jack henry
& ASSOCIATES INC.®

Jack Henry & Associates Inc. – Ensenta

Type II System and Organization Controls Report (SOC 2)

Report on a Service Organization's Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Processing Integrity Throughout the Period October 1, 2019, to September 30, 2020.

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations™

KP KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

SECTION I:
ASSERTION OF JACK HENRY & ASSOCIATES INC. – ENSENTA MANAGEMENT

ASSERTION OF JACK HENRY & ASSOCIATES INC. – ENSENTA MANAGEMENT

We have prepared the accompanying description in section III titled "Jack Henry & Associates Inc. – Ensenta's Description of Its Payment Processing Services System" throughout the period October 1, 2019, to September 30, 2020, (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 payment processing services system that may be useful when assessing the risks arising from interactions with Jack Henry & Associates Inc. – Ensenta's system, particularly information about system controls that Jack Henry & Associates Inc. – Ensenta 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, Availability, and Processing Integrity (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*).

Jack Henry & Associates Inc. – Ensenta uses NCR and RagingWire to provide SaaS data center services and data center colocation services, respectively. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Jack Henry & Associates Inc. – Ensenta, to achieve Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements based on the applicable trust services criteria. The description presents Jack Henry & Associates Inc. – Ensenta's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Jack Henry & Associates Inc. – Ensenta's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Jack Henry & Associates Inc. – Ensenta, to achieve Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements based on the applicable trust services criteria. The description presents Jack Henry & Associates Inc. – Ensenta's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Jack Henry & Associates Inc. – Ensenta's controls.

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

a. the description presents Jack Henry & Associates Inc. – Ensenta's payment processing services system that was designed and implemented throughout the period October 1, 2019, to September 30, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Jack Henry & Associates Inc. – Ensenta's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Jack Henry & Associates Inc. – Ensenta's controls operated effectively throughout that period.

SECTION II:
INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

The Board of Directors
Jack Henry & Associates Inc.
663 W. Highway 60
Monet, MO 65708

Scope

We have examined Jack Henry & Associates Inc. – Ensenta's accompanying description in section III titled "Jack Henry & Associates Inc. – Ensenta's Description of Its Payment Processing Services System" throughout the period October 1, 2019, to September 30, 2020, (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 and operating effectiveness of controls stated in the description throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Processing Integrity (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*).

Due to the global pandemic declared by the World Health Organization on March 11, 2020, physical and environmental controls could not be tested; instead, controls were corroborated through remote inspection of related systems and tools.

The information included in section V, "Other Information Provided by Jack Henry & Associates Inc. – Ensenta That Is Not Covered by the Service Auditor's Report," is presented by Jack Henry & Associates Inc. – Ensenta management to provide additional information and is not a part of the description. Information about Jack Henry & Associates Inc. – Ensenta's user access revocation process has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements based on the applicable trust services criteria.

Jack Henry & Associates Inc. – Ensenta uses NCR and RagingWire to provide SaaS data center services and data center colocation services, respectively. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Jack Henry & Associates Inc. – Ensenta, to achieve Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements based on the applicable trust services criteria. The description presents Jack Henry & Associates Inc. – Ensenta's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Jack Henry & Associates Inc. – Ensenta's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, 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 Jack Henry & Associates Inc. – Ensenta, to achieve Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements based on the applicable trust services criteria. The description presents Jack Henry & Associates Inc. – Ensenta's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Jack Henry & Associates Inc. – Ensenta'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

Jack Henry & Associates Inc. – Ensenta 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 Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements were achieved. In section I, Jack Henry & Associates Inc. – Ensenta has provided its assertion titled "Assertion of Jack Henry & Associates Inc. – Ensenta Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Jack Henry & Associates Inc. – Ensenta 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 and operating effectiveness 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 and operated effectively 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 and operating effectiveness 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 or did not operate effectively
- 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 on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on 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 users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating 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 policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

a. the description presents Jack Henry & Associates Inc. – Ensenta's payment processing services system that was designed and implemented throughout the period October 1, 2019, to September 30, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Jack Henry & Associates Inc. – Ensenta's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2019, to September 30, 2020, to provide reasonable assurance that Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Jack Henry & Associates Inc. – Ensenta's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of Jack Henry & Associates Inc. – Ensenta, user entities of Jack Henry & Associates Inc. – Ensenta's payment processing services system during some or all of the period October 1, 2019, to September 30, 2020, business partners of Jack Henry & Associates Inc. – Ensenta subject to risks arising from interactions with the payment processing 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.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

December 22, 2020

SECTION III:
JACK HENRY & ASSOCIATES INC. – ENSENTA'S DESCRIPTION OF ITS PAYMENT PROCESSING SERVICES SYSTEM

OVERVIEW

Services Provided

Jack Henry & Associates, Inc. ® (Jack Henry) was founded in 1976 as a provider of core information processing solutions for community banks. Today, Jack Henry's extensive array of products and services includes processing transactions, automating business processes, and managing information for approximately 9,000 financial institutions and diverse corporate entities. Jack Henry provides its products and services through three primary business brands:

- **Jack Henry Banking®** is a leading provider of integrated data processing systems to approximately 1,000 banks ranging from community banks to multi-billion-dollar institutions with assets of up to $50 billion. Jack Henry's banking solutions support both in-house and outsourced operating environments with three functionally distinct core processing platforms and more than 140 integrated complementary solutions.
- **Symitar®** is a leading provider of core data processing solutions for credit unions of all sizes, with more than 800 credit union customers. Symitar markets two functionally distinct core processing platforms and more than 100 integrated complementary solutions that support both in-house and outsourced operating environments.
- **ProfitStars®** is a leading provider of highly specialized core agnostic products and services to financial institutions that are primarily not core customers of the Company. ProfitStars offers highly specialized financial performance, imaging and payments processing, information security and risk management, retail delivery, and online and mobile solutions. ProfitStars' products and services enhance the performance of traditional financial services organizations of all asset sizes and charters, and non-traditional diverse corporate entities with approximately 9,000 customers, including over 7,200 non-core customers.

Jack Henry's products and services provide its customers solutions that can be tailored to support their unique growth, service, operational, and performance goals. Its solutions also enable financial institutions to offer the high-demand products and services required by their customers to compete more successfully, and to capitalize on evolving trends shaping the financial services industry. Additional information is available at jackhenry.com.

Jack Henry & Associates Inc. – Ensenta (Ensenta) is a leading provider of real-time, cloud-based solutions for mobile and online payments and deposits. Ensenta currently serves more than 1,100 financial institutions and government agencies with patented technologies supporting the ATM, mobile, online desktop, merchant, and branch channels. With the addition of Ensenta, Jack Henry & Associates now supports approximately 2,300 financial institutions with remote deposit capture solutions. These proven payment technologies mitigate risk, minimize compliance exposure, increase back office efficiencies, and improve funds availability for consumers and businesses.

Ensenta is a part of Jack Henry & Associates, Inc. (Jack Henry) Payment Solutions. Payment Solutions also includes: iPay Solutions (iPay), Card Processing Solutions (CPS) and Enterprise Payment Solutions (EPS).

Ensenta provides imaging and digital deposit services for financial institutions (FI). Ensenta provides imaging and digital deposit services for FI, businesses, and government agencies, including the following:

- **EZAdmin** – Allows FI to centrally monitor and process check deposit transactions. Transactions originate from sources such as ATMs, mobile banking, and online deposits; payment cards are used to identify the user's account so that they can deposit checks.

- **Branch Capture** – Branch tellers scan checks and send them electronically for processing via EZAdmin.

- **Check Image ATM** – Customers configure their ATMs to scan checks and submit them electronically for processing to the Ensenta platform over IPsec virtual private network (VPN).

- **Partner ATM** – Customers configure their ATMs to scan checks and submit them electronically for processing to the Ensenta Platform over IPsec VPN or secure configurations of TLS 1.1 or higher.

- **Mobile API** – Account holders deposit checks using mobile phone camera.

- **My Deposit 3.0** – Web-based application that enables customers to deposit checks one at a time.

- **Business Remote Deposit Capture (bRDC)** – Enables small business customers to deposit multiple checks from the convenience of their office or smartphone. Ensenta supports real-time and batch versions, using duplex scanners that read both sides of the check in a single pass.

- **Government Collections App** – Enables government agencies to process remittance data and check payments with one user interface, provide barcode proof-of-purchase for guaranteed delivery of services, and support EMV-certified mPOS with credit/debit/e-payment and/or checks. Facilitates inter-agency collections with shared payment networks and integrates with existing government payment hubs and software platforms. Mobile apps can be used strictly by government agents or the general public.

- **Public App** – An application that is downloaded onto a mobile device allowing the customer to make a payment for goods or services to the government. The mobile interface presents a form for payment (a frame API) and starts an anonymous session with pay.gov. The payment information is entered by the customer directly on the pay.gov site (Ensenta does not have access to the information entered on the pay.gov site). A receipt with a QR code is generated by the Public App. The customer then provides the QR code to the government agency to redeem their purchase or service. No credit card numbers, or sensitive authentication information is stored.

Internal Control Framework

Jack Henry's Framework of Internal Control is based on the 2013 COSO (Committee of Sponsoring Organizations of the Treadway Commission) Framework which is comprised of Entity Level Controls (ELCs) that are enterprise wide and have a pervasive effect toward the achievement of Jack Henry's operating, reporting, and compliance objectives while guarding against inherent risks. Jack Henry's ELCs have been mapped to components and principles of frameworks such as COSO and COBIT. Each of the components and principles are required to be present and functioning and operating together in an integrated manner.

Control Environment

Jack Henry has a defined governance structure comprised of a Board of Directors, Executive Officers, and various Board and management strategic committees. The Board of Directors is independent from management and is granted charter authority and responsibility to carry out its oversight responsibilities. The full Board of Directors is updated quarterly on activities of each Board Committee. Jack Henry's Board of Directors adheres to governance principles, as specified in a set of Corporate Governance Guidelines, including setting the tone-at-the top, and a commitment to ethics and integrity. The Board has delegated certain authority to four committees: (1) Audit Committee, (2) Risk and Compliance Committee (3) Governance Committee, and (4) Compensation Committee, each with a written charter. Committees meet and report regularly to the Board. The Board receive periodic training and educational material to keep up to date on emerging trends and topics.

Board of Directors

The Board of Directors and senior management have formulated a set of policies on integrity, ethics, and core values. These policies are displayed on Jack Henry's internal intranet and on newsletters. The core values depict the guidelines by which every employee ("associate", "staff" or "personnel")) at Jack Henry, and the company as a whole, operates to fulfill the mission in a manner consistent with the organization's philosophy. Reporting and monitoring are aligned with roles and responsibilities. Internal control structures are guided by COSO, COBIT, ITIL, and NIST frameworks. Regulatory requirements and industry standards, together with security and operational considerations, influence control design.

Audit Committee

The Audit Committee is comprised of members of the Board of Directors who are independent of the company. The Audit Committee oversees the internal audit function by reviewing and approving Corporate Audit Services staffing, audit plans, published reports, and performance benchmarks. The Audit Committee also oversees the engagement of System and Organization Controls (SOC) audits and the annual financial statement audit. Corporate Audit Services is subject to recurring federal financial institution regulatory agency reviews and Quality Assessment Reviews required by the Institute of Internal Auditors (IIA) International

Professional Practices Framework (IPPF). Corporate Audit Services is considered operationally independent.

Risk and Compliance Committee

The Risk and Compliance Committee of the Board of Directors is responsible for oversight of corporate compliance, business continuity planning and testing, information security, and Enterprise Risk Management (ERM). The Vice President of ERM provides pertinent reports and metrics to the Risk and Compliance Committee for review.

Governance Committee

The Governance Committee of the Board of Directors is responsible for board governance, which includes performing periodic assessments to determine whether the board and its committees are functioning effectively according to the minimum background and skills.

Compensation Committee

The responsibilities of the Compensation Committee of the Board of Directors include establishing goals and objectives for senior executive officers, evaluating performance of the senior executive officers, and approving compensating, bonus and other incentive compensation progress for Jack Henry senior executive officers.

Code of Conduct

Management has published a Code of Conduct and an Employee Handbook that applies to Jack Henry board members, executive management, and employees, and is provided upon hire, communicated to Jack Henry employees periodically, and upon departure from the company. Employees must acknowledge acceptance of the Jack Henry Employee Handbook (including the Code of Conduct) annually or each time the Employee Handbook is revised. Jack Henry has established a Corporate Ethics program allowing employees, contractors and vendors to submit anonymous e-mail or telephone (voicemail) reports of any noted violations of the Code of Conduct. These submissions are reviewed and tracked to resolution. Submission summaries are provided to the Board of Directors via the Audit Committee, and the Risk and Compliance Committee. Jack Henry has published its expected code of conduct for business partners and vendors on the company's website.

Human Resources Policies

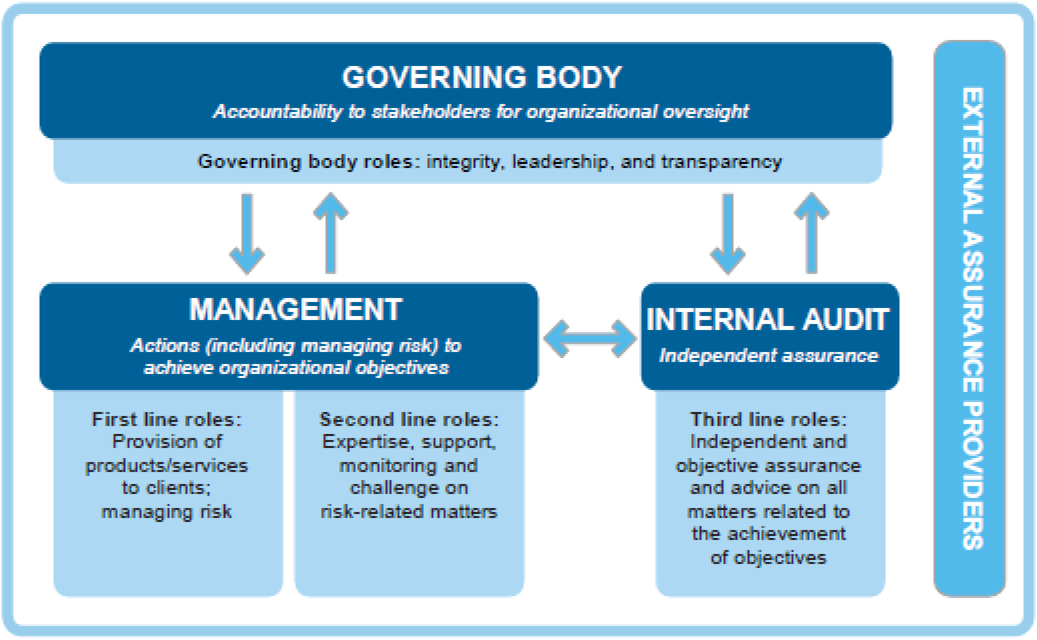
Management has established and periodically updates standards for hiring individuals. The Human Resources department updates materials outlining Jack Henry's policies and procedures on attracting, training, coaching, evaluating, and retaining personnel. Prior to hiring new employees background checks and drug screens are performed. Non-disclosure agreements (Propriety Rights and Confidentiality Agreement) are signed upon hire. Job descriptions are available for positions within the company. Training and awareness programs are provided to employees to promote ethical behavior throughout the organization and to develop and retain sufficient and competent personnel. Appropriate training is provided upon hire to familiarize individuals with Jack Henry, and ongoing training is provided as deemed necessary to assist in employees having the appropriate skills to perform assigned responsibilities. The performance of each employee is reviewed annually by management.

Organizational Structure

The organization is structured to define lines of authority and effectively communicate important information to various levels and departments within the organization. Management evaluates the organizational structure as the company evolves, for continued effectiveness and efficiency to support Jack Henry's objectives. Organizational structure is appropriate given Jack Henry's size, complexity of operations, and geographic locations. Lines of authority are published within organizational charts posted to the Jack Henry's intranet. Senior Management develops a succession plan across the company, which is updated periodically.

