



---

## SOC 3

REPORT ON MANAGEMENT'S ASSERTION ON THE EFFECTIVENESS OF CONTROLS  
WITHIN THE HOSTING AND CLOUD SERVICES SYSTEM  
RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY, AND PRIVACY  
FOR THE PERIOD OCTOBER 1, 2024 TO SEPTEMBER 30, 2025  
AND INDEPENDENT SERVICE AUDITOR'S REPORT THEREON

## **TABLE OF CONTENTS**

<b>SECTION I:</b>	<b>INDEPENDENT SERVICE AUDITOR'S REPORT</b>	<b>1</b>
<b>SECTION II:</b>	<b>MANAGEMENT ASSERTION OF NAVISITE LLC</b>	<b>3</b>
<b>SECTION III:</b>	<b>DESCRIPTION OF NAVISITE LLC'S HOSTING AND CLOUD SERVICES SYSTEM</b>	<b>4</b>

## SECTION I: INDEPENDENT SERVICE AUDITOR'S REPORT

Navisite LLC  
Andover, Massachusetts

### SCOPE

We have examined Navisite LLC's (Navisite) accompanying assertion titled "Management Assertion of Navisite LLC" that the controls within Navisite's Hosting and Cloud Services System (system) were effective throughout the period October 1, 2024 to September 30, 2025 to provide reasonable assurance that Navisite's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in *TSP 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

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

### SERVICE AUDITOR'S RESPONSIBILITIES

Our responsibility is to express an opinion, based on our examination, on 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.

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

Our examination included the following:

- 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 Navisite's service commitments and system requirements based on the applicable trust services criteria.

- performing procedures to obtain evidence about whether controls within the system were effective to achieve Navisite's service commitments and system requirements based on the applicable trust services criteria.

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

#### **INHERENT LIMITATIONS**

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

#### **OPINION**

In our opinion, management's assertion that the controls within Navisite's Hosting and Cloud Services System were effective throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Navisite's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

*Schneider Downs & Co., Inc.*

Pittsburgh, Pennsylvania  
December 12, 2025



## SECTION II: MANAGEMENT ASSERTION OF NAVISITE LLC

We are responsible for designing, implementing, operating, and maintaining effective controls within Navisite LLC's (Navisite) Hosting and Cloud Services System throughout the period October 1, 2024 to September 30, 2025 to provide reasonable assurance that Navisite's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Point of Focus—2022)* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system (description) is presented in Section III 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 October 1, 2024 to September 30, 2025, to provide reasonable assurance that Navisite's service commitments and system requirements were achieved based on the applicable trust services criteria. Navisite's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III.

Navisite uses subservice organizations to provide hosting and cloud services and backup storage protection. In addition, Navisite's services were designed with the assumption that certain controls would be implemented by user entities. The description does not disclose the actual controls at the subservice organizations and user entities. Certain trust services criteria can be met only if the complementary subservice organization and user entity controls assumed in the design of Navisite's controls are suitably designed and operating effectively, along with the related controls at Navisite. We monitor the effectiveness of controls at the subservice organizations on an annual basis.

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

We assert that the controls within the system were effective throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Navisite's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by:

AF448A0267B34EE...

Aaron Boissonnault  
Chief Information Security Officer & SVP of  
Managed Services

December 12, 2025

Date



## SECTION III: DESCRIPTION OF NAVISITE LLC'S HOSTING AND CLOUD SERVICES SYSTEM

### BACKGROUND

Navisite LLC (Navisite or the Company) is a global cloud managed service provider (MSP). Navisite offers a range of enterprise applications, infrastructure, messaging services, cloud services, and professional services. It deploys applications provided by vendors that include Microsoft, Oracle, and IBM. The Company supports these applications for its customers and manages the infrastructure within which the applications are processed. The Company enables customers to deploy their applications under Software-as-a-Service (SaaS) arrangements and offers enterprise and business application hosting services that are fully managed and protected within a virtual private, public, or hybrid cloud through which Navisite offers a suite of customized IT-as-a-Service solutions.

