SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S ASSERTION RELATED TO ITS

Nava Benefits Platform

Relevant to Security, Availability, and Confidentiality

For the period May 15, 2025 to May 15, 2026

TOGETHER WITH INDEPENDENT AUDITORS' REPORT



Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report....1

Scope 1

Service Organization's Responsibilities....1

Service Auditors' Responsibilities....1

Inherent Limitations 2

Opinion 2

2. Assertion of Nava Benefits Management 3

3. Description of Nava Benefits' Platform 4

Company Background 4

Services Provided....4

Principal Service Commitments and System Requirements....4

Components of the System 6

1. Independent Service Auditors' Report

To the Management of Advocate Inc. (Nava Benefits)

Scope

We have examined Nava Benefits' accompanying assertion titled "Assertion of Nava Benefits Management" (assertion) that the controls within Nava Benefits' Platform (system) were effective throughout the period May 15, 2025 to May 15, 2026, to provide reasonable assurance that Nava Benefits' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria.*

Service Organization's Responsibilities

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

Service Auditors' Responsibilities

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

Our examination included:

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

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

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Nava Benefits' Platform were effective throughout the period May 15, 2025 to May 15, 2026, to provide reasonable assurance that Nava Benefits' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Sensiba LLP

San Jose, California
June 29, 2026

NAVA

2. Assertion of Nava Benefits Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Advocate Inc. (Nava Benefits) Platform (system) throughout the period May 15, 2025 to May 15, 2026, to provide reasonable assurance that Nava Benefits' service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Nava Benefits' Platform," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 15, 2025 to May 15, 2026, to provide reasonable assurance that Nava Benefits' service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA*, Trust Services Criteria.*

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

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

We assert that the controls within the system were effective throughout the period May 15, 2025 to May 15, 2026, to provide reasonable assurance that Nava Benefits' service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Advocate Inc. Management

June 29, 2026

3. Description of Nava Benefits' Platform

Company Background

Nava Benefits, founded in 2019, is a tech-enabled insurance Benefits Brokerage that aims to make healthcare more affordable and accessible for all Americans. Its mission is to improve healthcare by offering high-quality, affordable plans to employees and saving money for employers. Built by a team of experts in technology, insurance, and employee benefits, Nava offers healthcare solutions, year-round employee advocacy, and ongoing measurement to monitor and recommend healthcare plans, thus enabling clients to provide the required benefits to their employees while lowering overall plan cost. It offers innovative Renewal and Funding strategies to People teams and a fantastic benefits experience to its Members through the AI- powered Nava Benefits Mobile Application.

Nava Benefits has been name done of Inc. Magazine's Power Partners within the Benefits Brokerage services category, as well as to Inc. magazine's annual Best Workplaces list. Nava was founded by experienced entrepreneurs and is based in New York City, but its team is spread across the United States.

Services Provided

Nava Benefits, founded 2019, provides insurance Benefits Brokerage services throughout the United States to mid-size companies.
Nava Benefits services include:

- sales and servicing clients in the purchase or and automating renewing health benefits
- supports benefits administration back-office tasks to streamline benefits administration for clients
- modern member support to employees and beneficiaries, with AI- and people-powered support and benefit enrollment assistance

Principal Service Commitments and System Requirements

Nava designs its processes and procedures related to Benefits Brokerage to meet its objectives for its sales, onboarding, enrollment, eligibility, client services and member support services. Those objectives are based on the service commitments that Nava makes to clients, the laws and regulations that govern the provision of benefits brokerage services, and the financial, operational, and compliance requirements that Nava has established for the services, as well as state privacy security laws and regulations in the jurisdictions in which Nava operates.

Security commitments to clients are documented and communicated in Service Level Agreements (SLAs) and other customer/ vendor agreements, as well as in the description of the service offering provided in Nava's website. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Benefits Brokerage Applications that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit is implemented. The encryption technologies and methods utilized are defined in the encryption policies and procedures. Critical data including personal information and passwords is required to be stored in an encrypted format. In addition, where employees utilize mobile devices (i.e., phones, laptops, etc.) to access the in-scope systems, the connection must be established in a secure manner using encryption.
- Nava establishes operational requirements that support the achievement of security commitments, service levels, relevant laws and regulations, and other system requirements. Such requirements are communicated in Nava's system policies and procedures, system design documentation, and contracts and service level agreements with customers, vendors and third parties. Changes to commitments, requirements, and responsibilities are communicated to external parties, including impacted customers and vendors.
- Nava maintains robust processes to ensure that all relevant team members are appropriately licensed with regulatory insurance bodies and appointed with the necessary insurance carriers. They undergo rigorous checks to verify credentials and actively monitor licensing requirements to meet state and federal regulations. Additionally, we have structured systems in place to keep our team members current with continuing education requirements, ensuring they stay informed about industry developments and best practices. These measures reinforce our commitment to delivering expert guidance and exceptional service to our clients.
- Organizational and information security policies are formally documented to support the functioning of internal controls and processes and define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Benefits Brokerage services. Nava ensures that the company's organizational and information security policies and procedures are made available to its personnel.