Corporate Audit Services has championed adoption of the IIA's Three Lines Model. When following the model, as illustrated below, responsibilities among various functions of the organization are generally classified as follows:

- First line roles: provision of products/services to clients; managing risk
- Second line roles: expertise, support, monitoring and challenge on risk-related matters
- Third line roles: independent and objective assurance and advice on all matters related to the achievement of objectives


GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership, and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS

Although governing bodies are not considered to be among the three lines, no discussion of risk management systems could be complete without also considering the essential role of the governing bodies (i.e., boards of directors or equivalent bodies). Governing bodies are the primary stakeholders served by the lines, and they are the parties best positioned to determine that the Three Lines Model is reflected in the organization's risk management and control processes.

Risk Assessment

The ERM Framework, implemented by the Corporate Compliance and Risk Management Department, provides guidance and information related to the tolerance, response, and assurance of risks identified across the organization, including those related to external financial reporting objectives. The program drives awareness throughout the organization through active management of business unit risks to protect and grow the business units and organization as a whole. Jack Henry's ERM Committee (ERMC) is chaired by the Vice President of ERM. ERMC meeting participants include Executive Management, divisional Vice Presidents, and business unit managers representing a wide range of operations. Assessment of the significance of risks to the achievement of business objectives is performed as part of risk analysis, such that an appropriate balance between risk and reward is maintained. Business unit risks are evaluated against various standards through the use of risk dashboards and score cards, as part of the ERM process. These documents and the underlying processes capture the potential significance of identified risks based on the likelihood and impact. Risk inputs are derived from a number of sources, including but not limited to, industry research, management self-assessments, client and employee surveys, audits, vulnerability assessments, and compliance reviews. Observations and action items from assessments are documented, classified and tracked for resolution through jGRC and reporting periodically to relevant stakeholders. Based on the assessed risks within the company, insurance coverage has been obtained to minimize the impact of any loss events.

Individual business units are responsible for assessing their risks and implementing appropriate controls to avoid, transfer, share, mitigate, or accept identified risks. Once a risk is identified and assessed, the corresponding business unit is responsible for the mitigating strategy of that risk. The risk score card includes information such as the risk response and activities to mitigate the risks. Each business unit is responsible for ongoing monitoring of risks and documenting risk mitigation. Formalized assurance is provided through Corporate Audit Services. ERM oversight, including review and guidance of risk decisions and responses, is provided by the Audit Committee, the Risk and Compliance Committee, the ERMC, Chief Risk Officer, and the Vice President of ERM. Management performs periodic control assessments to identify or validate the controls in place to mitigate risks to the business and the services offered. Additionally, management confirms or updates control owners for the controls.

The organization has a Chief Risk Officer (CRO) who is a member of the corporate executive team reporting to the President and Chief Executive Officer. The CRO provides oversight for the following corporate functions: Enterprise Information Security, Corporate Audit Services, Enterprise Continuity, Enterprise Risk Management, Corporate Compliance and Risk, and Occupational Risk Management.

Jack Henry has assigned a Chief Information Security Officer (CISO) who reports to the CRO and provides periodic updates to the Risk and Compliance Committee. The CISO oversees the staff responsible for implementation and monitoring of controls. The CISO is responsible for working with each business unit (BU) to develop a strategy that verifies the appropriate security practices are in place. The CISO also provides leadership in the implementation of a security program which protects Jack Henry and its clients.

The Software Security Group reports to the CISO and is responsible for establishing secure coding standards, monitoring compliance with corporate standards, performance or engagement of application security vulnerability assessments, and responding to security risks. Identified risks and mitigation strategies are discussed with management via reporting to the CRO, CISO, Enterprise Software Security Council, Corporate Security Council, ERMC, and the Risk and Compliance Committee. The Enterprise Architecture Group evaluates new technology to assess any application risks that need to be considered and mitigated prior to implementation.

The Infrastructure Security Group (ISG) reports to the CISO and provides oversight and guidance on managing infrastructure and network security risks on an ongoing basis, including results of periodic vulnerability assessments The ISG also conducts an annual IT risk assessment. Risks identified and risk mitigation is communicated and approved by management. Additionally, Enterprise Information Security evaluates new planned technology to assess any infrastructure risks that need to be considered and mitigated prior to implementation.

Enterprise Business Continuity and Disaster Recovery is overseen by Enterprise Continuity (EC) which reports to the Vice President of ERM. The EC department works with business units to develop business impact and recovery planning documentation, as well as schedule both business continuity and disaster recovery exercises. Strategies and results are discussed with management via reporting to the CRO, Vice President of ERM, ERMC, and the Risk and Compliance Committee. Documentation of business continuity and disaster recovery assessments, plans and exercises are independently reviewed by Enterprise Resilience Governance which is part of the Corporate Risk and Compliance department.

Corporate Risk and Compliance reports to the Vice President of ERM. The department works with BUs to identify risks and compliance issues within the organization. Identified risks, compliance issues, and mitigation strategies are discussed with management via reporting to the CRO, the Vice President of ERM, various business unit risk committees, product change control boards, the ERMC, and the Risk and Compliance Committee.

Occupational Risk Management reports to the Vice President of ERM and is responsible for workplace safety and compliance. Identified risks, compliance issues, and mitigation strategies are discussed with management via reporting to the CRO and the Risk and Compliance Committee.
An annual fraud risk assessment is completed where department managers are asked detailed questions to identify potential risks. The fraud and risk survey are distributed to the ERMC, the Audit Committee, and the Risk and Compliance Committee. Furthermore, the Corporate Security Council (CSC) and Enterprise Software Security Committee (ESSC) serve a dual purpose of identifying organizational risks and approving solutions to mitigate the identified risks. Many CSC and ESSC participants are also members of the ERMC.

Monitoring

Jack Henry has established a layered approach to monitor the quality of the services provided to its financial institutions. Management has implemented controls and reporting to help meet or exceed expected performance levels. Managers are provided with regular reporting that allows them to monitor performance issues. Division and unit managers monitor performance against goals and provide status reports to senior Jack Henry management. Corporate Audit Services provides validation that the established policies and procedures are followed as directed by senior management and the Board of Directors. Monthly Audit Committee meetings are held to discuss audit findings from the current review period and to track the progress in resolving outstanding issues from previous reviews, audits, and examinations. The Audit Committee reviews reports issued by Corporate Audit Services, Federal regulators, and third-party audit vendors.

Management Steering Committee

The Management Steering Committee reviews a variety of monthly reports to compare actual performance to budgeted and planned performance. The Management Steering Committee also holds regular meetings to gauge performance against the strategic plan.

Administration

Vice Presidents are responsible for coordinating the overall planning, budgeting, service quality, and formulating the Information Security strategic direction. Budgets are prepared on an annual basis and are approved by Jack Henry executive management.

Corporate Audit Services

Jack Henry is subject to reviews by internal auditors on a regular basis. Reports are issued by Corporate Audit Services to audit unit management, applicable Vice Presidents, Chief Risk Officer, the Vice President of ERM, executive management, regulators, the company's external audit firm, and the Audit Committee of Jack Henry's Board of Directors. Involvement of the internal auditor includes an understanding and evaluation of:

- Business objectives
- Management structure
- Systems development and programming
- Data integrity
- Computer operations and controls
- Physical security
- Logical security
- Business resumption contingency planning

Corporate Security Council (CSC)

The CSC provides oversight, guidance, leadership, and sponsorship to Jack Henry's enterprise information security and data privacy programs to assure the confidentiality, integrity and privacy of Jack Henry and our clients' data.

Cybersecurity Task Force (CTF)

The CTF exists to monitor and report cybersecurity risk, share relevant threat information that could potentially impact Jack Henry or customers, and determine if business units are working collectively to manage cybersecurity risks.

Enterprise Software Security Committee

The ESSC acts as an enterprise-wide oversight group to provide governance for secure software development practices. The primary function of the ESSC is to supply guidance to improve the company's secure development practices.

Infrastructure Security Committee

The ISC acts as an enterprise-wide oversight group within Jack Henry to provide governance for secure infrastructure and system configuration practices. The primary function of the ISC is to provide guidance to improve the company's secure configuration practices.

Quality Assurance (QA)

Jack Henry's QA function is responsible for final testing and control of application software releases. New software releases are provided to Quality Assurance or Release Services from the development teams.

Vendors and Subservice Organizations

Jack Henry maintains a vendor management program whereby third-party vendors are evaluated to assess if they are a reputable and financially solvent entity. Additionally, Jack Henry monitors subservice organizations through service-level agreements, periodic reports, and periodic visits to the subservice organizations facilities and review of SOC 1 or 2 reports, when available.

Information Systems

Jack Henry uses various servers, processors, disk storage units, tape units, printers, routers, and networking technologies in conducting its operations. This infrastructure supports offered products and services. Jack Henry has multiple data centers to support this infrastructure and has built-in redundancy to maintain the availability of systems. The components of the information systems relevant to the scope of this report are discussed further within this section.

Policy, Standards, Procedures, and Guidelines

Written operating instructions are used for supporting Jack Henry operations. These instructions cover normal operations, error message response actions, and restart/recovery instructions. A corporate policy regarding the appropriate handling of confidential consumer information of financial institutions has been established. The corporate policy is also posted on the For Clients portal for clients to gain access to the information. Security policies to provide support for, and implementation guidance of, the Jack Henry Security Program are posted on the company's intranet site and require annual update and sign off by employees. Each employee is informed annually of the importance of maintaining the appropriate level of security over confidential information through the distribution of these policies, the Jack Henry employee manual, and mandatory quarterly security awareness training.

Communication

Jack Henry employees are kept informed of the corporate and individual responsibilities through a variety of communication channels. The corporate intranet provides timely announcements where employees can access a wide range of information that includes, but is not limited to, corporate news, corporate policies, organization charts, significant changes, phone listings, internal education opportunities, security and safety guidance, resource center libraries, and incident response procedures. Each new employee participates in a standardized educational program to learn about the availability of corporate resources, the requirements for maintaining the confidentiality of data, and corporate ethics. Staff meetings are used to reinforce the goals at the department level. Employees are requested to complete surveys periodically, and an independent surveying company is used to compare results with other similarly sized companies to assess Jack Henry in terms of work environment, management, compensation, benefits, and other factors. Results are communicated to the Board of Directors. Additionally, the Board, executive management and vice presidents hold an annual strategic planning meeting to discuss company objectives, the current marketplace and the industry's future direction.

Multiple channels of communication are used to facilitate the flow of information between Jack Henry and its clients. The Jack Henry For Clients portal is the primary communication tool to provide information on performance, significant changes, security, maintenance schedules, operations, SOC audits and gap letters. Jack Henry and clients have contracts in place that specify responsibilities and obligations of the parties. Email is encrypted using a third-party solution to protect confidential information. The quarterly publication, the "Regulatory News Report," provides compliance-related information to clients. Feedback is obtained through regular client service surveys and in targeted focus groups. The results of the surveys are posted on Jack Henry's intranet site which helps support personnel to adjust performance based on the feedback. Educational opportunities are available at the annual Jack Henry Annual Conference or through in-house training or Internet-based training programs.

Regulatory Commitments

Ensenta is required to comply with regulatory compliance requirements that include PCI DSS, SOX, and SOC 2.

Contractual Commitments

Contracts are documented between Ensenta and its clients to describe the services being provided. Ensenta commits to compliance with PCI DSS and applicable regulations, commits to maintaining and testing a reasonable disaster recovery plan, and makes commitments to the privacy and security of non-public personal information within their documented contracts.

Service level agreements (SLAs) are documented and defined by senior management on a per-contract basis for clients and business partners. Internal monitoring services are in place to monitor service downtime, and communication procedures are put in place to notify appropriate personnel when agreed upon if duration is exceeded.

System Design

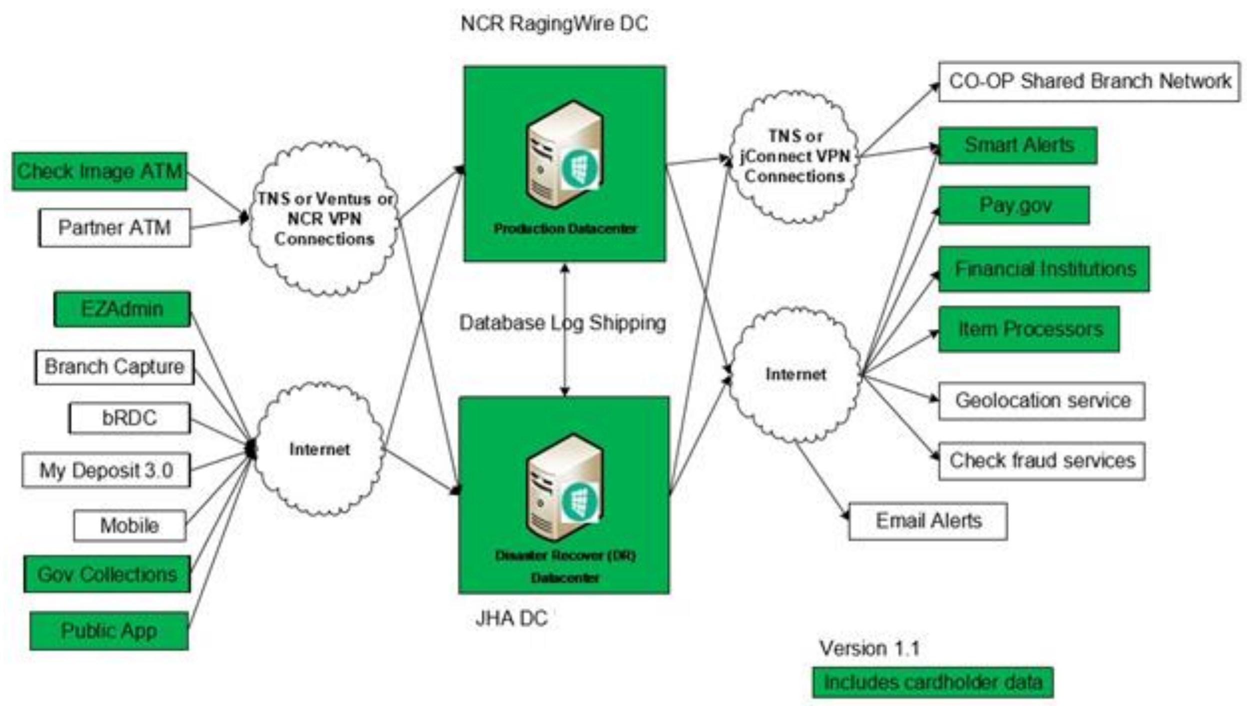
Ensenta designs its payment processing services system to meet its regulatory and contractual commitments. These commitments are based on the services that Ensenta provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Ensenta has established for its services. Ensenta establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Ensenta’s system policies and procedures, system design documentation, and contracts with clients.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

Infrastructure

A hardware inventory list of the organization's production environment is maintained and contains device name, device type, vendor, function, OS, location, and related notes.

Network diagrams are required to be created and maintained for all networks that process, transmit, or store Tier 1 and Tier 2 information. The NetOps and Compliance groups are responsible for reviewing and maintaining these diagrams at least annually, and the Ensenta logical data flow and network infrastructure diagram is shown below.



Software

A software inventory is maintained by Ensenta and documents vendor, function, and license information.

People

The following personnel were interviewed as part of the audit engagement:

- Scrum Master
- Senior Scrum Master
- Systems/Network Administration, Senior Manager
- Compliance Analyst
- Database Administration, Manager
- Audit Support Analyst

- Director of Installations
- Customer Support Manager
- Talent Acquisition Operations Manager
- Human Resources (HR) Compliance/SPHR Processes Supervisor
- Senior Manager of Talent Acquisition
- HR Business Partners, Senior Manager
- Cybersecurity Operations Manager
- Network Engineer, Advanced
- System Network Administrator, Manager
- Implementation Manager
- Asset Protection, Supervisor
- Information Security Engineer, Advanced

Data

Ensenta receives, stores, and/or transmits deposits data and credit card and ACH payment data, including permanent account numbers (PANs), CVVs, expiry, bank account numbers, and cardholder/account holder names. Data flow diagrams are created and maintained for each process or service that handles Tier 1 and Tier 2 information; Tier 1 data includes PCI data and sensitive customer data.