Navisite provides services for organizations in service and product-oriented sectors, including healthcare, public services, financial services, retail and leisure, equipment rental, service and maintenance, energy, food and beverage, fashion, manufacturing and distribution, and engineering and construction industries.

In January 2024, Navisite was acquired by Accenture. The acquisition helped to bolster and scale Accenture's application and infrastructure managed services capabilities. Accenture performs centralized functions on behalf of Navisite, including onboarding, security awareness training, certain Human Resources (HR) functions, data loss prevention, anti-virus management, vendor management, and certain privacy functions. These centralized controls performed by Accenture are not included within the scope of this report.

Navisite operates a data center in Andover, Massachusetts and utilizes various third-party organizations to operate numerous facilities within the U.S. and overseas. Refer to the [Locations](#) and [Use of Subservice Organizations](#) sections below for additional details regarding the scope of this report and the locations that support the Company's in-scope services.

### LOCATIONS

Navisite's corporate headquarters and service delivery facility are located at:

- 400 Minuteman Road, Andover, MA 01810

In addition, Navisite also maintains other service delivery facilities located at:

- 2425 Cascade Pointe Blvd, Charlotte, NC 28208, United States (Since the acquisition by Accenture, this location is now maintained by Accenture. However, Navisite is still responsible for management of the business process services (BPS) operations that occur at this location.)
- 2805 Lafayette Street Santa Clara, CA 95050, United States
- 2681 Kelvin Ave. Irvine, CA 92614, United States

## USE OF KEY VENDOR ORGANIZATION

Navisite has engaged Salesforce, a cloud-based CRM, as a key vendor to store and manage client-related data. Navisite’s Salesforce instance is hosted on Hyperforce, Salesforce’s hyperscale infrastructure, ensuring security, scalability, and compliance with local data residency requirements. Navisite maintains management oversight regarding user access, data governance, and reporting for Salesforce. Additionally, Navisite management has established service level reporting for Salesforce. On at least a monthly basis, or when outages occur, Navisite management holds periodic meetings with its key vendor to monitor the execution of the controls. Salesforce’s relationship with Navisite is managed through Accenture’s Vendor Management Program.

## USE OF SUBSERVICE ORGANIZATIONS

Navisite utilizes the following subservice organizations for aspects of physical hosting in the following operations centers and facilities. Navisite management has established service level reporting for all subservice providers listed below. On at least a monthly basis, or when outages occur, Navisite management holds periodic meetings with its subservice providers to monitor the execution of the controls.

Facility Manager	Facility Physical Location(s)
Amazon Web Services, Inc. (AWS)	Asia Pacific (Mumbai)- ap-south-1 Asia Pacific (Singapore)- ap-southeast-1 Asia Pacific (Sydney)- ap-southeast-2 Canada (Central)- ca-central-1 EU (Ireland)- eu-west-1 EU (London)- eu-west-2 US East (N. Virginia)- us-east-1 US East (Ohio)- us-east-2 US West (N. California)- us-west-1 US West (Oregon)- us-west-2
Oracle Cloud Infrastructure (OCI)	US Ashburn (us-ashburn-1) US Phoenix (us-phoenix-1) UK Cardiff (uk-cardiff-1) UK London (uk-london-1) EU Amsterdam (eu-amsterdam-1) EU Frankfurt (eu-frankfurt-1)