NAVA

Components of the System

Infrastructure

Primary Infrastructure		
Hardware	Type	Purpose
Servers	AWS EC2, ECS (Fargate)	Hosts applications and databases
AWS RDS	AWS RDS	Database server
Firewall	AWS Web Application Firewall	Used to segment client networks from the WAN and each other
Storage	AWS S3, SFTP	Storage of application data
Cache	AWS ElastiCache (Redis)	Redis cache for database
Google Workspace	Identity Provider	Primary email; productivity software; google drives; Identity provider for Nava's employees' logins to Admin Tool
Microsoft 365	Cloud-based application	Auxiliary email; productivity software

Software

Primary Software		
Software	Operating System	Purpose
Salesforce	Cloud	CRM
OS X	MacOSX	Computers/ Laptops OS
Windows	Windows	Computers/Laptops OS
Google Workspace	Cloud	IDP, Productivity tools like Gmail, Documents, Sheets, etc.
Virtru	Cloud	Secured email and file sharing
Zoom	Cloud	Video conference
Notion	Cloud	Documentation
Admin Tool	Cloud	Nava's custom client servicing application
Parabola	Cloud	Data processing, ETL
Dagster	Cloud	Data Processing orchestration services
Airbyte	Cloud	Orchestrate data processing activities
Amazon Web Services	Cloud	RDS, GuardDuty, CloudWatch, EC2, ECS
Linear	Cloud	Ticketing System
SonarCloud	Cloud	Vulnerability Scanning
GitHub	Cloud	Software Version Control Hosting
Terraform	N/A	Infrastructure As Code

Primary Software		
Software	Operating System	Purpose
NordLayer	Cloud	VPN connection to cloud apps and tools

People

Nava has approximately 150 employees organized in the following functional areas:

Corporate
Executives, senior management, and company administrative support staff, including Sales, Marketing, Business Operations, Finance & Accounting and People (human resources). These personnel use sales and financial tools, including Salesforce, to measure performance at an overall corporate level, and to report metrics both internally and externally to Nava's clients.

Client Services
Personnel that provide consulting services to clients, using the Benefits Brokerage applications. They provide direct day-to-day services to Nava's clients HR professionals, such as benefit plan design, benefit renewal, eligibility verification, reporting and other benefits administration back- office tasks.

Member Support Services

Personnel that support clients' employees and beneficiaries, answering their benefit questions via emails and assisting them in benefit enrollment and helping members to maximize their usage of the Nava Member mobile application.

Engineering
Personnel that provide software development services and support to Nava's Benefits Brokerage systems and applications. Engineering Develops, tests and maintains the custom software for Nava, and deploys custom software to production. This includes the Admin Tool, AI and Data Processing System. The staff includes software developers, data engineers, AI engineers and DevOps engineers. DevOps maintains AWS infrastructure and keeps the various testing and production environments operational.

IT
Functions as a help desk, providing technical assistance to Nava employees. Provides support in productivity software, like email and videoconferencing tools, and security software like end- point anti-malware protection. Monitors internal and external security threats and maintains current anti-malware software. Handles laptop asset management and distribution to Nava employees. Supports People with employee accounts during onboarding and termination.

Data

Data, as defined by Nava, constitutes the following:

- Company data: Nava's clients Company-level data/files
- Census data: Nava's clients Employee-level data/files
- Eligibility reports: benefits-eligible changes that occur in Nava's clients' benefits administration systems
- Systems and Applications Logs: application-level log entries that comprise of information and exceptions; and login and data modifications audit trail

Data classification policies and procedures are formally established to define data classification schemes, who can access what data, how data is secured, how long data should be retained, and how/when it is purged or destroyed. Data must be classified and structured in a consistent manner. As data is no longer required for business purposes, it is appropriately purged or destroyed. Appropriate internal controls have been implemented to protect confidential documents, files, or directories from inappropriate access. In addition, access to confidential and/or customer data is restricted to authorized personnel based on job role and responsibilities.

Management has defined and documented the components of the data critical to supporting the in-scope system including a description of what the critical data is and is used for, the source of the data, and how the data is stored and transmitted.
Operational personnel review data input, processed, and output from the in-scope system for completeness, accuracy, and timeliness. Errors in the processing of critical data are detected, investigated, and resolved in a timely manner.