A Records and Data Retention Policy is maintained by the organization and requires specified data to be retained only as long as required for legal, regulatory, and business needs. Data retention requirements are based on SOX and NACHA/ACH requirements, and data is required to be retained in support of the following:

- Business reasons in support of FI users researching transactions
- Business reasons in support of FI users researching deposits
- Business reasons in support of duplicate check reviews
- Business reasons in support of FI file download
- Regulatory reasons in support of SOX, SOC 2, and PCI requirements

Ensenta uses SQL Server Transparent Data Encryption (TDE) to encrypt its production databases, backups, and log files at rest. User acceptance testing (UAT) databases are also encrypted and serve as a testing ground for rehearsal of encryption procedures. Each year, the organization is required by PCI to rotate the TDE keys. The procedure is documented within the Annual Key Change Procedure for SQL Server TDE, which references three independent procedures for rotation:

- The database master key in the master database
- The key-encrypting key (certificate) stored in the master database
- The data encryption keys for each database

Ensenta uses SQL Server Always Encrypted column level encryption to protect sensitive data classified as “Confidential – Tier 1”, both at rest and in transit. TDE data encryption keys (DEK) are rotated every five years, key encryption keys (KEK) are rotated annually, and the master encryption key is rotated annually. All other encryption systems use native key management systems and the encryption keys cannot be influenced externally.

Sensitive data within the organization is secured any time it must be transmitted or received via open, public networks. HTTPS/TLS protocols are used when information is transmitted over the internet, and Cisco AnyConnect VPN technologies use SSL/TLS to encrypt the traffic to the Ensenta production, disaster recovery, and ECUAT environments. F5 VPN uses SSL/TLS to encrypt the traffic to the Jack Henry networks and Ensenta EcDev environments. FTPS/SFTP technologies are used to transmit data to some clients, and RDP is used to manage systems remotely. Passwords are stored encrypted, or hashed equivalents are stored by native systems.

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

The Security, Availability, and Processing Integrity categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security, Availability, and Processing Integrity criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services Security, Availability, and Processing Integrity criteria are included in section IV of this report. Although the applicable trust services criteria and related controls are included in section IV, they are an integral part of Ensenta's description of its payment processing services system.

Management Philosophy

Management's communication sets the tone and direction for the entire organization through the Employee Handbook and all-hands videos. The Employee Handbook is made available to all employees for reference on the Policy Center, and videos are distributed to personnel at least quarterly.

Security, Availability, and Processing Integrity Management

The organization's security, availability, and processing integrity requirements are managed using a combination of documented policies and procedures, management oversight, and network systems and hardware. These management practices are implemented in all areas of the control environment to protect systems, data, and personnel and to ensure compliance with industry best practices and standards.

Security, Availability, and Processing Integrity Policies

Business unit policies are developed by management or by a SME in their relevant department and are reviewed annually by Ensenta personnel or as changes to the organization's risk profile occur.

The following policies were reviewed as part of the audit engagement:

- Enterprise Cybersecurity Policy
- Business Continuity and Disaster Recovery Program Overview Plan
- Records and Data Retention Policy
- Risk Management Policy
- Risk Assessment Methodology
- Third-Party Risk Management Policy
- Incident Management Policy
- System Security and Maintenance Policy
- Information Security Policy
- Change Management Policy
- Network Systems Configuration Standards Policy
- Workstation Configuration Standards
- Firewall Standards and Procedures

- Firewall Standards
- Employee Handbook
- Background Screening Policy
- Cybersecurity Incident Response Policy
- Incident Response Plan
- PCI System Testing Policy
- System Monitoring Policy
- Agent Logging and Monitoring Policy
- Vulnerability Management Policy
- Data Protection Policy
- Access Control Policy
- Corporate Active Directory Policy
- Account Management Policy
- Physical Security Policy
- Visitor Access Policy

Personnel Security

An Employee Handbook is maintained by the organization to communicate general corporate and personnel policies, including the code of conduct, statement on ethics, information confidentiality, and progressive discipline. All new hires receive the handbook as part of onboarding and are required to acknowledge their understanding of the included policies. The handbook is maintained in a location that is accessible by all personnel.

Job descriptions are documented for all critical functions within Ensenta, including the following:

- Systems Network Administrator
- Software Engineer
- Project Manager
- QA Analyst Advanced
- Project Manager

Physical Security and Environmental Controls

A Physical Security Policy is documented by Ensenta to provide guidance for the established physical security controls in place within the facility. The organization’s facility has three access points, which are locked at all times and require an access card for entry. All facility access is managed by the building’s facility management. A video surveillance system is in place to monitor access to the building, and video cameras are mounted on the ceiling and are protected with coverings to prevent tampering or disabling. Video recordings are retained for at least 90 days.

A Visitor Access Policy is in place within the organization and requires all visitors to sign visitor logs; the logs are required to be retained for at least one year. Visitors are required to document their name, company, date, time entering/leaving the facility, and the employee being visited. A confidentiality notice is on the top of the registration form for acknowledgement by all visitors.

Environmental controls are in place to protect the Ensenta facility, server room, and equipment and are managed and maintained by the building's facility management team. HVAC units are established to control the humidity and temperature, and a fire detection and a dry-pipe sprinkler suppression system are in place. Fire extinguishers are placed throughout the facility, and a UPS is implemented within the server room.

Documented guidelines are in place for securing and destroying paper and electronic media that contains sensitive or confidential information. Hardcopy materials and electronic storage devices are required to be destroyed when no longer necessary. One shred bin is positioned within the Ensenta facility, and the bin is secured with a lock; the opening of the bin is small enough to prevent retrieval of documents from within the bin, and the volume of paper contained within the bin does not cause overflow or cause personnel to discard sensitive documents in alternative locations.

Change Management

Application and system change management policies and procedures are implemented within Ensenta and require the documentation of approval by authorized parties and the testing of functionality. YouTrack is used to facilitate the change management process. The tickets capture a description and technical specifications of the change, approval by management, and the performance of peer reviews. Source code is checked-out or copied to a test or development environment, and program changes are tested in a separate, controlled environment. Appropriate personnel perform the migration of changes to production in a controlled manner, and release to production and back-out procedures are managed through Octopus.

The organization's Windows server configuration standard is based off the NIST Windows Server STIG, and all Windows systems are hardened prior to being deployed to Ensenta networks. Linux systems are configured based on industry best knowledge of Jack Henry personnel, and AlgoSec is used to validate that network devices are configured to meet PCI and ISO requirements. Configuration standards are required to be updated as new vulnerabilities are identified, and IT personnel are responsible for reviewing vendor and industry best practices websites and reviewing the results of vulnerability scans and penetration tests. Additionally, these personnel are responsible for performing the related remediation to remain current and knowledgeable of security-related controls and defenses that are impactful to system configurations.

A firewall solution is in place to screen traffic from the internet and between the DMZ and/or the internal network, and are configured to deny all traffic that is not explicitly authorized for a specific business need and only allow traffic that is necessary to perform business. Additionally, firewalls been implemented at the Ensenta office suite, and network architecting and configuration guidance are provided for firewalls. Firewalls rules are required to be audited every six months.

Application Development

Ensenta has defined processes in place to ensure that applications are not vulnerable to injection flaws, buffer overflow, cryptographic storage, insecure communications, improper error handling, and "High" vulnerabilities. Application code changes are reviewed by a developer who is not the code's author and is knowledgeable in security coding practices and are reviewed against OWASP security recommendations and best practices; an acceptable result is required to be obtained prior to promoting the code to production. Veracode application scanning is performed every Wednesday against Git and notifies the development team of issues detected so they can be researched and verified. If an issue is verified, a YouTrack ticket is opened to ensure that the issue is addressed. Issues found in pre-production are prioritized, and critical and high issues are required to be addressed before the code can be promoted to production.

Source code within the organization is managed via Stash Git's version control system, and only developers, database administrators (DBAs), and NetOps have access to the application code. The Ensenta development, UAT, disaster recovery, and production environments are unique environments that are logically separated, and separation of duties is in place for the development/test and production personnel. QA personnel are responsible for QA activities and code deployment to QA systems, and developers are responsible for developing code; Network Administrators are responsible for managing the organization's networks and systems.

System Monitoring

Network logging and monitoring tools are in use within the Ensenta environment, and the production systems are configured to log and are offloaded to the NTT Security's syslog collector and Jack Henry Splunk centralized logging systems. The disaster recovery, ECUAT, and ECDEV environments are configured to log and offload the logs to the Jack Henry Splunk centralized logging system. The systems are configured to detect anomalous activity or activity exceeding trigger levels and to send alerts to IT personnel for investigation. Logs are required to be retained for one year and include the following elements:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

Cisco's Sourcefire Next-Generation IPS is implemented within the networks to perform intrusion detection/prevention on the production environment and is managed by NCR managed services. The disaster recovery and development environments use McAfee Network Security Manager and IBM Security SiteProtector Systems to perform intrusion detection/prevention and are managed by Jack Henry hosted services. The ECUAT environment uses Azure IDS/IPS technologies and is managed by Ensenta personnel. Additionally, OSSEC is implemented in the production and disaster recovery environments.

Virus protection is required to be employed on all systems and workstations running Windows, Linus, or Mac Operating Systems. The protection is enabled to scan in real-time and is scheduled to run regularly scheduled scans no less than monthly; the definitions must be updated no less than weekly. Trend Micro Deep Security is deployed to all servers in the production and disaster recovery environments, MS Windows Defender is deployed to all servers in the development and UAT environments, and McAfee ePolicy Orchestrator is deployed to all laptops and is scheduled to run at regular intervals to ensure the virus signatures are kept up to date.

A Vulnerability Management Policy is maintained by Ensenta to provide roles, responsibilities, guidance, and timelines related to the assessment and mitigation of vulnerabilities and to ensure information systems and the information processed are properly protected. Internal and external penetration testing and web application scans are required to be performed annually on the production networks by a third-party specializing in penetration testing. Internal and external vulnerability scans are performed at least quarterly on the production networks, and Veracode scans are executed on the application code on a weekly basis. Any "critical" or "high" vulnerabilities identified in the testing are required to be remediated and retested to validate the vulnerability has been remediated.

A defined process is in place to ensure that security updates and patches are installed in a timely manner, generally within one month. Outside sources, such as security mailing lists, vendor notifications, and regularly monitored security-based websites, are used to identify new vulnerabilities that could impact networks and systems.

Problem Management

Incident response policies and procedures are documented by Ensenta to guide personnel on how to identify, respond to, recover from, and if necessary, escalate security-related incidents to executive management. Incidents are investigated by the responsible personnel and if necessary, remediated and documented. Incident processes are updated as needed to prevent the reoccurrence of the incident, and the Ensenta Incident Response Plan includes the following:

- Incident Management Planning
- Implementation
- IRT Guidelines
- Training
- Incident Management
- Roles and Responsibilities
- Coverage and Response
- Legal
- Escalation to Disaster
- Incident Review
- Incident Procedure, Corrective Action
- Preventive Action
- Escalated CARs from Functional Areas
- Preventive Action – Improvements
- Corrective Action
- Preventive Action
- Root Cause Analysis

Personnel responsible for incident response are required to be trained, and incident response training is provided through response to actual incidents. An annual incident response training exercise is performed as well. A dedicated fraud and security email account, the Jack Henry ForClients portal, and a customer support phone number are in place to allow customers to report compliance, security, and availability issues

Data Backup and Recovery

Data backup and recovery policies and procedures are in place within Ensenta. Daily backups are taken of all production databases on a nightly basis. The backup files are encrypted with SQL Server TDE, and full backups are taken weekly on Saturday evenings. Differential backups are taken daily throughout the week and transaction log backups are taken every 15 minutes. Backup files are retained according to the following schedule:

- Full backups (.bak) – One week
- Differential backups (.diff) – One day
- Transaction log backups (.trn) – One week

Backups are restored at least once per month to validate integrity, and the DBA team receives a daily report via email detailing the results of the previous evening's backups. The organization's log shipping files are continuously monitored, and if an invalid file appears, DBAs and Operations are alerted immediately. A full database restore is performed once per month at a minimum, and backup disks (PROD and DR) are stored on an appliance and do not leave the NCR/RagingWire Ashburn Data Center. Data is replicated from the primary data center to the disaster recovery data center, and backups are configured to be on a rotation so that the oldest data available is within a two-week period. The backups are used to facilitate restores when systems are corrupted.

A business continuity and disaster recovery plan has been established within Ensenta to govern the disruption or failure of critical business systems and processes and the disruption of personnel to perform critical operations. A business impact analysis (BIA) is performed as well to determine recovery time objectives (RTO) and costs of outages. Financial impact, operation/client impact, compliance/legal/regulatory impact, and reputational impact are considered as part of the BIA, and Ensenta has an RTO of six hours and a recovery point objective (RPO) of one hour. The following are documented as part of the business continuity and disaster plan:

- Disaster Declaration
- Department Business Impact Analysis
- Business Continuity Plan Testing
- Business Impact Analysis – Application
- IT Disaster Recovery Plan
- Risk Assessment
- IT Disaster Recovery Plan Testing
- Client Responsibilities
- Recommendations for Clients
- Notification for Clients
- Last Update to the Plans
- Last Plan Exercise

The business continuity plans are required to be reviewed at least annually or when a significant change occurs within the business. The disaster recovery plans and processes are reviewed and tested at least annually, and the test consists of performing a simulated failover to the disaster recovery network.

System Account Management

An Access Control Policy is documented by Ensenta to define the workflow for creating, changing, or terminating logical access to systems and applications. Access requirements for systems and access management are established within the Corporate Active Directory Policy, and Cherwell/JSource is used to request access to Jack Henry corporate systems. IT staff are responsible for providing access to systems and networks based on requests from HR or an authorized manager. All requests to make changes to or add access rights to the Ensenta systems and networks are submitted via a change request ticket to the Security Officer. The request is required to be approved by management prior to the request being granted, and when the request is granted, the ticket is updated. Access privileges are assigned based on job functions and responsibilities, and all employees, including System Administrators, are required to have a unique user ID before being granted access to the networks and applications.

Access control systems are used to restrict access to networks, systems, and applications, and the systems are limited to authorized individuals. Network password complexity and privileges are enforced through Active Directory and/or native access controls in the applications, and defined procedures are in place for assigning first-time passwords and performing password resets. The password control parameters enforced include the following:

- Password must meet complexity requirements: Enabled
- Minimum password length: 8 characters
- Maximum password age: 90 days
- Minimum password age: 1 days
- Enforce password history: 12 passwords remembered
- Store passwords using reversible encryption: Disabled

Account lockout parameters include the following:

- Account lockout duration: 240 minutes
- Account lockout threshold: 6 invalid login attempts
- Reset account lockout counter: After 120 minutes

Passwords are stored encrypted, or hashed equivalents are stored by native systems. Two-factor authentication is required to be used when accessing Tier 1 data remotely, and all non-console access requires the use of multi-factor authentication. The production and disaster recovery networks are remotely accessed through AnyConnect VPN systems and are configured for two-factor authentication. The ECUAT network is remotely accessed via RDP, only after connecting to the production or disaster recovery network. The Jack Henry F5 VPN is used to access the Jack Henry corporate and development networks; all require the use of two-factor authentication. Third parties are never provided remote access to the organization's systems.

New clients are assigned to an Installation team member, who sets up and revokes the client accounts in EZAdmin. Clients are responsible for adding or removing accounts for their personnel, and the Installation team members can be directed to remove an account on the client's behalf if the person requesting the removal is authorized. If a client completely cancels services, the cancellation must be communicated to the pay center directly or through the reseller, and the EZAdmin accounts are disabled on an agreed upon timeline.

Access of terminated personnel is required to be revoked immediately or upon the agreed termination date. All Active Directory accounts, remote access capabilities, and physical access capabilities are required to be removed when personnel are terminated, and termination checklists are used to ensure all access is removed appropriately.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of the payment processing services system during the period from October 1, 2019, through September 30, 2020.

COMPLEMENTARY USER-ENTITY CONTROLS

Jack Henry & Associates Inc. – Ensenta's services are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. Jack Henry & Associates Inc. – Ensenta's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. Jack Henry & Associates Inc. – Ensenta also provides best practice guidance to clients regarding control element outside the sphere of Jack Henry & Associates Inc. – Ensenta responsibility.

This section describes additional controls that should be in operation at user organizations to complement the Jack Henry & Associates Inc. – Ensenta controls. Client Consideration recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Jack Henry & Associates Inc. – Ensenta.

- User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Jack Henry & Associates Inc. – Ensenta's services.

- Transactions for user organizations relating to Jack Henry & Associates Inc. – Ensenta's services should be appropriately authorized, and transactions should be secure, timely, and complete.

- For user organizations sending data to Jack Henry & Associates Inc. – Ensenta, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to Jack Henry & Associates Inc. – Ensenta's services.