Facility Manager	Facility Physical Location(s)
Microsoft Azure (Azure)	North Central US – Illinois South Central US – Texas East US - Virginia Central US - Iowa East US 2 - Virginia Australia East - New South Wales Australia Southeast – Victoria West US - California East Asia - Hong Kong UK South – London UK West - Cardiff North Europe - Ireland West Europe - Netherlands Canada Central - Toronto Southeast Asia – Singapore
Google Cloud Platform (GCP)	US-West1 - Oregon US-West2 - Los Angeles US-West3 - Salt Lake City US-West4 - Las Vegas US-Central1 - Iowa US-East1 - South Carolina US-East4 - N. Virginia US-East5 - Columbus US-South1 – Dallas Asia East1 - Taiwan
TierPoint	Nashville, TN (Eddy Lane)
Digital Realty Trust (DRT)	Santa Clara, CA Woking, UK
Galaxy Data Centers	Redhill, UK
Cologix	Toronto, Ontario (Canada) Vancouver, British Columbia (Canada)
Center Square (previously Evoque)	Irvine, CA Ashburn, VA

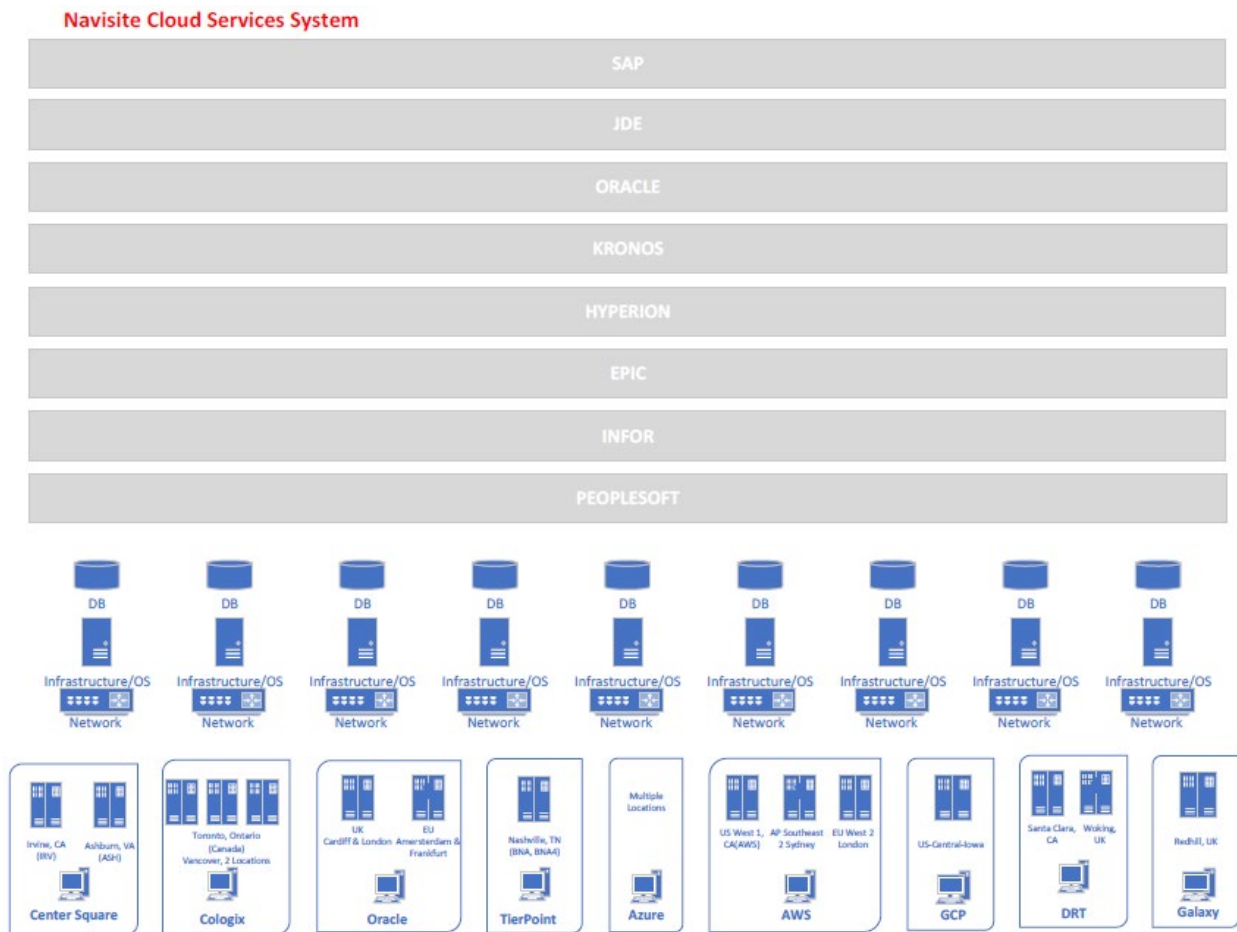
As described above, Navisite delivers cloud services within multiple different environments. These include its own virtual private cloud (VPC) environment, within Oracle Cloud Infrastructure (OCI) and Amazon’s public cloud environment, and within the joint resources of its own VPC and OCI and Amazon’s public cloud to provide a hybrid cloud environment.