As data is entered into the in-scope systems, edit checks are in place to help prevent incomplete or incorrect data from being entered in. In addition, the company has documented and maintains data flow diagrams, process flowcharts, narratives and procedures manuals to identify the relevant internal and external information sources of the system as well as how data moves within the environment.

For many Nava's clients, Census data processing is initiated automatically on a periodic basis. For some clients, this is initiated manually by Nava's Client Services personnel using Nava's Benefits Brokerage Applications. Census data files are transported securely through Secure FTP or secure email to the Data Processing System. The Census data are normalized and transformed into an in-house usable format and stored in the company's transactional or warehouse databases. The databases are encrypted at rest. Once the client's Company and Census data is processed and setup, the client's employees are able to view their benefit information or obtain AI-powered customer support with the Nava Mobile Application.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change control, and data communication standards. Logical access includes system settings and configurations, password requirements, access management, authentication, and system and access logging requirements.

All teams are expected to adhere to the Nava policies and procedures that define how services should be delivered. These materials are located on Compliance Automation platform and Nava intranet and can be accessed by any Nava employee.

Physical Security

Nava does not have any physical facilities. Nava uses AWS for Nava's infrastructure and systems. Nava uses cloud-based applications for productivity software.

Logical Access

Nava uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

Privileged access to the in-scope environment is restricted to authorized and appropriate personnel and formally reviewed at least annually. User activity is configured to be logged on to the in-scope systems, and those logs are retained and reviewed as needed.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the Nava network using google Workspace user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of google Workspace.

Passwords must conform to defined password standards and are enforced through google Workspace authentication settings. These settings are part of the configuration standards and force users to change passwords at a defined interval. Employees' laptops are screen locked out after a defined period of inactivity and require reentry of the user ID and password after a period of inactivity.

Employees access Benefits Brokerage systems through the Internet using the SSL functionality of their web-browser. Employees must supply a valid user ID and password to gain access to the Benefits Brokerage systems and cloud resources. Passwords must conform to password configuration requirements configured in google Workspace.

Nava's clients' employees may utilize the Nava Benefits mobile application by signing on with their user id and a one-time passcode sent to their email account or mobile number. Upon hire, employees are assigned to a position in the HR management system. Prior to the employees' start date, the employee will be provisioned with accounts and access privileges to Benefits Brokerage systems according to their job function.

On an annual basis, access rules for each role are reviewed by the respective systems owner, including operational personnel from People, Sales, Client Services & Support, and Engineering. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by management. As part of this process, management reviews access by privileged roles and requests modifications based on this review.

When employees are terminated, People submits the list of terminated employees to IT to suspend or delete employee access. Every quarter, IT will delete the suspended employee access.

Computer Operations – Backups

Nava has established formal data backup policies and procedures outlining the data backup process, including how and when critical data is backed up. Both critical internal as well as customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of backup failure, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup. Data restorations are completed at least annually to test successful data backup recovery.

Computer Operations – Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, document, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents within the in-scope environment. Incidents must be analyzed, classified, prioritized, documented, tracked, investigated, and addressed timely. The status, remediation efforts, resolution of incidents are communicated to affected users.

Nava monitors the capacity utilization and system performance of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. The monitoring tools are configured to send alerts when capacity utilization or system performance dip below the established thresholds. Alerts are investigated and resolved by support personnel.

Processing capacity and system performance is monitored 24x7x365.Nava evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- AWS server utilization
- AWS database storage
- Data processing system utilization and storage

Nava has implemented a patch management process to ensure infrastructure systems are patched in accordance with operating system and application framework updates and patches. Nava system owners review proposed operating system patches to determine whether the patches are applied and are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Nava personnel validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Nava maintains documented change management policies and procedures to guide personnel in documenting and implementing system (e.g., application, infrastructure, network, etc.) changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures. The change control procedures also outline the process to follow for emergency changes.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Leads approve changes prior to migration to the production environment and documents those approvals within the ticketing system. Access to promote changes to the production environment is restricted to authorized personnel requiring such access for their role and responsibilities.

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

Nava has implemented a patch management process to ensure Nava's systems and applications infrastructure are patched in accordance with vendor recommended operating system and framework patches. Nava system and application owners review proposed operating system and framework patches to determine whether the patches are applied. Nava personnel are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Nava personnel validate that all patches have been installed and if applicable that reboots have been completed.

Changes made to in-scope systems are communicated to internal users that are affected by the given change.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Anti-malware endpoint protection software is installed on the in-scope computers, which is configured to run scans and push updates regularly. The firewall systems and antivirus protection are configured according to the anti-malware and firewall policies and procedures.