- User organizations should report to Jack Henry & Associates Inc. – Ensenta in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Jack Henry & Associates Inc. – Ensenta.

- User organizations are responsible for notifying Jack Henry & Associates Inc. – Ensenta in a timely manner of any changes to personnel directly involved with services performed by Jack Henry & Associates Inc. – Ensenta. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Jack Henry & Associates Inc. – Ensenta.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with Jack Henry & Associates Inc. – Ensenta.

- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by Jack Henry & Associates Inc. – Ensenta.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV:
TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

Applicable Trust Services Criteria Relevant to Security, Availability, and Processing Integrity

Although the applicable trust services criteria and related controls are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," they are an integral part of Jack Henry & Associates Inc. – Ensenta's system description throughout the period October 1, 2019, to September 30, 2020.

Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

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 achievement of Jack Henry & Associates Inc. – Ensenta's service commitments and system requirements. 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.

Availability

The trust services criteria relevant to availability address the need for information and systems to be available for operation and use to achieve the service organization's service commitments and system requirements.

Availability refers to the accessibility of information used by Jack Henry & Associates Inc. – Ensenta's systems, as well as the products or services provided to its customers. While the availability objective does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems), it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Processing Integrity

The trust services criteria relevant to processing integrity address the need for system processing to be complete, valid, accurate, timely, and authorized to achieve the service organization's service commitments and system requirements.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.

Trust Services Criteria for the Security, Availability, and Processing Integrity Categories			
Control Environment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	New hires within the organization are required to acknowledge their understanding of various policies as part of the onboarding process.	Interviewed the Talent Acquisition Operations Manager, Human Resources (HR) Compliance/SPHR Processes Supervisor, and Senior Manager of Talent Acquisition and verified new employees are required to sign or electronically acknowledge the Jack Henry Code of Conduct, Jack Henry Enterprise Cybersecurity Policy, Employee Handbook, Jack Henry Acceptable Use Policy, and Proprietary Rights and Confidentiality Agreement (PRCA) Reviewed the Onboarding Agency Contractor Process and verified contractors are required to sign Third-Party Agreements and Staffing Confidentiality Agreements and they are set up in the corporate learning solutions system to complete required training programs Observed personnel records and Jack Henry Policy Center records for 3 of 8 personnel hired over the audit period and verified new hires have physically or digitally signed the following: • Jack Henry Code of Conduct • Jack Henry Enterprise Cybersecurity Policy • Employee Handbook • Jack Henry Acceptable Use Policy • Proprietary Rights and Confidentiality Agreement (PRCA)	No Relevant Exceptions Noted
CC1.1.2	Policies and procedures are in place to guide hiring and employment practices within the organization.	Interviewed the Talent Acquisition Operations Manager, HR Compliance/SPHR Processes Supervisor, and Senior Manager of Talent Acquisition and verified	No Relevant Exceptions Noted

		policies and procedures have been implemented to guide hiring, employment, and departure of personnel Reviewed the Hiring Guide for Managers SOP (June 2020) and verified hiring managers are provided guidance for hiring and topics include the following: • Posting Process • Applicant Review • Interview Process • Offer Process • Requests to Waive the Posting Process Reviewed the Employee Handbook (June 2019) and verified content related to recruitment, hiring, training, and remedial actions is established	
CC1.1.3	Responsible personnel within the organization are provided guidance for handling voluntary or involuntary terminations.	Reviewed the Exit Process SOP (July 2020) and verified HR personnel are given guidance for voluntary and involuntary terminations Observed Jira tickets for 3 of 4 personnel terminated over the audit period to ensure that logical and physical access to Jack Henry facilities and systems was requested to be revoked for terminated personnel	No Relevant Exceptions Noted
CC1.1.4	Management communicates and oversees the implementation of the code of conduct, integrity, and ethics to new and current employees.	Interviewed the HR Business Partners, Sr. Manager and verified the Standards of Conduct policy is documented within the Employee Handbook and all employees are required to acknowledge the Employee Handbook as part of the onboarding process Observed Jack Henry Policy Center and verified the Employee Handbook is available for employees to reference Observed Jack Henry Policy Center records for 3 of 8 personnel hired over the audit period and verified the Employee Handbook was electronically acknowledged	No Relevant Exceptions Noted

		Reviewed the Employee Handbook and verified the code of conduct, integrity, and ethics are addressed	
CC1.1.5	An Employee Handbook is distributed to all new hires to communicate the code of conduct, statement on ethics, information confidentiality, and progressive discipline.	Reviewed the Employee Handbook and verified general corporate and personnel policies and content have been established and include the following: • Code of conduct • Statement on ethics • Information confidentiality • Progressive discipline Interviewed the Talent Acquisition Operations Manager, HR Compliance/SPHR Processes Supervisor, and Senior Manager of Talent Acquisition and verified new hires receive an Employee Handbook and are required to acknowledge receipt and to abide by the policies contained within it Observed Jack Henry Policy Center and verified the Employee Handbook is available for employees to reference Observed Jack Henry Policy Center records for 3 of 8 personnel hired over the audit period and verified the Employee Handbook was electronically acknowledged	No Relevant Exceptions Noted
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	A board of directors is in place within the organization to exercise oversight of the development and performance of internal control.	Interviewed the Compliance Analyst and verified the Board of Directors meets quarterly and files SEC-related forms required of public companies Reviewed 3 of 4 SEC Form 10-Q Forms for Jack Henry & Associates, Inc., submitted quarterly, and verified the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) have attested to the execution and responsibilities associated with SOX	No Relevant Exceptions Noted

CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	A hierarchical organizational structure is in place to segment business functions and to provide oversight and leadership.	Interviewed the Compliance Analyst and verified a hierarchical organizational structure is utilized to segment functions and provide oversight Observed separate groups perform limited roles of responsibility, those functions together represent the totality of the work that is performed, and all groups report to a member of management Observed the Organizational Chart and verified roles and responsibilities have been separated Reviewed critical job descriptions and verified the general duties and requirements necessary for each position are documented	No Relevant Exceptions Noted
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	Security awareness training is performed as part of the onboarding process and is required to be completed quarterly thereafter.	Interviewed the HR Business Partners, Senior Manager and verified security awareness training is performed as part of the onboarding process and quarterly thereafter through the Jack Henry University online training portal Observed Jack Henry University training portal records and verified a sample of 3 of 8 personnel hired over the audit period completed security awareness training close to the onboarding date Observed Jack Henry University training portal records and verified that all Ensenta personnel had taken security awareness training in Q1	No Relevant Exceptions Noted
CC1.4.2	All new employee are required to undergo background checks, and the employment offer is contingent on the results.	Interviewed the Talent Acquisition Operations Manager, HR Compliance/SPHR Processes Supervisor, and Senior Manager of Talent Acquisition and verified new	No Relevant Exceptions Noted

		employees are required to undergo background checks and the results are contingent to the job offer Observed personnel records for 3 of 8 personnel hired over the audit period and verified Employment Background Investigations, Inc. is used to perform background checks and includes the following checks: • Social Security Trace • Criminal Records Search • Education Verification • Employment Verification • Motor Vehicle Records Examination • Drug Test • National Criminal Record Database • OFAC PLUS Reviewed the Background Screening Policy (December 2019) and verified candidates must be screened for the following: • Social Security Trace • Criminal Records Search • Education Verification • Employment Verification • Motor Vehicle Records Examination • Drug Test • National Criminal Record Database • OFAC PLUS Reviewed the Background Review and Hire SOP (February 2020) and verified background checks must be reviewed to approve or deny employment	
CC1.4.3	Independent contractors within the organization are required to perform background checks.	Reviewed the Independent Contractor Agreement, Exhibit B, and verified contractors are subject to the same pre-employment screening as employees of Jack Henry Interviewed the Talent Acquisition Operations Manager, HR Compliance/SPHR Processes	No Relevant Exceptions Noted

		Supervisor, and Senior Manager of Talent Acquisition and verified independent contractors are required to perform background checks and the requirement is written into the contract	
CC1.4.4	All temporary personnel are provided through temporary staffing agencies, and background checks are performed by the agency.	Interviewed the Talent Acquisition Operations Manager, HR Compliance/SPHR Processes Supervisor, and Senior Manager of Talent Acquisition and verified temporary personnel are provided through temporary staffing agencies and background checks are performed by the agency Reviewed the Hiring Agency Contractor Process and verified the hiring agency is responsible for completing the background checks	No Relevant Exceptions Noted
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	Defined processes are in place for the creation, approval, and maintenance of the organization’s policies.	Interviewed the Senior Scrum Master and verified Jack Henry policies are developed by management or by a SME in their relevant department and are reviewed annually by the Corporate Security Council; business unit policies are developed by management or by a SME in their relevant department and are reviewed annually by business unit or Ensenta personnel Observed the revision history for a variety of organizational policies and verified the policies had been reviewed within the audit period by the Corporate Security Council or by Ensenta personnel Reviewed the Enterprise Cybersecurity Policy and verified cybersecurity policies are required to be reviewed annually or as changes are made to the organization’s risk profile	No Relevant Exceptions Noted
CC1.5.2	Multiple systems are in use within the organization to monitor operational quality and control.	Interviewed the Scrum Master and verified different groups utilize	No Relevant Exceptions Noted

		different systems to monitor activities to ensure operational quality: • Development teams and NetOps utilize Jira and Kanban to track and manage workflows and issues • Customer Support utilizes Salesforce to track and manage workflows and issues • Automated systems are implemented to provide notifications of issues within the system in near-real time	

Trust Services Criteria for the Security, Availability, and Processing Integrity Categories			
Communication and Information			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	Data flow diagrams are maintained by the organization to illustrate how sensitive data moves throughout the environment.	Interviewed the Scrum Master and verified data flows are documented to track how data enters and flows within the network and is stored Observed data flow diagrams compared against the hardware inventory list and the network diagrams and verified the diagrams are consistent with the systems in the networks Reviewed the Enterprise Cybersecurity Policy (August 1, 2020) and verified data flow diagrams are required to be created and maintained for each process or service that handles Tier 1 and Tier 2 information Reviewed the organization's data flow diagram (January 14, 2020) and verified the diagram had been reviewed during the audit period	No Relevant Exceptions Noted
CC2.1.2	Ensenta receives, stores, and/or transmits deposit data and credit card and ACH payment data.	Interviewed the Senior Scrum Master and verified PANs, CVV, expiry, bank account numbers, and cardholder/ account holder names are received, stored, and/or transmitted through Ensenta systems Reviewed the organization's data flow diagram and verified Ensenta receives, stores, and/or transmits deposit data and credit card and ACH payment data	No Relevant Exceptions Noted
CC2.1.3	The organization generates and uses relevant, quality information to support the functioning of internal controls.	Observed the Jira system and Kanban boards and verified the system is utilized to manage system change requests and application sprints and it is utilized by management to ensure that projects stay on track or to	No Relevant Exceptions Noted

		identify if additional resources are needed Observed the Salesforce dashboards and verified service tickets are monitored by management to ensure that workloads are balanced, issues stay on track, and to identify if additional resources are needed Observed the Ensenta System Status system and verified system status reports are sent to the Operations and Support hourly when there are no issues, and every 15 minutes when issues are detected Observed the Event Listener and Splunk monitoring systems and verified systems are utilized to monitor for anomalies Observed Ensenta's Splunk dashboard and verified systems health is monitored and alerts are generated if issues are detected	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	IT personnel within the organization review vendor and industry best practices websites, review the results of vulnerability scans and penetration tests, and perform the related remediation to remain current and knowledgeable of security-related controls and defenses that are impactful to system configurations.	Interviewed the Systems/Network Administration, Senior Manager and verified IT personnel are constantly reviewing vendor and industry best practices websites, reviewing the results of vulnerability scans and penetration tests, and performing the related remediation to remain current and knowledgeable of security-related controls and defenses that are impactful to system configurations Observed external and internal vulnerability scans and verified Jack Henry personnel experienced in vulnerability scanning are utilized to determine vulnerabilities, and the vulnerability findings are risk ranked by criticality	No Relevant Exceptions Noted

CC2.2.2	Application code within the organization is scanned on a weekly basis, and identified vulnerabilities are risk ranked by criticality for remediation.	Interviewed the Systems/Network Administration, Senior Manager and verified Veracode is utilized to scan application code weekly Observed 5 of 52 Veracode scan reports and verified application scans are performed weekly Observed annual application penetration test reports and verified third-party vendors are utilized to determine vulnerabilities and the vulnerability findings are risk ranked by criticality	No Relevant Exceptions Noted
CC2.2.3	Information security responsibilities for personnel are defined within the information security policies	Interviewed the Audit Support Analyst and verified new personnel are provided the Jack Henry Cybersecurity Policy as part of the onboarding process, which outlines the information security responsibilities of all personnel Observed JHAToday Policy Center records of 3 of 8 personnel hired over the audit period and verified the Enterprise Cybersecurity Policy form was digitally acknowledged Observed the Jack Henry Policy Center and verified corporate policies, including the Cybersecurity Security Policy, are maintained in a location that is accessible by all personnel Observed the Ensenta SharePoint and verified Ensenta specific information security policies provide all personnel with security-based guidance and are maintained in a location accessible by all applicable Ensenta personnel	No Relevant Exceptions Noted
CC2.2.4	Job descriptions are maintained for all critical functions within the organization.	Interviewed the HR Business Partners, Senior Manager and verified critical job descriptions are documented Observed the Organizational Chart and verified roles and responsibilities have been separated, follow the functional	No Relevant Exceptions Noted

		format, and functions report up to executive management Reviewed critical job descriptions and verified a general description and requirements are documented for the following: • Systems Network Administrator • Software Engineer • Project Manager • QA Analyst Advanced • Project Manager	
CC2.2.5	Management sets the tone and direction for the organization through the Employee Handbook and all-hands videos.	Interviewed the Audit Support Analyst and verified culture and tone is set by management through the Employee Handbook and quarterly all-hands videos Observed the corporate policies contained within the Employee Handbook and verified it is maintained and accessible by employees for reference on the Policy Center Observed personnel records for 3 of 8 personnel hired over the audit period and verified that Employee Handbook acknowledgement forms were signed and dated Observed the Jack Henry MS Stream video site and verified all-hands videos were recorded and distributed over the audit period, and videos are distributed to personnel at least quarterly	No Relevant Exceptions Noted
CC2.2.6	Personnel responsible for incident response activities are required to participate in annual training exercises.	Interviewed the Cybersecurity Operations Manager and Scrum Master and verified incident response training is provided through responding to actual incidents and through an annual incident response training exercise Observed Incident Report 203, in which an incident occurred on May 11, 2020, and verified incidents are investigated and, if necessary, remediated and documented	No Relevant Exceptions Noted

		Observed processes were updated as needed to prevent the reoccurrence of the incident, if possible Reviewed the Ensenta Incident Response Plan (January 13, 2020) and verified personnel responsible for incident response are required to be trained Reviewed the Jack Henry Cybersecurity Incident Response Policy (August 1, 2020) and verified the Cybersecurity Incident Response Team personnel are responsible for incident response and are required to be trained	
CC2.2.7	Information security policies are distributed to all personnel as part of onboarding, and are maintained in a location that is accessible by all personnel.	Interviewed the Audit Support Analyst and Senior Scrum Master and verified all personnel are provided Jack Henry corporate and Ensenta specific information security policies as part of the onboarding process and the policies are maintained where personnel can readily access them, if necessary Observed the JHAToday Policy Center and verified corporate policies, including the Enterprise Cybersecurity Policy, are maintained in a location that is accessible by all personnel Observed the Ensenta SharePoint and verified Ensenta specific information security policies provide all personnel with security-based guidance and are maintained in a location accessible by all relevant Ensenta personnel	No Relevant Exceptions Noted
CC2.2.8	The organization communicates objectives and responsibilities related to incident handling and response using the Incident Response Plan.	Reviewed the Jack Henry Cybersecurity Incident Response Policy and verified incident response guidance has been documented and includes the following: • Roles and Responsibilities • Reporting • Incident Classification • Cybersecurity Incident Response Team	No Relevant Exceptions Noted