Management’s description of its Hosting and Cloud Services System includes only the control activities of Navisite and excludes the control activities of subservice organizations.

Navisite employs several tools to monitor and manage the Service Delivery Infrastructure. Navisite has developed "User Experience Monitoring" and "Batch Token Trending" to provide transparent application awareness for the Hosting and Cloud Services System. A custom-built at-a-glance dashboard is used by the Navisite Operations Center to monitor the overall health of each customer environment. This monitoring allows for quick reaction and proactive identification of issues.

*Boundaries of the System*

The diagram below summarizes the boundaries of the Hosting and Cloud Services System:



**DESCRIPTION OF SERVICES PROVIDED**

Application Infrastructure Services

A secure virtual private, public, or hybrid cloud infrastructure designed to support customer unique application portfolio and infrastructure preferences.

### Application Management Services

Complete application support, including technical and functional application assistance to maximize the productivity of customer software applications, whether they are hosted by Navisite or on customer premises.

### Application Lifecycle Services

Fully managed, integrated application services delivered in the Navisite VPC, public cloud, or hybrid cloud environment. This includes integrated infrastructure, upgrades, and application management services to ensure customer applications readily adapt as an organization's business changes.

### Database Administration Services

Navisite provides a full suite of remote database administration (DBA) services for SQL Server, Oracle, MySQL, PostgreSQL, MongoDB, and DB2, running on all major operating system (OS) platforms including Windows, UNIX, Linux, VMS, and z/OS. Navisite's clients are not buying the services of a single database administrator; they're buying the collective knowledge of an entire staff of expert professionals. This solution allows clients to leverage the expertise of dozens of technicians at a cost less than traditional in-house consultants or full-time employees. All remote DBA services are provided on demand from Navisite's service delivery operations centers across locations.

### Oracle Applications Administration Services

Navisite's Oracle E-Business Suite (EBS) experts manage hundreds of environments daily and have extensive EBS infrastructure, functional and development experience. While paying strict adherence to technical, functional and industry best practices, Navisite's experts assist each customer in tailoring EBS to meet their processing requirements and implement best practices, so customers get the most out of their EBS product investments. Navisite's EBS team routinely performs conversions, migrations, upgrades, family packs and patches, along with custom PL/SQL interfaces, forms, and reports development. With Navisite's Oracle EBS Functional Support, customers don't have to worry about projects being completed late and over budget.

### Windows and Unix/Linux Operating System Administration Services

Navisite's operating system services are designed to ensure customers' server environments are cost-effective, highly available and exceed performance expectations. From initial system design to maintenance, tuning, and monitoring, Navisite provides a full suite of operating system solutions. The Company has extensive experience providing remote operating system support for Windows and all major variants of UNIX and Linux. Navisite assumes total ownership of the security, performance, availability, and improvement of customers' OS environments. The Company's operating system teams have expertise in system design, space management, disaster recovery analysis, security administration, migrations, upgrades/patches, tuning and performance. From initial design to maintenance, tuning, and monitoring, Navisite customizes an OS support solution to meet each customer's needs.