An intrusion prevention system (IPS) and intrusion detection system (IDS) are in-place to prevent and detect unusual activity. The IPS and IDS systems are configured to send alerts when potential threats or unusual system activity are detected. Alerts are investigated and resolved by support personnel.

Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Networks and customer environments are segmented logically from each other using VLANs to restrict access.

Nava monitors the in-scope systems to identify potential security threats and vulnerabilities and to detect unusual system activity. The monitoring tools are configured to send alerts when potential threats or unusual system activity are detected. Alerts are investigated and resolved by support personnel.

Nava has formally defined policies and procedures in place regarding completing penetration tests and vulnerability scans and addressing and remediating identified vulnerabilities.

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

Vulnerability scanning is performed by a third-party vendor on an annual basis in accordance with Nava's policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Nava. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests are preformed after vulnerabilities are remediated, and on-going scans are performed as needed. Scanning is performed during non-peak windows, according to approved templates and protocols. Scanning tools requiring installation in the Nava system are implemented through the Change Management process. Vulnerabilities identified from the penetration tests and vulnerability scans performed are formally documented, prioritized, addressed and remediated in a timely manner and in accordance with company policies and procedures.
Authorized employees may access the system through the Internet with the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system. User activity is configured to be logged on the in-scope VPN technologies, and those logs are retained and reviewed as needed. Privileged access to the VPN technology is restricted to authorized personnel requiring such access for their role and responsibilities.

Boundaries of the System

The scope of this report includes the Services performed by Nava Benefits. This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls:

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

- **Security**: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.
- **Availability**: Information and systems are available for operation and use to meet the entity's objectives.
- **Confidentiality**: Information designated as confidential is protected to meet the entity's objectives.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Nava's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Nava's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to company tools and data applicable to their role and understand their responsibility for adhering to the policies and procedures contained therein.
- A confidentiality statement agreeing not to disclose proprietary or confidential information to unauthorized parties.
- Background checks are performed for employees as a component of the hiring process.
- Employees, third parties, and customers are informed of how to report unethical behavior in a confidential manner.

Commitment to Competence

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

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

- As part of the hiring process, management evaluates a candidates' competencies, skillsets, and prior experience.
- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.
- Security awareness and job-related training is provided at least annually to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

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

Nava's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Job descriptions are formally documented and communicated to employees, and management reviews the written job descriptions at least annually for accuracy.

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.
- Organizational charts are reviewed for accuracy at least annually by management.

Human Resource Policies and Practices

Nava's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. Nava's human resources policies and practices are related to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to acknowledge acceptance of policies applicable to the employee following new hire orientation on their first day of employment and a confidentiality agreement.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

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

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

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

Nava has established personnel that are responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Nava attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management. Management has established formal risk assessment policies and procedures which states that a formal risk assessment must be completed at least annually and include an identification and review of risks relating to fraud, vendors and third parties, and changes to the environment (i.e., people, processes, technologies).

In addition, Nava performs appropriate due diligence procedures to verify that each vendor and third-parties environment is secure. Where control gaps are identified, Nava works with the vendor to address and remediate.

Integration with Risk Assessment

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

Information and Communications Systems

Information and communication is an integral component of Nava's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Nava, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various regular calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, town hall meetings are held bi-weekly to provide Nava personnel with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Nava personnel via the company's messaging system.

Specific information systems used to support Nava's Benefits Brokerage system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Nava's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.
Management also maintains a formal internal controls program that describes the internal controls implemented, who is responsible for performing each control, the frequency each control operates, the control type, and how the control is executed. In addition, management meets annually to assess the effectiveness and performance of internal controls within the environment. Executive management maintain independence from those that operate the key internal controls within the environment.

On-Going Monitoring

Nava's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications. In addition, Nava has assigned formal responsibility for coordinating and monitoring the compliance and audit activities to ensure the internal controls environment is formally evaluated at least annually.

Management's close involvement in Nava's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure Nava's personnel safeguard clients data through secured handling of systems and data.

Reporting Deficiencies

Nava uses a combination of a Compliance Automation platform and internal tracking tools to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

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

Incidents in the Last 12 Months

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

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Nava Benefits' Platform.

Subservice Organizations

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

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

Security Category	
Criteria	*Controls expected to be in place*
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	

Security Category	
Criteria	*Controls expected to be in place*
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.	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

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

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

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

Complementary User Entity Controls

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to Nava Benefits.
2. User entities are responsible for notifying Nava Benefits of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Nava Benefits services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Nava Benefits services.
6. User entities are responsible for providing Nava Benefits with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Nava Benefits of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.