		• Responding • Incident Declaration, Escalation, and Communications • Lessons Learned Reviewed the Ensenta Incident Response Plan and verified incident response guidance has been documented and includes the following: • Incident management planning • Implementation • IRT guidelines • Training • Incident management • Roles and responsibilities • Coverage and response • Legal • Escalation to disaster • Incident review • Incident procedure • Preventive action • Escalated CARs from functional areas • Preventive action – improvements • Corrective action • Root cause analysis	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	The descriptions of services and responsibilities are communicated to clients in contracts, which are required to be established before services are provided.	Interviewed the Scrum Master and verified the descriptions of services and responsibilities are documented in contracts, and contracts must be established before services are provided Observed the corporate website and verified the description of services performed aligns with the description of services provided to government and financial institutions (FI) Reviewed product briefs and verified marketing materials align with the services provided by Ensenta Reviewed the Master Service Agreement (October 30, 2019) and	No Relevant Exceptions Noted

		verified services and responsibilities have been documented and agreed to by both parties with the signing of the agreement	
CC2.3.2	Customers are provided multiple methods to contact the organization regarding compliance, security, and availability issues.	Interviewed the Senior Scrum Master and verified a dedicated fraud and security email account, Jack Henry ForClients portal, and customer support phone number are in place to allow customers to report compliance, security, and availability issues Observed support personnel during the virtual onsite answering phone calls and responding to client emails, phone calls, and the support portal and verified clients use these means to contact the organization Observed processes for onboarding new clients and the Ensenta website and verified contact information is provided to customers to report complaints and security and availability issues Observed the Ensenta corporate website and verified contact information has been provided to the public Observed the Jack Henry corporate website and verified the clients have access to the ForClients portal	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Processing Integrity Categories			
Risk Assessment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The organization is compliant with all industry requirements that impact operations.	Interviewed the Compliance Analyst and verified SOX, SOC 2, and PCI DSS are the only industry requirements that impact operations Reviewed the SOC 2 Type II Audit Report and verified the audit period was for April 1, 2019, to September 30, 2019 Reviewed the Ensenta PCI DSS AoC (March 19, 2020) and verified it was performed by a QSA company and is current Reviewed SEC Form 10K for Jack Henry & Associates, Inc., submitted for the fiscal year ended December 31, 2019, and verified the CEO and CFO have attested to the execution and responsibilities associated with SOX	No Relevant Exceptions Noted
CC3.1.2	The organization conducts an annual risk assessment based on specified company objectives.	Reviewed the Enterprise Cybersecurity Policy and verified risk assessments are required to be performed annually and after significant changes to the environment Interviewed the Scrum Master and verified a formal risk assessment occurs annually and when there are significant changes to business processes and/or other risk factors; the risk assessment utilizes ISO 27005 framework Reviewed the Risk Management Policy (December 16, 2019) and verified risk assessment guidelines are provided and risk assessments are required to be performed annually	No Relevant Exceptions Noted

		during the first quarter of each year, using the ISO 27005 framework Reviewed the Jack Henry Risk Assessment Methodology (August 1, 2020) and verified the Enterprise Information Security team is required to perform risk assessments every 12 to 36 months depending upon the risk of the business unit	
CC3.2	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.		
CC3.2.1	Risks identified within the organization’s risk assessment are documented, assigned, and tracked through remediation or acceptance.	Interviewed the Scrum Master and verified risks identified in the risk assessment are evaluated for potential ways to reduce known risks and vulnerabilities Observed the jGRC system and verified issues identified in audits and risk assessments are documented, assigned, and tracked through remediation or acceptance Reviewed the Ensenta Risk Assessment (December 16, 2019) and verified the risk assessment documented risk levels, risk analysis, and the related remediation recommendations	No Relevant Exceptions Noted
CC3.2.2	The organization’s risk assessment identifies all corporate assets and potential threats to those assets and ranks risks based on likelihood and impact.	Reviewed the Ensenta Risk Assessment and verified the risk assessment process was followed and controls are implemented to address the following: • Fraud teams and tools have been set up to detect fraud • System impact and likelihood are assessed • Reviews are performed of the risk of potential business disruptions and legal impact • Vendors are assessed annually for SOC compliance • Management reviews risk assessment and approves remediation or accepts risk	No Relevant Exceptions Noted

		Reviewed the Enterprise Cybersecurity Policy and verified risks are measured based on likelihood of the vulnerability being exploited and the impact is successfully executed	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	Risks relating to fraud are assessed as part of the annual risk assessment.	Reviewed the Ensenta Integrated Fraud Check-Product Brief (2019) and verified Ensenta provides a real-time fraud warning solution to detect check fraud Observed the EZAdmin fraud/risk configuration settings and verified FI can choose the following fraud-related risk checks: • Limits • Amounts • Image Acquisition • Risk Policy • Date • Duplicate • Score • Geolocation • Early Warning Services • Blacklist • Gray List • Other and Custom Rules	No Relevant Exceptions Noted
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The organization performs a risk assessment following any significant changes to the environment.	Reviewed the Enterprise Cybersecurity Policy and verified risk assessments are required to be performed annually and after significant changes to the environment Interviewed the Scrum Master and verified the risk assessment utilizes ISO 27005 framework	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Processing Integrity Categories

Monitoring Activities

Ctrl #	Description of Controls	Service Auditor’s Tests of Controls	Test Results
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	Ongoing security evaluations are performed by personnel to ensure components of internal controls are in place and functioning.	Interviewed the Senior Scrum Master and verified operational security procedures are performed daily, quarterly, bi-annually, and annually to reduce the risk of security incidents being undetected for a prolonged period of time Observed the following security processes are performed on a regular basis: • Risk assessments • Third-party internal penetration testing • Vendor compliance verification • Third-party internal/external vulnerability testing • Policy reviews • Training • System/network device alerts • Firewall ruleset reviews • Patching • Internal user access audits	No Relevant Exceptions Noted
CC4.1.2	The organization participates in independent audits to ensure their continued compliance with required frameworks.	Interviewed the Compliance Analyst and verified independent audits were performed for the SOX, SOC 2, and PCI frameworks Reviewed the SOC 2 Type II Audit Report, with an audit period from April 1, 2019, to September 30, 2019 Reviewed the Ensenta PCI AoC, which was completed on March 19, 2020, and deemed PCI DSS compliant Reviewed the SEC Form 10K for Jack Henry & Associates, submitted for the fiscal year ending June 30, 2019, and verified the CEO has attested to the	No Relevant Exceptions Noted

		execution and responsibilities associated with the Sarbanes-Oxley Act	
CC4.2	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.		
CC4.2.1	Regular meetings are held with executive management to discuss risk rankings and mitigation strategies.	Reviewed the Ensenta Risk Assessment and verified the risk assessment process was followed and controls are implemented to address the following: • Fraud teams and tools have been set up to detect fraud • System impact and likelihood are assessed • Reviews are performed of the risk of potential business disruptions and legal impact • Vendors are assessed annually for SOC compliance • Management reviews risk assessment and management approves remediation or accepts risk	No Relevant Exceptions Noted
CC4.2.2	Appropriate personnel are notified of any suspicious or unauthorized activity within the organization's network.	Reviewed the Ensenta Incident Management Policy (June 4, 2020) and verified personnel are staffed at all times, and the following alerts are monitored: • Unauthorized activity • Critical IDS alerts • Unauthorized critical system or content file changes	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Processing Integrity Categories

Control Activities

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	Roles and responsibilities are defined for the organization's development/test and production personnel.	Interviewed the Scrum Master and verified application code must be tested by QA personnel prior to promotion to the production environment Observed 30 of 442 YouTrack tickets and verified changes to the applications were tested prior to being promoted to production Reviewed job descriptions and verified QA personnel are responsible for QA activities and code deployment to QA systems, Developers are responsible for developing code, and Network Administrators are responsible for managing networks and systems Reviewed the System Security and Maintenance Policy (June 30, 2020) and verified application code changes require unit and regression testing to be performed	No Relevant Exceptions Noted
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	General information security policies are in place within the organization and are required to be acknowledged by all personnel.	Observed the JHAToday Policy Center records for 3 of 8 personnel hired over the audit period and verified the Enterprise Cybersecurity Policy form was digitally acknowledged Reviewed the Enterprise Cybersecurity Policy and verified general information security policies and content have been established and include: • Objectives • Roles and Responsibilities • Policy Compliance	No Relevant Exceptions Noted

		• Related Policies, Standards, and Processes Reviewed the Ensenta Information Security Policy (January 13, 2020) and verified general information security policies and content have been established to address PCI DSS requirements	
CC5.2.2	Security-based guidance is provided to all personnel through the information security policies.	Interviewed the Audit Support Analyst and Scrum Master and verified all personnel are provided the Information Security Policy, which provides all personnel with security-based guidance Observed the JHAToday Policy Center and verified corporate policies, including the Enterprise Cybersecurity Policy, are maintained in a location that is accessible by all personnel Observed the Ensenta SharePoint and verified Ensenta specific information security policies provide all personnel with security-based guidance and are maintained in a location accessible by all applicable Ensenta personnel	No Relevant Exceptions Noted
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	The organization’s business continuity and disaster recovery plans are reviewed and tested on an annual basis.	Interviewed the Compliance Analyst and verified the Business Continuity Plan is reviewed annually, and the disaster recovery plan is reviewed and tested annually Reviewed the Business Continuity Plan (Aril 20, 2020) and verified the plan is required to be updated annually and/or when a significant change occurs Reviewed the Ensenta Business Continuity and Disaster Recovery Program Overview Plan (January 2020) and verified the disaster recovery plan is required to be tested annually	No Relevant Exceptions Noted

		Reviewed the DR Test Results (January 2020) and verified the BCP/DR was performed on December 12, 2019, and the exercise consisted of performing a simulated failover to the newly built DR network, which included connectivity and application validations Observed all tests were successful and no changes or updates to documentation or processes were needed	

Trust Services Criteria for the Security, Availability, and Processing Integrity Categories

Logical and Physical Access Controls

Ctrl #	Description of Controls	Service Auditor’s Tests of Controls	Test Results
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.		
CC6.1.1	Source code for the organization is managed using a third-party version control system.	Interviewed the Scrum Master and verified source code is managed via Stash Git’s version control system Observed the Stash Git software repository and verified it is actively being utilized to track code modifications and to restrict access to the code base Observed Active Directory/Git access control lists and verified only developers, DBA, and NetOps have access to the application code Reviewed the System Security and Maintenance Policy and verified Stash Git is to be utilized to manage code changes	No Relevant Exceptions Noted
CC6.1.2	All users with the organization are required to have unique user IDs.	Interviewed the Systems Engineer, Senior and Systems/Network Administration, Senior Manager and verified all employees, including System Administrators, are required to have unique user IDs before being granted access to the networks and applications Observed Jack Henry and Ensenta Active Directory and EZAdmin access control systems and verified user IDs are unique Reviewed the Enterprise Cybersecurity Policy and verified an identity and access management policy has been established and each associate is required to have a unique user ID	No Relevant Exceptions Noted

CC6.1.3	Procedures are in place within the organization to define processes for the encryption of sensitive data at rest and the use of encryption keys.	Interviewed the Database Administration, Manager and Systems/Network Administration, Senior Manager and verified SQL Server Transparent Data Encryption (TDE), SQL Server Always Encrypted, and Storage Array Encryption are utilized to encrypt sensitive data at rest Observed FlashSystem configurations and verified the system is enabled to utilize AES-256-bit configuration, USB keys are utilized to hold the encryption keys, databases are mapped to the system, and the key management system is native, and users cannot change them Observed a sample of database backup files stored on the production fileserver system and verified the files are encrypted and data contained is meaningless if opened Observed data records in the production database and verified sensitive data is encrypted at rest with Always Encrypted Observed production DB schema and verified elements have been configured to encrypt the data in the columns Observed SQL database data and verified that columns containing sensitive information have been encrypted Observed key-custodian acknowledgement forms of the Ensenta personnel with access to encryption keys and verified all forms were signed and dated Reviewed the Data Protection Policy (December 18, 2019) and verified a policy has been established and defines the processes for changing	No Relevant Exceptions Noted

		encryption keys, frequency of rotation, and reasons that might necessitate an immediate key change	
CC6.1.4	SQL Server TDE is utilized by the organization to encrypt sensitive data at rest, including database backups and logs.	Interviewed the Database Administration, Manager and Systems/Network Administration, Senior Manager and verified SQL Server TDE, SQL Server Always Encrypted, and Storage Array Encryption are utilized to encrypt sensitive data at rest Reviewed the Encryption Procedures (December 18, 2019) and verified SQL Server TDE is utilized to encrypt sensitive data at rest Reviewed the Rotate Data Encryption Keys for SQL Server TDE process (February 6, 2020) and verified procedures have been developed to change TDE DEKs and they are required to be rotated every five years Reviewed the Rotate Key-Encrypting Key for SQL Server TDE process (February 6, 2020) and verified procedures have been developed to change TDE KEKs and they are required to be rotated annually Reviewed the Rotate Data Master Key for SQL Server TDE process (February 6, 2020) and verified procedures have been developed to change TDE master keys, and they are required to be rotated annually Observed query of the database encryption keys and certificates in the production environment and verified that encryption_state is 3, meaning the data is encrypted with TDE using AES-256-bit encryption Observed SQL TDE vendor documentation and verified database backups and logs are encrypted with the TDE functionality	No Relevant Exceptions Noted

		Observed the process of generating key encryption keys for SQL TDE and verified that the DEK and KEK are AES-256-bit keys and are stored in the master database	
CC6.1.5	Procedures are in place to guide the use of Always Encrypted master keys.	Reviewed the Always Encrypted Key Procedures (February 6, 2020) and verified procedures have been developed to change Always Encrypted master keys, and they are required to be rotated annually and the DEK to be rotated every five years Observed the process of generating key encryption keys for SQL Always Encrypted and verified that the DEK and KEK are AES-256-bit keys and are stored in different locations Interviewed the Database Administration, Manager and Systems/Network Administration, Senior Manager and verified SQL Server TDE, SQL Server Always Encrypted, and Storage Array Encryption are utilized to encrypt sensitive data at rest	No Relevant Exceptions Noted
CC6.1.6	Authentication and management mechanisms are utilized to restrict access to the organization's systems.	Interviewed the Systems Engineer, Senior and Systems/Network Administration, Senior Manager and verified authentication and management mechanisms are utilized to restrict access to systems Observed the Ensenta and Jack Henry Active Directories and EZAccess, SQL Server, standalone Linux systems, standalone networking devices, and standalone Flash Storage Arrays access control systems and verified access systems are utilized to restrict access to networks, systems, and applications, and the systems are limited to authorized individuals	No Relevant Exceptions Noted
CC6.1.7	Privacy policies have been implemented by the organization for handling personal information in accordance with relevant legislation and regulations.	Interviewed the Compliance Analyst and verified clients are responsible for providing end users with privacy notices related to the use of real-time, cloud-based solutions for mobile and	No Relevant Exceptions Noted

		online payment and deposit services, and clients sign MSAs which contain language related to confidentiality and are given access to the corporate Privacy Policy Reviewed the MSA template and verified there is a section related to confidentiality within the contract Reviewed the Privacy Policy and verified the policy is publicly available and discloses what data is collected and when and why data may be disclosed, as well as the processes to opt out	
CC6.1.8	Requirements related to the protection and return/destruction of confidential information are documented within the organization's mutual non-disclosure agreement (NDA).	Interviewed the Compliance Analyst and verified service providers are required to sign NDAs Reviewed the NDA template and verified intellectual property/trade secrets are agreed to be kept secret and requirements are defined relating to the protection and return/destruction of confidential information Observed the process of working with third parties where data is required to be shared and verified NDAs are signed by both parties prior to sharing the data	No Relevant Exceptions Noted
CC6.1.9	Policies related to proprietary rights and confidentiality agreements and the privacy of consumer financial information are documented within the Employee Handbook.	Reviewed the Employee Handbook and verified policies related to proprietary rights and confidentiality agreements and the privacy of consumer financial information have been documented Observed Jack Henry Policy Center records for 3 of 8 personnel hired over the audit period and verified the Employee Handbook was electronically acknowledged Interviewed the Compliance Analyst and verified personnel are required to sign Employee Handbook acknowledgements that contain	No Relevant Exceptions Noted