## Monitoring and Problem Resolution Services

Navisite provides 24-hours-a-day, seven-days-a-week, 365-days-a-year monitoring to hundreds of customers. The Company's Navisite Operations Center (NOC) monitoring offering allows Navisite technicians to monitor every component of the application architecture, including middle-tier servers and network devices. Navisite's monitoring experts are able to quickly deploy a customized monitoring solution that meets each customer's unique monitoring requirements. A full-featured monitoring portal allows customers to "see what Navisite sees."

Navisite's team of dedicated personnel are responsible for creating, implementing, and enhancing a strategic blueprint for the proactive monitoring and troubleshooting required to prevent database problems before they occur.

Since the proactive support blueprint is already in place, companies employing Navisite to support their databases don't have to spend the additional money required to create a proactive support environment. Navisite's Level 2 NOC teams consist of professionals who are trained in databases, infrastructure administration, monitoring, problem prevention, and quick problem resolution. The team is also responsible for improving and enhancing Navisite's proactive monitoring capabilities.

Since systems are far too complex to train personnel in all products' maintenance utilities, as well as the monitoring and troubleshooting activities required to provide high-quality support, Navisite's Level 2 Database Support and NOC team is organized by database and OS product support. This separation of support responsibilities allows Navisite to provide platform-specific training to monitoring personnel. During customer integration, Navisite is able to create customized resolution processes based on server, database, job, time of day, and return code generated.

## SQL Server Business Intelligence Services

Navisite's Microsoft Business Intelligence (BI) solutions help customers gain insight by transforming raw, underutilized data into valuable business information. Business intelligence provides the critical insight needed to foster better business decisions, uncover new revenue opportunities and improve cost management. Navisite's Microsoft BI solutions help customers empower their decision makers to visualize the information they need to analyze past performance, optimize current operations and predict future business trends. Navisite's dedicated BI team provides services for SQL Server Integration Services (SSIS), SQL Server Analysis Services (SSAS), SQL Server Reporting Services (SSRS), and Power BI that cover the entire business intelligence lifecycle, from initial design to mature application support.

Navisite's BI team is able to design and implement BI data stores that range in size from hundreds of gigabytes to terabytes. Navisite BI experts are able to enhance existing architecture, as well as partner with customers to design and implement custom-tailored solutions that meet their unique needs. Navisite's customized, scalable SQL Server Power BI and SSIS/SSAS/SSRS solutions help customers unlock the power of their data to drive differentiation and make better, faster business decisions. From strategic planning to production and beyond, Navisite BI experts are with the customer every step of the way, managing customer solutions, empowering success, and ensuring full maximization of the customers' BI investment.

## Cloud Database-as-a-Service (DBaaS) and Infrastructure-as-a-Service (IaaS) Services

Migrating databases to the cloud does not have to be a challenge. Navisite works with customers to determine if the application's requirements for security, availability, performance and DB features can be achieved using a cloud-based database system. Navisite offers best practices and guiding principles designed to achieve successful cloud implementations.

After migration to the cloud is completed, Navisite is able to provide the same set of administration services for cloud database systems that it does for on-premises implementations. Navisite's cloud database management system (DBMS) support team provide a full suite of DBA services that include object change management, SQL and database tuning, problem analysis and correction, security, backup/recovery, application development support, and advanced feature analysis and implementation.

### Colocation

Navisite provides data center space, power, and connectivity for customers' IT infrastructure environments. Customers are responsible for managing their IT infrastructure environments.

### Managed Hosting

Navisite manages customer infrastructure, including complex and simple hosting services, as well as content delivery services, all of which enable customers to concentrate on their core business and not on their infrastructure.

