business task. In addition, the employee(s) must accept the company's Acceptable Use Policy before access will be granted. When granting access, employees will ensure grants are scoped to the minimum duration to complete the relevant business task. Root access is not granted unless absolutely necessary to perform the job function.

Account Audit: The responsible team will conduct continuous audits of accounts, privileges, and password management, and is required to document access change requests in JIRA.

Revocation: Role Changes and Termination: Managers must notify the company's Operations team if an employee has been terminated or changes roles. In the case of termination, the former employee's access is required to be revoked immediately. In the case of a role change, the employee's access should be revised

within three days after changing roles. In some cases, access will be revoked as a disciplinary measure for policy violation.

Complementary User Entity Control: *User entities are responsible for provisioning and de-provisioning users' access to the user entity's instance.*

Administrator and Remote Access: Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions. Two-factor authentication is required to access production data. Remote access to the production infrastructure is limited to authorized individuals and utilizes industry standard encryption protocol.

Access to Client Data: Client data is stored within Evisort's production database instance. Access to client data within the Evisort production database by Evisort employees is restricted to authorized users. In addition, client users have access to their data only and no other clients' data.

Encryption of Client Data: Evisort understands the sensitivity of its clients' data and has therefore implemented security controls to protect the confidentiality of the data. Client data within Evisort's production databases is encrypted.

Infrastructure Authentication: Multifactor authentication is required for administrator access to the AWS infrastructure.

Workstation Use and Security: The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment. The guidance is appropriate to the workstation type (e.g., fixed workstation, portable workstation/laptop computer, tablet computer, smartphone, etc.) and location (e.g., office, home, public place, etc.).

Session Lock: Employee workstations are required to be configured to automatically log off after a modest period of inactivity.

Physical Access: Only authorized individuals (e.g., employees and building management) are allowed to access the Evisort office. Access to non-main entrance doors of the Evisort office is controlled by the employee's phone through Nexkey. When an employee terminates employment, their Nexkey access to the Evisort office is removed. Nexkey access is also reviewed on a monthly basis.

Inventory of Information Assets: Evisort maintains an inventory listing of servers and workstations in order to protect them from security events, maintain the confidentiality of data, and ensure availability. The inventory is dynamically built and constantly updated by the Vanta tool which looks to AWS to see which virtual machines are running. Vanta also prompts management to classify and document information related to each machine.

Virtual Private Cloud (VPC): Cloudflare is used to manage the Evisort Virtual Private Cloud (VPC). VPC rules are configured to block unauthorized traffic into the production network. Access to modify VPC rules is restricted to authorized individuals.

Laptop Encryption: To minimize the risk of data being compromised in the event hardware or data is lost or stolen, all Evisort laptops are encrypted.

Transmission Encryption: Whether web-based or via mobile applications, all data transfers between users and the Evisort system are secured using Transport Layer Security (TLS) and industry standard encryption. Evisort has also documented a cryptography policy that outlines the requirements for encrypting data and transmissions.

Removable Media: Evisort has taken measures to restrict employee use of removable media to help mitigate both the risk of data loss as well as the risk of malware being introduced onto Evisort systems. By policy, the use of removable media is not allowed.

Hardware and Data Disposal: Evisort's policies related to data protection address the handling of devices and media that may potentially contain sensitive Company or client data, including personally identifiable information (PII). Evisort defines specific requirements for hardware and data disposal in its security policies.

System Operations Controls

Incident Response Program: Evisort has a documented Incident Response Plan (IRP) which establishes the procedures to be undertaken in response to information security incidents. The IRP has been communicated to appropriate personnel and includes the following:

- Escalation procedures
- Incident severity identification and classification
- Roles, responsibilities, and communication strategies in the event of a compromise, to include designation of an Incident Response Team
- Containment and eradication strategies
- Communications protocols, internally and externally
- A retrospective analysis to determine the root cause and implement incident response enhancements

The IRP is updated annually, and more frequently based upon incident outcomes and lessons learned, as appropriate. In years that security incidents do not occur, Evisort conducts a test of the IRP and the ability of the Incident Response Team to execute the plan on an annual basis and documents the test procedures and test results. Gaps, areas of improvement, and lessons learned are utilized to modify the plan, as needed.

Incident Monitoring and Recordkeeping: Evisort maintains a record of security incidents. The incident records include a description of the incident and relevant facts (e.g., information that was disclosed), mitigations, risk assessment, and outcomes.

Antivirus and Patching: Evisort deploys malware detection software on all workstations that can access the production environment and has configured malware detection software to perform daily scans with immediate notification if malware is detected. Evisort applies security patches to user workstations constantly, so at any given time workstations are on the most current or next most current operating system version. Production servers are monitored continuously within AWS and patches are applied for known vulnerabilities.

Change Management

An effective system development and maintenance process is critical to the availability and integrity of Evisort's system. Evisort is a proprietary and in-house developed system where custom changes are often necessary to enhance system functionality. Evisort follows a defined development policy for making changes to the system used to support the services provided to their clients. Evisort's Change Management Policy describes how changes to the Evisort system are proposed, reviewed, deployed, and managed. The policy covers all changes made to the Evisort software, regardless of their size, scope, or potential impact.

The policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted computer performance
- Productivity loss
- Introduction of new vulnerabilities, configuration errors, and software bugs in infrastructure and code
- Exposure to reputational risk

A request for a change can come internally from management or externally from a client. A project management tool is used to track which changes are authorized for development. Once assigned, an engineer develops the change and then oversees any needed testing or peer reviews. For code changes, engineering uses a software development platform to manage and record activities related to the change management process. The tool enforces version control and is used to document control points within the change management process.

Once a change is ready for deployment to production, the assigned engineer submits the change's pull/merge request for peer review, testing, and approval to release the change to production. Once approved in the pull/merge request, a product manager releases the change to production. Evisort also communicates product updates with stakeholders at: https://www.notion.so/Recently-Released-Features-19a6b757b13a441d9a0e869cce48af33.

Authorization to Implement Changes: Evisort restricts the ability to implement changes into the production environment to only those individuals who require the ability to implement changes as part of their job function.

Change Logging & Monitoring: A Gitlab notification is automatically sent out to a Slack channel of appropriate employees whenever code is deployed to production.