		Confidentiality Agreement language as part of the onboarding process	
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.		
CC6.2.1	Project plans are utilized to facilitate the client onboarding process.	Interviewed the Director of Installations and verified new clients are assigned an Implementation Coordinator, who creates a Salesforce project plan and sets up/revokes the client's services in EZAdmin Observed 25 of 247 setup forms and Salesforce projects for new client onboards and verified that Project Plans are generated to facilitate the onboarding process Observed EZAdmin system configurations for the 25 of 247 new client onboards and verified that they had been added to the system	No Relevant Exceptions Noted
CC6.2.2	Clients are required to provide a service cancellation notice to have their accounts or systems removed from Ensenta's services.	Interviewed the Customer Support Manager and verified the client must provide a service cancellation notice to Jack Henry Ensenta, then the accounts or systems are removed on an agreed upon timeline Observed 5 of 49 Salesforce escalations generated to facilitate a client offboarding and verified that client accounts or systems were requested to be disabled Observed EZAdmin configurations for 5 of 49 clients requesting a full departure from services or partial removal of services and verified that the client accounts or individual systems were disabled from EZAdmin and the data returned or deleted as required by MSAs	No Relevant Exceptions Noted
CC6.2.3	Defined processes are in place for registering and deregistering client access to the organization's application.	Interviewed the Implementation Manager and verified new clients are assigned to an Installation team member who sets up/revokes the	No Relevant Exceptions Noted

		client's accounts in EZAdmin, and clients are responsible for adding or removing accounts for their personnel Observed the client onboarding process and verified the setup form has been completed and client administrative account(s) and any other account that has been communicated to be set up Observed the client offboarding process and verified a client's administrative account and any other accounts are systematically disabled	
CC6.2.4	Defined processes are in place for authorizing and approving user access to the organization's corporate systems and development environment.	Interviewed the Systems Engineer, Senior and Scrum Master and verified HR or Hiring Managers create a Cherwell/JSource ticket requesting access to Jack Henry corporate systems and Ensenta development environment, and managers or NetOps creates YouTrack tickets and approves or denies access to the Ensenta systems Observed YouTrack tickets utilized to request access for 3 of 8 personnel hired over the audit period and compared them to the access granted to the Ensenta managed Active Directory access control systems and verified the access requests were authorized, that access was not provided until the request was made, and that the access provided to the new employees matched that which was requested Observed 3 of 8 Cherwell/JSource tickets utilized to request access of personnel hired over the audit period and verified that Cherwell/JSource is utilized to request access to Jack Henry corporate systems Reviewed the Corporate Active Directory Policy (January 20, 2020) and verified access requirements for	No Relevant Exceptions Noted

		systems and network access management have been established Reviewed the Access Control Policy (April 14, 2020) and verified a workflow has been established for creating, changing, or terminating logical access	
CC6.2.5	Access to the organization's systems is required to be revoked immediately or upon the agreed termination date for terminated or separated employees.	Interviewed the Systems Engineer, Senior and Scrum Master and verified the access of terminated personnel is required to be revoked immediately or upon the agreed termination date Observed Ensenta managed Active Directory domains and EZAdmin platform access control systems and verified logical access granted to the 3 of 4 personnel terminated over the audit period was removed or inactive Observed the Jack Henry Corporate Active Directory access control system and verified logical access granted to the 3 of 4 personnel terminated over the audit period was removed or inactive Observed Continuum's access control list and verified that physical access granted to 3 of 4 personnel terminated over the audit period was removed or inactive Reviewed the Account Management Policy (August 29, 2019) and verified all Active Directory accounts and remote access are required to be removed when personnel are terminated Reviewed the Jack Henry Enterprise Cybersecurity Policy and verified physical access is required to be revoked when personnel access is no longer necessary *Exception: One terminated user account still existed in one of the lower development environments. Once*	Exception Noted

		identified, Ensenta removed the account, and the auditor validated this was performed before the audit was completed.	
CC6.2.6	Network password complexity and privileges are enforced through Active Directory and/or native access controls within applications.	Interviewed the Systems Engineer, Senior and Systems/Network Administration, Senior Manager and verified network password complexity and privileges are enforced through Active Directory and/or native access controls in applications Observed four Ensenta Active Directory group policies and verified that password control parameters include the following: • Password must meet complexity requirements: Enabled • Minimum password length: 8 characters • Maximum password age: 90 days • Minimum password age: 1 day • Enforce password history: 12 passwords remembered • Store passwords using reversible encryption: Disabled Observed Jack Henry Active Directory group policies and verified that password control parameters include the following: • Password must meet complexity requirements: Enabled • Minimum password length: 8 characters • Maximum password age: 90 days • Minimum password age: 1 day • Enforce password history: 12 passwords remembered • Store passwords using reversible encryption: Disabled Observed pwquality.conf file and verified that “lcredit=1,” “dcredit=1,” “ucredit=1,” “ocredit=1,” “minclass= 1,” “maxrepeat=3,” and “minlen=8”	No Relevant Exceptions Noted

CC6.2.7	Account lockouts are configured and enforced within the organization’s systems.	Observed four Ensenta Active Directory group policies and verified that account lockout parameters include the following: • Account lockout duration: 240 minutes • Account lockout threshold: 6 invalid logon attempts • Reset account lockout counter after 120 minutes Observed Jack Henry Active Directory group policy and verified account lockout parameters include the following: • Account lockout duration: 240 minutes • Account lockout threshold: 6 invalid logon attempts • Reset account lockout counter after 120 minutes Reviewed the SSG Standards – Passwords document and verified Jack Henry corporate password and lockout parameters have been defined and align with the test results above Observed system-auth file and verified that “retry=3” and “unlocktime=never”	No Relevant Exceptions Noted
CC6.2.8	First-time and password reset procedures are in place within the organization.	Observed the process to set first-time passwords and verified that HR tools automatically set up a new user in Jack Henry Active Directory and generate the first-time password when creating the account Observed the JHAToday system and verified users can automatically reset their password when inside the Jack Henry network Observed the process for resetting passwords remotely and verified Jack Henry Helpdesk asks three challenge questions to validate the person’s identity before resetting the password; Active Directory is set to enforce the password change on the initial login	No Relevant Exceptions Noted

		Observed the process for resetting passwords in Ensenta Production, DR, ECUAT, and ECDevelopment environments Reviewed the SSG Standards – Passwords document (March 6, 2020) and verified users have a mechanism to change their passwords and validate the user prior to changing the password	
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.		
CC6.3.1	Policies and processes are in place within the organization to govern the granting, modification, and revocation of access to systems and applications.	Interviewed the Systems Engineer, Senior and Scrum Master and verified processes to govern the granting, modifying, and revocation of access to systems and applications have been established Observed YouTrack tickets utilized to request access for 3 of 8 personnel hired over the audit period and compared them to the access granted to the Ensenta managed Active Directory access control systems and verified the access request was authorized, access was not provided until the request was made, and the access provided to the new employees matched that which was requested Observed 3 of 8 Cherwell/JSource tickets utilized to request access of personnel hired over the audit period and verified that Cherwell/JSource is utilized to request access to Jack Henry corporate systems Reviewed the Corporate Active Directory Policy and verified access requirements for systems and network access management have been established	No Relevant Exceptions Noted

		Reviewed the Access Control Policy and verified a workflow has been established for creating, changing, or terminating logical access	
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	Access to the organization's office suite is managed through a centralized access control system.	Interviewed the Systems/Network Administration, Senior Manager and verified Jack Henry corporate manages the physical security of its corporate office space; if doors are opened without using an access card, Asset Protection is notified, and they send the police if the incident occurs after hours Observed Continuum access control systems and verified access to the office suite is managed through the centralized access control system and notifications are made if the doors are opened without an access card *Note: Observations were performed via a virtual onsite using a Webex session.*	No Relevant Exceptions Noted
CC6.4.2	A video surveillance system is in use within the organization, and data is stored for at least three months.	Interviewed the Systems/Network Administration, Senior Manager and Asset Protection, Supervisor and verified Jack Henry corporate manages a video surveillance system to monitor access to the corporate facility; the Branson data center is managed by Jack Henry corporate systems Observed the corporate facility during a virtual onsite visit and verified four video cameras are strategically located to monitor access to the facility Observed video cameras are mounted on ceilings of the facilities and are protected with coverings to prevent tampering or disabling Observed the FLIR video management system and verified video recordings	No Relevant Exceptions Noted

		are maintained for at least 90 days and the system and cameras are operational Reviewed the Physical Security Policy (December 18, 2019) and verified surveillance cameras are utilized and data is stored for at least three months *Note: Observations were performed via a virtual onsite using a Webex session.*	
CC6.4.3	Visitor logs are in use within the organization’s corporate facility, and the logs are required to be retained for at least one year.	Interviewed the Systems/Network Administration, Senior Manager and verified a visitor log system or paper visitor log is utilized to document visitor entry to the corporate facilities Observed reception areas of the corporate facility during virtual onsite and verified that visitor logs were present and that visitors are required to document their name, company, date and time entering/leaving the facility, and employee being visited; a confidentiality notice is on the top of the registration form Observed visitor logs and verified consistent usage over the audit period and that the logs are retained for at least one year Reviewed the Visitor Access Policy (December 20, 2019) and verified visitors are required to sign visitor logs and the logs are required to be retained for at least one year *Note: Observations were performed via a virtual onsite using a Webex session.*	No Relevant Exceptions Noted
CC6.4.4	Physical security and access controls are in place within the organization’s facility and are managed by Jack Henry corporate.	Interviewed the Systems/Network Administration, Senior Manager and verified Jack Henry corporate manages the physical security of its corporate office space Observed the multi-tenant facility via a virtual onsite and verified the facility	No Relevant Exceptions Noted

		has three access points, which are locked at all times and require an access card; all facility access is managed by the building’s facility management Observed elevators via a virtual onsite and verified an access card is required to get to any floor and access is restricted to only those floors allowed by the access card Observed the corporate office space via a virtual onsite and verified the offices suite is located on the second floor and has four perimeter doors: the main lobby and three other entrances Observed the Continuum card access control system and electronic and magnetic locking systems and verified office suite and server room access is controlled by a centralized access control system Observed the corporate data center via a virtual onsite and verified the perimeter doors are locked at all times and a proximity badge is required before access is allowed Observed the Continuum access control list and verified security profiles exist that restrict personnel to the office suite and security zones related to their job responsibilities Observed the Continuum access control list and verified logs are retained for at least 12 months Observed the Continuum access control list and verified that access is restricted to authorized personnel Observed the Continuum access control list and verified that each employee has a unique account	

		Observed the Continuum access control list and verified the access for the 3 of 4 personnel terminated over the audit period was disabled or removed Reviewed the Physical Security Policy and verified guidance for physical security controls has been established *Note: Observations were performed via a virtual onsite using a Webex session.*	
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.		
CC6.5.1	Documented guidelines are in place for destroying paper and electronic media containing sensitive or confidential information.	Reviewed the Data Handling Requirement Standards (September 3, 2020) and verified data handling guidelines have been established and describe how to secure and destroy media Reviewed the Records and Data Retention Policy (May 13, 2020) and verified guidelines are in place for destroying paper and electronic media that contains sensitive or confidential information *Note: Observations were performed via a virtual onsite using a Webex session.*	No Relevant Exceptions Noted
CC6.5.2	Defined processes are in place within the organization to ensure the secure destruction of media and equipment.	Interviewed the Systems/Network Administration, Senior Manager and verified hardcopy materials and electronic storage devices are required to be shredded when no longer necessary Observed the corporate office suite and verified one DataSafe shred bin is positioned within the facility, the bin is secured with a lock, the opening of the bin is small enough to prevent retrieval of documents from within the bin, and the volume of paper contained within the bin is not causing overflow or	No Relevant Exceptions Noted

		causing personnel to discard sensitive documents in alternative locations Observed processes for destroying electronic media at the Ensenta corporate facility and verified hard drives are picked up and destroyed by DataSafe Observed the Branson, Missouri, data center and verified that a MediaClone SuperWiper Pro device is established *Note: Observations were performed via a virtual onsite using a Webex session.*	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	Two-factor authentication is required to be in use for remote access to the organization's networks.	Interviewed the Systems Engineer, Senior and Systems/Network Administration, Senior Manager and verified the following: • The production and DR networks are remotely accessed through AnyConnect VPN systems and are configured for two-factor authentication • The ECUAT network is remotely accessed via RDP only after connecting to the production or DR network • Jack Henry F5 VPN is utilized to access the Jack Henry corporate and development networks Observed AnyConnect VPN configurations and verified unique certificates are installed on workstations and are required along with a traditional credential set prior to being allowed access to systems Observed responsible personnel authentication and verified access requires a traditional user ID and password and the unique certificate assigned to the workstation/laptop	No Relevant Exceptions Noted

		Observed F5 VPN and SafeNet Authentication Service configurations and verified users utilize their Active Directory credentials and once authenticated are forwarded to SafeNet Authentication Service for the second factor of authentication Observed SafeNet Authentication Service configurations and verified the accounts are configured to use MobilePASS or eToken tokens, which enforces all personnel and users to authenticate with two-factor authentication before being allowed to access systems Observed responsible personnel authentication and verified access requires a traditional user ID and password, a fob is used to provide the 6-character OTP, and a unique four-digit PIN must be entered before access is granted Reviewed the Data Handling Requirement Standards and verified two-factor authentication is required when accessing Tier 1 data remotely Reviewed the Access Control Policy and verified that all non-console access requires multi-factor authentication	
CC6.6.2	Defined procedures are in place to ensure all sensitive information is encrypted and protected when transmitted and stored within the organization.	Interviewed the Systems Engineer, Senior and Scrum Master and verified passwords are stored encrypted or hashed equivalents are stored by native systems Observed Ensenta Active Directory group policy configurations on all four Active Directory domains and verified that Kerberos is enabled Observed Ensenta Active Directory configurations on all four Active Directory domains and verified "Store passwords using reversible encryption" is set to "Disabled"	No Relevant Exceptions Noted

		Observed Jack Henry corporate Active Directory group policy configurations and verified Kerberos is enabled Observed Jack Henry corporate Active Directory configurations and verified “Store passwords using reversible encryption” is set to “Disabled” Reviewed the password procedures and verified passwords are required to be encrypted during transmission and storage on all system components	
CC6.6.3	A firewall solution is in place to screen traffic from the internet and between the DMZ and/or the internal network, and it is configured to deny all traffic that is not explicitly authorized for a specific business need.	Interviewed the Scrum Master and verified a firewall solution is in place to screen traffic from the internet and between the DMZ and/or the internal network and is configured to deny all traffic that is not explicitly authorized for a specific business need and only allow traffic that is necessary to perform business Observed firewall configurations in the production and DR environments and verified traffic is restricted at the network perimeter and between the DMZ and/or the internal networks to only that which is necessary to perform business operations Observed firewall configurations at the corporate office suite and verified traffic is restricted at the network perimeter to only that which is needed for business operations Observed Network Security Group configurations in the ECUAT and ECDEV environments and verified traffic is restricted at the network perimeter and between the DMZ and/or the internal networks in the production and DR environments Observed the Nipper report and verified firewall configurations are reviewed at least annually against industry-accepted configurations	No Relevant Exceptions Noted

		Observed the process to address firewall configuration findings and verified the findings were identified as false positives, remediated, or accepted as necessary for business processes and added to the risk assessment	
CC6.6.4	The organization's firewall rule sets are required to be reviewed every six months.	Observed two YouTrack tickets and verified firewall rule sets are reviewed every six months Reviewed the Firewall Standards and Procedures and verified network architecting and configuration guidance has been provided for firewalls and firewalls rules should be audited every six months	No Relevant Exceptions Noted
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.		
CC6.7.1	Information involved in application service transactions is protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay.	Interviewed the Systems Engineer, Senior and Scrum Master and verified the following: • HTTPS/TLS protocols are utilized when information is transmitted over the internet • Cisco AnyConnect VPN technologies utilize SSL/TLS to encrypt the traffic to the Ensenta production, DR, and ECUAT environments, and F5 VPN utilizes SSL/TLS to encrypt the traffic to the Jack Henry networks and Ensenta EcDev environments • FTPS/SFTP technologies are utilized to transmit data to some clients • RDP is utilized to manage systems remotely Observed the results of running Qualys SSL Labs scans and verified TLS 1.1 and/or 1.2 protocols are utilized to encrypt communications over the internet, certificates are valid and issued by Comodo RSA Organization Validation Security Server CA, some acceptable cipher suites are configured	No Relevant Exceptions Noted

		to be utilized, and the scan resulted in an “A” or “B” rating Observed Registry Hive for 4 of 33 production, 3 of 24 DR, 3 of 12 UAT, and 4 of 30 development and verified TLS 1.1 and 1.2 protocols have been configured Observed SFTP/FTPS configurations in production, DR, ECUAT, and development environments and verified that SSH-2 and TLS 1.2 are utilized Reviewed AnyConnect VPN configurations and verified the TLS 1.2 protocol is configured for VPN to access the Ensenta production, DR, and ECUAT environments Reviewed F5 VPN configurations and verified the TLS 1.2 protocol is configured for VPN to access the Jack Henry networks and Ensenta EcDev environments Observed Active Directory group policy configurations on all four Active Directory domains and verified that “Require use of specific security layer for remote (RDP) connections” is set to “Enabled”; “Security Layer” is set to “SSL (TLS 1.0)”; “Server authentication certificate template” is set to “Enabled”; “Certificate Template Name” is set to “RemoteDesktopSSL” or “RemoteDesktopSecure”; “Set client connection encryption level” is set to “Enabled”; “Encryption Level” is set to “High Level”; and “Choose the encryption level from the drop-down list” is not enabled	
CC6.7.2	The organization’s development/test environments are required to be separated from the production environments.	Interviewed the Scrum Master and verified development, UAT, DR, and production environments are unique environments that are logically separated	No Relevant Exceptions Noted