### Professional Services

Navisite Professional Services help customers with project services to enable a cloud journey or gain value from investments in IT. Professional Services are broken into three main areas:

- Cloud - Helping customers with all aspects of their cloud journey with a strong focus on database and enterprise applications.
- Customer Application Development - Providing project services to design, deploy, and maintain custom developed applications and web applications.
- BI and Data Analytics - Projects to unlock the value of a customer's data, allowing them to make informed, timely business decisions.

Navisite's team of dedicated global experts partner with customers to create a project roadmap and deploy solutions that meet unique business requirements and ensure projects are completed smoothly and effectively, from cloud migrations and custom application development/management to database refactoring and data analytics. With the Company's flexible approach, the customer pays only for services they need, with the ability to scale up services to support changing priorities.

Navisite provides these services to a range of vertical industries through its direct sales force and channel relationships, and offers expertise to industries like manufacturing/distribution, financial services, healthcare, pharmaceuticals, publishing/media industries, and the public sector.

Navisite service offerings are enhanced by its proprietary Collaborative Applicability Management (CAM) platform, which enables the Company to work directly with customers' IT systems and system integrators and other third parties to provide operations of outsourced application and infrastructure, as well as access to information through the platform's user interface.

## **SERVICE DELIVERY ORGANIZATION AND STRATEGY**

### Customer Integration

Navisite dedicates a team of professionals responsible for the customer integration process. The Company assigns a dedicated project manager to each customer who becomes responsible for that organization's integration experience. The integration team is tasked to ensure that all customer transitions into the Navisite support infrastructure are completed as efficiently and quickly as possible.

### System Implementation

Policies and procedures exist that document the process of implementing new customer systems into production. For new customer implementations, the project is initiated and authorized by the customer sales order signature prior to initiating the build. Navisite Engineering personnel perform Quality Assurance (QA) testing for operating system and hardware infrastructure prior to delivering the new system to the customer.

For those customers subscribing to the self-managed cloud service, and for those who've elected to convert to the ManageMe Server Management option to undergo a process to harden the server to be in compliance with Navisite's required standards, the Company issues an acceptance request that's sent to the customer via email for each project implementation.

### Primary and Secondary Administrators

Primary and secondary administrators are responsible for learning everything Navisite needs to know about the customer to provide high-quality support. They are the owners of that account and become responsible for the customer's overall satisfaction with Navisite services.

Primary and secondary administrators know customer contacts on a first-name basis, their backgrounds and what they expect from a service provider. They're also responsible for learning the customer's toolsets, change management strategies and procedures, best practices, and day-to-day support requirements. All information is documented by the primary and secondary support administrators in customer-specific support portal support documents. Primary and secondary administrators are also responsible for educating fellow support professionals about customers' environments.

### Subject Matter Experts

Navisite assigns selected staff members to become subject matter experts in one or more database disciplines, including advanced features, backup and recovery, highly available architectures, SQL tuning and database performance, business intelligence, database monitoring, UNIX/Windows scripting, operating system interaction, and database security. Primary and secondary administrators work with Navisite's subject matter experts to ensure each customer benefits from the expertise for problem solving and complex feature implementations.

## Level 2 Database Support and NOC Monitoring Specialists

Navisite's Level 2 Database Support and NOC are staffed by personnel whose sole focus is to monitor customers' environments and take proactive action to mitigate and/or prevent problems to ensure the highest availability and performance possible. Navisite's Level 2 Database Support and NOC specialists differ from traditional help desk technicians who record information then escalate the problem to more senior personnel. Level 2 Database Support and NOC are staffed around-the-clock with dedicated professionals trained in database and OS administration, monitoring, problem prevention and quick problem resolution.

Level 2 Database Support and NOC specialists are also responsible for continuously enhancing Navisite's monitoring infrastructure to improve effectiveness and performance. Level 2 Database Support and NOC teams start each shift with a review of all incidents (alerts and warnings). Representatives from the Level 2 Database Support and NOC teams meet with product teams to provide expert advice when necessary. Morning meetings are held to discuss notification status. The meetings' goals are incident notification analysis and reduction.