		Observed Active Directory access control lists and network configurations and verified development, UAT, DR, and production environments are logically separated Reviewed the System Security and Maintenance Policy and verified development/test environments are required to be segregated from production environments	
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.		
CC6.8.1	Trend Micro Deep Security is deployed to all servers in the organization's production and disaster recovery environments.	Interviewed the Systems/Network Administration, Senior Manager and Information Security Engineer, Advanced and verified Trend Micro Deep Security is deployed to all servers in the production and DR environments Observed the Trend Micro Deep Security configuration in the production environment and verified antivirus is installed on all servers and running, scans are scheduled to run on Thursdays at 11 PM, and new updates are pulled daily at 9:55 AM and are pushed to the systems daily at 9:30 PM Observed the Trend Micro Deep Security configuration in the DR environment and verified antivirus is installed on all servers and running, scans are scheduled to run daily at 5:30 PM, and new updates are pulled daily at 10 PM and are pushed to the systems weekly at 12:40 PM Reviewed the Antivirus Requirement Policy (January 6, 2020) and verified the following: • Virus protection is required on all systems and workstations running Windows, Linus, or Mac operating systems • It is enabled to scan in real-time	No Relevant Exceptions Noted

		• It is scheduled to run regularly scheduled scans no less than monthly • The definitions must be updated no less than weekly	
CC6.8.2	Microsoft Windows Defender is deployed to all servers in the organization’s development and UAT environments.	Interviewed the Systems/Network Administration, Senior Manager and Information Security Engineer, Advanced and verified Windows Defender is deployed to all servers in the development and UAT environments Observed Azure Management Console’s anti-malware configurations in the ECUAT and ECDEV environments and verified antivirus is installed on all servers and running, scans the systems in real-time, and signatures and updates are part of the monthly patching process Reviewed the Antivirus Requirement Policy (January 6, 2020) and verified the following: • Virus protection is required on all systems and workstations running Windows, Linus, or Mac Operating Systems • It is enabled to scan in real-time • It is scheduled to run regularly scheduled scans no less than monthly • The definitions must be updated no less than weekly	No Relevant Exceptions Noted
CC6.8.3	McAfee ePolicy Orchestrator is deployed to all laptops and is scheduled to run at regular intervals to ensure the virus signatures are kept up to date.	Interviewed the Systems/Network Administration, Senior Manager and Information Security Engineer, Advanced and verified McAfee ePolicy Orchestrator is deployed to all laptops and is scheduled to run at regular intervals to keep the virus signatures up to date Observed McAfee ePolicy Orchestrator configurations and verified antivirus is configured to perform automatic updates and push	No Relevant Exceptions Noted

		them to the managed workstations daily at 11:30 AM Observed McAfee ePolicy Orchestrator configurations and verified antivirus is configured to perform periodic scans on workstations Observed McAfee ePolicy Orchestrator Management Console reports and verified antivirus definitions were updated within the past two days Reviewed the Antivirus Requirement Policy (January 6, 2020) and verified the following: • Virus protection is required on all systems and workstations running Windows, Linus, or Mac operating systems • It is enabled to scan in real-time • It is scheduled to run regularly scheduled scans no less than monthly • The definitions must be updated no less than weekly	

Trust Services Criteria for the Security, Availability, and Processing Integrity Categories			
System Operations			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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.		
CC7.1.1	The organization ensures that applications are not vulnerable to injection flaws, buffer overflow, cryptographic storage, insecure communications, improper error handling, and "High" vulnerabilities.	Interviewed the Scrum Master and verified that application code changes are reviewed by a developer who is not the code's author and who is knowledgeable in security coding practices and that changes are reviewed against OWASP security recommendations and best practices; an acceptable result is obtained prior to promoting code to production Observed 30 of 442 YouTrack tickets and verified code reviews are performed by developers other than the code's author and code reviews are accepted prior to be merged into the release build Observed the developer training spreadsheet and verified developers had received application security training within the previous 12 months Observed Veracode application scanning is performed every Wednesday against Git and notifications are sent to the development team for issues detected so that they can be researched and verified Reviewed 5 of 52 Veracode scan reports and verified application scans are performed weekly Reviewed the System Security and Maintenance Policy and verified code changes are required to be reviewed by personnel other than the author of the code	No Relevant Exceptions Noted

		Reviewed the PCI System Testing Policy (December 18, 2019) and verified Veracode scans are required to be performed every Wednesday	
CC7.1.2	Internal and external vulnerability scans are required to be performed quarterly and after any significant change to the networks, and external and internal penetration testing is required to be performed annually and after any significant changes.	Interviewed the Scrum Master and verified the following: • Internal and external penetration testing and web application scans on the production networks are performed annually by a third party specializing in penetration testing • Internal and external vulnerability scans are performed at least quarterly on the production networks • External/internal penetration testing is performed twice per year, and application scans are performed annually • Veracode is executed weekly by Ensenta on the application code Reviewed external vulnerability scans and internal vulnerability scans and verified vulnerability scans are performed at least quarterly Reviewed the external/internal penetration test (performed March 16 and March 20, 2020 by NTTSecurity) and verified external penetration testing and application scans are performed annually by a third party specializing in penetration testing and/or vulnerability scan testing Reviewed the external/internal penetration test and verified critical and high issues that were identified were retested to validate the remediation efforts Reviewed the PCI System Testing Policy and verified internal and external vulnerability scans are required to be performed quarterly and after any significant change to the networks and external and internal	No Relevant Exceptions Noted

		penetration testing is required to be performed annually and after any significant change; any “critical” or “high” vulnerabilities identified in the testing are required to be remediated and retested to validate that the vulnerability has been remediated Reviewed App Scan Reports (July 7, 2020) and verified application scans are performed annually and by a third-party provider Reviewed 5 of 52 Veracode scan reports and verified application scans are performed weekly Reviewed external vulnerability scans, internal vulnerability scans, penetration tests, application scans, and Veracode scans	
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.		
CC7.2.1	Network logging and monitoring systems are in use within the organization’s environment.	Interviewed the Systems/Network Administration, Senior Manager and Network Engineer, Advanced and verified production systems are configured to log and are offloaded to the NTT Security’s syslog collector and Jack Henry Splunk centralized logging systems; the DR, ECUAT, and ECDEV environments are configured to log and offload the logs to the Jack Henry Splunk centralized logging system Observed the Splunk system and NTT system and verified logs are retained for 12 months Observed NTT Security’s syslog collector and Splunk system configurations and verified systems have been configured to detect anomalous activity or activity exceeding trigger levels and to send alerts to IT personnel to investigate	No Relevant Exceptions Noted

		Reviewed the Internal Event Logging Policy (February 3, 2020) and verified logging must be enabled on systems and the logs are offloaded for centralized storage and alerting	
CC7.2.2	Audit logs within the organization are required to document defined elements.	Reviewed the System Monitoring Policy (December 18, 2019) and verified audit logs are required to contain the following elements: • User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected data, system component, or resource Observed the Splunk system and verified the logs contain the following elements: • Source IP • Destination IP • Destination port • Protocol type (e.g., TCP, UDP, ICMP) for certain devices • Timestamp Observed the NTT Security's syslog collector system and verified the logs contain the following elements: • Source IP • Destination IP • Destination port • Protocol type (e.g., TCP, UDP, ICMP) for certain devices • Timestamp	No Relevant Exceptions Noted
CC7.2.3	Unauthorized activity, critical IDS alerts, and unauthorized critical system or content file changes are monitored by the organization's personnel, and alerts are investigated as needed.	Interviewed the Systems/Network Administration, Senior Manager and verified Ensenta NetOps and Jack Henry security personnel are responsible for investigating system and network device alerts and invoking the incident response plan if necessary Observed the Splunk system and verified IDS/IPS and FIM alerts are	No Relevant Exceptions Noted

		programmatically monitored for issues or exceeding trigger levels and send alerts to Ensenta NetOps and Jack Henry Security personnel Observed Cisco wIPS system and verified rogue wireless alerts are sent to both the Prime – Data Center Rogue access points (APs) dashboard and Splunk – Data Center Rogue APs dashboard, which are reviewed daily by Cybersecurity personnel Observed alerts are reviewed by Cybersecurity personnel daily and the issues identified are researched, investigated, and invoke the incident response process if necessary Observed the EventListener is running to programmatically detect issues Observed NCR Managed Services is responsible for monitoring IPS alerts in the production environment and it reaches out to Ensenta NetOps personnel if issues are detected Reviewed the Security and Monitoring Response Process (March 30, 2020) and verified the Security team is on call at all times to respond to incidents Reviewed the Ensenta Incident Management Policy and verified the following alerts are monitored: • Unauthorized activity • Critical IDS alerts • Unauthorized critical system or content file changes	
CC7.2.4	Intrusion detection and prevention systems are in use within the organization's various environments, and alerts are forwarded to the necessary personnel for response.	Interviewed the Network Security Engineer and Network Engineering, Manager and verified the following: • Cisco Sourcefire's Next-Generation IPS has been implemented in the networks to perform intrusion detection/prevention on the production environment and is	No Relevant Exceptions Noted

		managed by NCR managed services • The DR and development environments utilize McAfee Network Security Manager and IBM Security SiteProtector Systems to perform intrusion detection/prevention and are managed by Jack Henry hosted services • The ECUAT environment utilizes Azure IDS/IPS technologies and is managed by Ensenta personnel • OSSEC is implemented in the production and DR environments Observed the results of running scripts on 30 of 460 servers and verified OSSEC is running on the production and DR servers Observed NCR manages the production firewall and reviewed NCR's Managed Service Provider PCI DSS AoC and verified firewalls or other IPS/IDS is required to be configured in the production environment Reviewed Azure documentation and verified IDS runs by default on public IPs in the ECUAT environment and alerts are forwarded to Splunk for alerting NetOps and Jack Henry Security personnel Observed McAfee Network security Manager and IBM Security SiteProtector system configurations and verified IPS appliances are implemented on the DR and development networks to monitor ingress and egress traffic at the perimeter of the networks and send alerts to the Jack Henry hosted services team Reviewed the Firewall Policy and verified intrusion detection is required to be enabled on firewalls	

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.		
CC7.3.1	Security incidents are analyzed to determine appropriate remediation and prevention activities.	Interviewed the Senior Scrum Master and verified incident response plans and procedures are documented to guide personnel on how to identify, respond to, recover from, and if necessary, escalate security-related incidents to executive management Observed Incident Report 203, in which an incident occurred on May 11, 2020, and verified incidents are investigated and if necessary, remediated and documented Observed processes are updated as needed to prevent the reoccurrence of the incident if possible	No Relevant Exceptions Noted
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.		
CC7.4.1	Incident response policies and procedures have been formally documented and implemented to define incident identification, reporting, containment, and remediation processes.	Interviewed the Senior Scrum Master and verified incident response plans and procedures are documented to guide personnel on how to identify, respond to, recover from, and if necessary, escalate security-related incidents to executive management Observed Incident Report 203, in which an incident occurred on May 11, 2020, and verified incidents are investigated and if necessary, remediated and documented Observed processes are updated as needed to prevent the reoccurrence of the incident if possible	No Relevant Exceptions Noted
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	The organization incorporates lessons learned from incident response activities into the incident response policies and procedures.	Observed Incident Report 203, in which an incident occurred on May 11, 2020, and verified incidents are investigated and if necessary, remediated and documented	No Relevant Exceptions Noted

		Observed processes are updated as needed to prevent the reoccurrence of the incident if possible	
CC7.5.2	A defined process is in place to ensure that security updates and patches are installed in a timely manner.	Interviewed the Systems/Network Administration, Senior Manager and System Network Administrator, Manager and verified a process exists to ensure that security updates/patches are installed in a timely manner, generally within one month Observed SCCM system in the production environment and verified update groups are manually created from the approved patches from the lower development environment and then pushed out to the servers; if a reboot is necessary, it is manually rebooted, and database patches are staggered in timelines from the other servers Observed SCCM systems in the production environment and verified all critical and security patches older than 30 days had been installed on the Windows servers Observed the process for updating Linux servers in the production environment and verified US-CERT is utilized to identify critical and security-related patches, and if identified, it triggers the Linux patching processes Observed Linux server logs in the production environment and verified yum update is manually executed as needed to download any available patches from the yum patch repository server Observed the yum patch repository server logs in the production environment and verified yum update is manually executed as needed to download any available patches	No Relevant Exceptions Noted

		Observed SCCM system in the DR environment and verified update groups are manually created from the approved patches from the lower development environment and then pushed out to the servers; if a reboot is necessary, it is manually rebooted, and database patches are staggered in timelines from the other servers Observed SCCM systems in the DR environment and verified all critical and security patches older than 30 days had been installed on the Windows servers Observed the Azure Update Manager in the ECUAT environment and verified patching deployment schedules are manually created from the approved patches from the lower development environment and then pushed out to the servers; if a reboot is necessary, it is manually rebooted, and database patches are staggered in timelines from the other servers Observed the process for updating Linux servers in the ECUAT environment and verified US-CERT is utilized to identify critical and security-related patches, and if identified, that triggers the Linux patching processes Observed Linux server logs in the production environment and verified yum update is manually executed as needed to download any available patches from the yum patch repository server Observed the WSUS system in the ECDEV environment and verified patching is configured for auto download on patch Tuesday and manual review and approval; databases are staggered on different days than the servers	

		Observed the Power BI Compliance Reporting Dashboard and verified Jack Henry Corporate SCCM enforces Jack Henry Windows workstation to download patches monthly and reboot as necessary Observed corporate Jamf Pro configurations and verified that the update policy is set to push new patches out every 15 minutes	
CC7.5.3	Outside sources are utilized to identify new vulnerabilities that could impact the organization's networks and systems.	Observed patches and vulnerabilities are designated with "security," "high," or other risk ranking Reviewed the Jack Henry Vulnerability Management Policy (July 1, 2019) and verified security patches are required to be installed within 30 days Reviewed the Network and Systems Configuration Standards and verified security resources and vendor notifications must be monitored Interviewed the Systems/Network Administration, Senior Manager and System Network Administrator, Manager and verified outside sources are utilized to identify new vulnerabilities that could impact networks and systems	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Processing Integrity Categories

Change Management

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
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.		
CC8.1.1	Change management policies and procedures are in place within the organization and require the documentation of authorization and the testing of functionality.	Interviewed the Scrum Master and verified change management policies and procedures are implemented and require the documentation of approval by authorized parties and the testing of functionality; YouTrack is utilized to facilitate the change management process Observed 30 of 237 YouTrack tickets utilized to promote changes to the production environment and verified the following: • Tickets document the change to be performed and are approved by management • Changes are tested in a separate, controlled environment if possible • Appropriate personnel perform the migration of changes to production in a controlled manner • Backout procedures are managed through Argosec and/or Octopus or other programmatic ways to revert back to previous configurations	No Relevant Exceptions Noted
CC8.1.2	Procedures are in place within the organization to manage changes to the production system.	Reviewed the Change Management Policy (September 11, 2020) and verified a system change procedure has been established and the following is required for every change to the production system: • Authorization • Change Advisory Board • Change Calendars • Change Freeze Periods • Change Maturation • Closure and Verification • Configuration Item Requirement	No Relevant Exceptions Noted

		- Defining Change - Documentation - Emergency Changes - Lead Time - Payment Card Industry Data Security Standard (PCI DSS) - Post-Implementation Review - Recording Change - Related Incidents/Problems - Risk Assessment - Segregation of Duties - Single Tool - Testing - Unauthorized Changes - Deployment	
CC8.1.3	Configuration standards are in place within the organization to ensure servers, workstations, and systems are appropriately hardened prior to deployment.	Interviewed the Scrum Master and verified the following: - The Windows server configuration standard is based off of the NIST Windows Server STIG, and all Windows systems are hardened prior to being deployed to Ensenta networks - Linux systems are configured based on industry best knowledge of Jack Henry personnel - AlgoSec is utilized to validate that network devices are configured to meet PCI and ISO requirements Observed that the Angosec system is used to monitor firewalls and that load balancers device configurations are compliant with PCI, ISO, NIST, and vendor best practices Observed the results of running scripts on configurations for 30 of 460 servers and verified the configurations align with the configuration standards Reviewed the Workstation Configuration Standards (December 5, 2019) and verified workstations are hardened prior to connecting to networks	No Relevant Exceptions Noted

		Reviewed the Ensenta Network Systems Configuration Standards Policy (December 18, 2019) and verified network and system components are required to be hardened prior to being promoted to the production environment and utilize configurations that are based on the NIST Windows Server STIG	
CC8.1.4	Firewall configuration guidelines are in place within the organization.	Reviewed the Ensenta Firewall Standards and Procedures (December 18, 2019) and verified network architecting and configuration guidance have been provided for firewalls and firewalls rules should be audited every six months Observed firewall configurations and verified the configuration setting aligns with PCI configuration requirements Reviewed the Firewall Standards (November 21, 2019) and verified the organization has formally documented hardening guidelines for firewalls Observed the Angosec system is used to monitor firewalls	No Relevant Exceptions Noted
CC8.1.5	Configuration standards within the organization are required to be updated as new vulnerabilities are identified.	Interviewed the Systems/Network Administration, Senior Manager and verified the following: • Vulnerabilities are monitored and reviewed and if needed, changes to Active Directory group policy, which is configured to the NIST Windows Server STIG, are altered to ensure the vulnerability does not enter the production environment with the introduction of new systems • AlgoSec policies are updated so that network devices are reviewed against the new policy • The few Linux systems that exist are manually configured if necessary	No Relevant Exceptions Noted

		Observed the process of reviewing issues that impact configuration standards and verified that penetration test results and vulnerability scan results are reviewed to understand if there is an impact to the configuration standards and the AD Group Policy and/or AlgoSec policy are updated as necessary Reviewed the Ensenta Network Systems Configuration Standards Policy and verified that standards are required to be updated as new vulnerabilities are identified	
CC8.1.6	Application and system change management procedures are in place within the organization.	Observed 30 of 442 YouTrack tickets utilized to promote code changes to the production environment and verified the following: • Ticket includes description/ technical specifications • Tickets are approved by management • Peer reviews are performed • Source code is checked out or copied to a test or development environment • Program changes are tested in a separate, controlled environment • Appropriate personnel perform the migration of changes to production in a controlled manner • Release to production and backout procedures are managed through Octopus Reviewed the System Security and Maintenance Policy (June 30, 2020) and verified an application and system change procedure has been established and the requirements are defined for all change to the production system	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, and Processing Integrity Categories

Risk Mitigation

Ctrl #	Description of Controls	Service Auditor’s Tests of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	The organization identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Reviewed the Ensenta Risk Assessment and verified the risk assessment process was followed and controls are implemented to address the following: • Fraud teams and tools have been set up to detect fraud • System impact and likelihood are assessed • Reviews are performed of the risk of potential business disruptions and legal impact • Vendors are assessed annually for SOC compliance • Management reviews risk assessment and management approves remediation or accepts risk	No Relevant Exceptions Noted
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	The organization assesses and manages risks associated with vendors and business partners.	Reviewed the Third-Party Risk Management Policy (June 2020) and verified that vendor compliance is reviewed periodically	No Relevant Exceptions Noted
CC9.2.2	Service level agreements (SLAs) are negotiated and formalized within client contracts.	Interviewed the Senior Scrum Master and verified SLAs are negotiated and formalized in client contracts Observed uptime spreadsheets/reports and verified uptimes are monitored monthly by management to ensure that SLA obligations are being met Reviewed the MSA template and verified the contract included the SLAs agreed upon by the two parties	No Relevant Exceptions Noted
CC9.2.3	Potential clients and service providers are required to sign non-disclosure agreements prior to the sharing of information.	Interviewed the Compliance Analyst and verified potential clients and service providers sign non-disclosure agreements before sharing	No Relevant Exceptions Noted

		information, and clients sign contracts with specific language regarding confidential information Reviewed the MSA template and verified there is a section related to confidentiality Reviewed the NDA template and verified intellectual property/trade secrets are agreed to be kept secret and the agreement defines requirements related to the protection and return/destruction of confidential information	
CC9.2.4	Subservice providers within the organization are monitored for compliance through the annual review of audit reports.	Interviewed the Audit Support Analyst and verified subservice providers are monitored for compliance by requesting and reviewing the most recent compliance reports; during periods between the completion of subsequent audits, vendors communicate significant changes to Jack Henry or provide bridge letters Observed the list of service providers and verified that SOC 2 Type II reports or other compliance reports are obtained annually Reviewed the Third-Party Risk Management Policy and verified potential service providers are requested to provide compliance reports before they can be selected for usage and their compliance is monitored at least annually	No Relevant Exceptions Noted
CC9.2.5	Due diligence is required to be performed prior to the engagement of new service providers and vendors.	Interviewed the Audit Support Analyst and verified new vendors are assessed by contacting other companies for references, vendor pricing, industry reputation, and PCI DSS and SOC 2 compliance; during periods between the completion of subsequent audits, vendors communicate significant changes to Jack Henry or provide bridge letters	No Relevant Exceptions Noted

		Observed the list of service providers and verified that SOC 2 Type II reports are obtained as due diligence and annually thereafter Reviewed the Third-Party Risk Management Policy and verified due diligence is required to be performed prior to engaging service providers	
CC9.2.6	Subservice providers are utilized within the organization’s environment to provide critical services for operations.	Interviewed the Scrum Master and verified there are currently two subservice providers: NCR data center service provider and RagingWire colocation data center; a list of approved service providers is maintained Observed the service provider list and verified there are only two subservice providers listed: • NCR – Data Center Service Provider • RagingWire – Data Center Colocation Services Observed NCR’s website and verified NCR provides technology managed services and is consistent with those provided to Jack Henry Ensenta Observed RagingWire’s website and verified RagingWire provides data center colocation services and is consistent with those provided to Jack Henry Ensenta	No Relevant Exceptions Noted

Additional Criteria for Availability

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
A1.1.1	Systems within the organization are monitored for performance impact and utilization.	Interviewed the Systems/Network Administration, Senior Manager and verified systems are monitored for performance impact and utilization through the use of Splunk and are utilized to determine when additional resources are required Observed Splunk dashboards and verified monitoring processes are in place and provide meaningful information to make resource determinations, and the groups are configured to programmatically increase or reduce instances as the load changes	No Relevant Exceptions Noted
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
A1.2.1	Appropriate environmental protections are in place within the organization to protect the facility, server room, and equipment.	Interviewed the Systems/Network Administration, Senior Manager and verified environmental controls have been established to protect the facility, server room, and the equipment Observed the corporate office suite and verified the following environmental controls were established and are managed and maintained by the building management team: • HVAC units have been established to control the humidity and temperature • Fire detection and a dry-pipe sprinkler suppression system are established • Fire extinguishers are in place Observed the corporate server room closet and verified the following environmental controls were	No Relevant Exceptions Noted

		established, and are managed and maintained by the building management team: • HVAC units have been established to control the humidity and temperature • A dedicated HVAC system is established as a backup system to the building's HVAC • Humidity control • Two APC Smart-UPS SRT 5000VA UPS Observed HVAC maintenance records and verified that preventive maintenance is performed on the HVAC annually Observed the fire extinguishers and verified they have been inspected within the audit period *Note: Observations were performed via a virtual onsite using a Webex session.*	
A1.2.2	A business continuity and disaster recovery plan has been established to govern the disruption to or failure of critical business systems and processes.	Interviewed the Compliance Analyst and verified a business continuity and disaster recovery plan has been established to govern the disruption to or failure of critical business systems and processes and disruption of personnel to perform critical operations Reviewed the Business Continuity Plan (April 20, 2020) and verified that the following have been considered: • Department Processing Overview • Contact Names and Phone Numbers • Website Links and Internal Shared Drive Paths • RTO Gaps and Workaround Procedures • Suite Recovery Procedures Reviewed the Ensenta Business Continuity and Disaster Recovery	No Relevant Exceptions Noted

		Program Overview Plan and verified the following is considered: • Disaster Declaration • Department Business Impact Analysis • Business Continuity Plan Testing • Business Impact Analysis – Application • IT Disaster Recovery Plan • Risk Assessment • IT Disaster Recovery Plan Testing • Client Responsibilities • Recommendations for Clients • Notifications for Clients • Last Update to BC/DR Plans • Last Plan Exercise	
A1.2.3	A business impact analysis (BIA) is performed by the organization to determine recovery time objectives (RTOs), as well as the costs of potential outages.	Interviewed the Compliance Analyst and verified a BIA has been performed to determine RTO and costs of outages Reviewed the BIA (April 14, 2020) and verified financial impact, operation/client impact, compliance/legal/regulatory impact, and reputational impact were considered; Ensenta was assessed with a BC/DR impact rating level of Critical with an RTO of six hours and an RPO of one hour	No Relevant Exceptions Noted
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	Data backup policies and procedures are documented and include requirements for full and partial backups to be performed on a defined frequency and for backups to be tested monthly.	Interviewed the Database Administration, Manager and verified the following: • Full backups are performed weekly and differential backups performed daily • Backups are retained for up two weeks • The database performs backup validation as part of the replication and backups • DBAs are notified if there are any backup related issues • NCR has a NetBackup agent running to pull the backup files weekly from the backup file server for an offsite backup	No Relevant Exceptions Noted

		• All application VMs are backed up weekly Observed SQL DB configurations and verified backups are performed as follows: • Full backups weekly • Differential backups daily • Transaction log backups every 15 minutes Observed DB Job properties and verified differential backups are performed daily and full backups are performed weekly locally Observed the DB Job properties and verified transactional backups are performed every 15 minutes locally Observed the production fileserver and verified that one week of full DB backups, seven days of differential of backups, and six days of transactional logs are retained Observed the DR fileserver Task Scheduler and verified the SFTP server is looking for new transactional log backups in the Production backup server every minute Observed DR fileserver backups and verified 45 days of transactional log backups are retained Observed Veeam backup configurations and verified application servers are backed up on Thursdays at 9 PM, and Veeam performs an integrity check at the end of the backup and alerts IT personnel if there is a failure Observed the Veeam backup system and verified backups are only retained for one week Reviewed the JPS Records and Data Retention Policy (May 2020) and	

		verified database data logs are replicated to a hot-standby database every 15 minutes and full and partial backups are required to be performed on a defined frequency; backups are required to be tested monthly	

Additional Criteria for Processing Integrity

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.		
PI1.1.1	Financial institutions are provided training as part of the onboarding process, as well as documentation on the proper usage of Ensenta's APIs.	Interviewed the Scrum Master and verified FI are provided training as part of the onboarding process and given documentation on the proper usage of Ensenta's APIs Observed processes for onboarding new FI and verified that training and user documentation is provided to each customer depending on the services that are being performed Observed FI are provided documentation for utilizing the APIs	No Relevant Exceptions Noted
PI1.1.2	Internal users within the organization are required to participate in training programs and acknowledge the corporate acceptable use policy.	Interviewed the Scrum Master and verified internal users are provided training as necessary for their job responsibilities and are required to acknowledge Jack Henry's Acceptable Use Policy Observed personnel records and Jack Henry Policy Center records for 3 of 8 personnel hired over the audit period and verified new personnel physically or electronically acknowledged the Jack Henry Acceptable Use Policy	No Relevant Exceptions Noted
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.		
PI1.2.1	The organization implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in services and reporting to meet defined objectives.	Interviewed the Scrum Master and verified different groups utilize different systems to monitor activities to ensure operational quality Observed the Jira system and Kanban boards and verified the system is utilized to manage system change requests and application sprints and is utilized by management to ensure that projects stay on track or to identify if additional resources are needed	No Relevant Exceptions Noted

		Observed the Salesforce dashboards and verified service tickets are monitored by management to ensure that workloads are balanced, issues stay on track, and to identify if additional resources are needed Observed the Ensenta System Status system and verified system status reports are sent to the Operations and Support hourly when there are no issues and every 15 minutes when issues are detected Observed the Event Listener and Splunk monitoring systems and verified systems are utilized to monitor for anomalies Observed Ensenta's Splunk dashboard and verified systems health is monitored and alerts are generated if issues are detected	
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.		
PI1.3.1	The organization implements policies and procedures over system processing to result in services and reporting to meet defined objectives.	Interviewed the Scrum Master and verified different groups utilize different systems to monitor activities to ensure operational quality Observed the Jira system and Kanban boards and verified the system is utilized to manage system change requests and application sprints and is utilized by management to ensure that projects stay on track or to identify if additional resources are needed Observed the Salesforce dashboards and verified service tickets are monitored by management to ensure that workloads are balanced, issues stay on track, and to identify if additional resources are needed Observed the Ensenta System Status system and verified system status reports are sent to the Operations and	No Relevant Exceptions Noted

		Support hourly when there are no issues and every 15 minutes when issues are detected Observed the Event Listener and Splunk monitoring systems and verified systems are utilized to monitor for anomalies Observed Ensenta's Splunk dashboard and verified systems health is monitored and alerts are generated if issues are detected	
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.		
PI1.4.1	The organization implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet defined objectives.	Interviewed the Scrum Master and verified different groups utilize different systems to monitor activities to ensure operational quality Observed the Jira system and Kanban boards and verified the system is utilized to manage system change requests and application sprints and is utilized by management to ensure that projects stay on track or to identify if additional resources are needed Observed the Salesforce dashboards and verified service tickets are monitored by management to ensure that workloads are balanced, issues stay on track, and to identify if additional resources are needed Observed the Ensenta System Status system and verified system status reports are sent to the Operations and Support hourly when there are no issues and every 15 minutes when issues are detected Observed the Event Listener and Splunk monitoring systems and verified systems are utilized to monitor for anomalies	No Relevant Exceptions Noted

		Observed Ensenta’s Splunk dashboard and verified systems health is monitored and alerts are generated if issues are detected	
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity’s objectives.		
PI1.5.1	Specific data within the organization is required to be retained only as long as required for legal, regulatory, and business needs.	Interviewed the Compliance Analyst and verified data retention is based on SOX and NACHA/ACH requirements and timeframes range from a few weeks to seven years Observed the following records are required to be retained by policy: • SOX documentation • Transaction logs • Instant support log • Alert log • Check images • MICR • X9.37 image archive posting files • EZAdmin user validity • Access log • EZAdmin password validity • System antivirus logs Reviewed the Records and Data Retention Policy and verified specified data is required to be retained only as long as required for legal, regulatory, and business needs	No Relevant Exceptions Noted

SECTION V:
OTHER INFORMATION PROVIDED BY JACK HENRY & ASSOCIATES INC. – ENSENTA THAT IS NOT COVERED BY THE SERVICE AUDITOR’S REPORT

MANAGEMENT'S RESPONSE

Note: Information about Jack Henry & Associate Inc. – Ensenta's planned system changes has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve the organization's service commitments and system requirements.

CC6.2.5 – Logical Access
The user account of the terminated associate with access to the development environment posed no risk to JHA as the account was disabled upon termination in the corporate Active Directory (validated by the auditor). Access to the development environment cannot occur without first being authenticated by the corporate Active Directory. Subsequent to the identification of the exception by the auditor, Management reviewed the list of employees with access to the development area to ensure all were current employees.

There is a business unit control around permissions for new, terminated, and/or transferred associates that did not include the specific development environment access. An update was made to the checklist to include that development environment. This control is independently tested internally on a recurring basis.