## Customer Success Managers (CSM)

Navisite has a dedicated unit that focuses solely on customer relationship management. CSM team members act as agents on behalf of the customer and have immediate access to Navisite support and management personnel. The customer's assigned CSM creates agendas and schedules recurring service quality review meetings according to each client's preference. Meetings focus on Navisite's current performance, adherence to service level agreements (SLAs) and future service delivery modifications. The Company remains flexible to meet customers' evolving support needs. Business and technical needs change frequently, and Navisite's CSM team ensures services continue to meet support requirements.

## *Principal Service Commitments and System Requirements*

Security, availability, confidentiality, and privacy commitments to user entities are documented and communicated in contracts and customer agreements. Security, availability, confidentiality, and privacy commitments include, but are not limited to, the following:

- Security, availability, confidentiality, and privacy principles within the fundamental design of the Hosting and Cloud Services System that are designed to permit system users least privileged access based on job responsibilities
- Use of encryption technologies to protect customer data both at rest and in transit
- Annual training and recertifications of skills development
- Monitoring controls in place to provide oversight of controls and processes within the operation of the Hosting and Cloud Services System, including processing capacity, transmission of data, and review of data
- Data disposal policies and procedures for proper processing and secure disposal and destruction for system hardware and confidential data, based on applicable laws and regulations
- Physical access to facilities and protected information assets are restricted to authorized personnel.

To support the security, availability, confidentiality, and privacy commitments to customers, Navisite has implemented an internal control structure designed to achieve its objectives related to the effectiveness and efficiency of operations, and reliability of information reporting. This system of internal control works to support the achievement of Navisite's strategies and related business objectives and is organized into the following categories: control environment, risk assessment, information and communication, monitoring, and control activities.

In order to meet these commitments, Navisite has identified certain system requirements related to security, availability, confidentiality, and privacy. Such requirements are communicated in Navisite's system policies and procedures and system design documentation. These requirements are made available to internal and external users of the system as applicable in order to fulfill their responsibilities as it relates to Navisite's service commitments. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, organization and information governance, how the system is operated, and how the internal business systems and networks are managed. 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 Hosting and Cloud Services System. These include entity level controls, logical and physical access controls, system operations controls, risk monitoring and management, change management controls, incident and request management controls, processing capacity controls, and data transmission controls as described in the following sections.

### *System Components*

Over the last two decades, Navisite has continuously improved its service delivery support architecture, processes, procedures and organizational infrastructure.

Navisite's standard offering provides 15-minute response time to critical issues that affect the availability of all systems monitored by its monitoring software and supported by its Level 2 Database Support personnel. Advanced telephony, smartphone applications and personal computer software and server implementations ensure Navisite support experts are always there when needed.

Navisite's support professionals utilize industry-leading administrative tools, repeatable process libraries, documentation portals, time entry and Information Technology Infrastructure Library (ITIL) compliant incident/work request systems. Dedicated quality control/quality improvement specialists constantly review the Company's support infrastructure to ensure Navisite customers are benefiting from support practices and products available.

### *Infrastructure*

Navisite's service delivery architecture is composed of four main service delivery components:

- Security - Tools, technologies, and processes Navisite utilizes to ensure the safety of its internal systems and customer environments.
- Connectivity - Mechanisms Navisite uses to connect to customer environments to perform administrative activities.
- Monitoring - Architecture Navisite provides 24-hour-a-day, seven-day-a-week, 365-day-a-year monitoring services to its customers.

- Work Request Management - System Navisite uses to receive work requests from customer personnel. Navisite uses ServiceNow as the work request management system to manage all incidents, requests, or any other type of issues.

Data Center personnel can monitor all customer instances on one screen using Navisite's custom-built, technology-agnostic management portal (agent-based/agent-less, Simple Network Management Protocol (SNMP), Management Information Base (MIB), Management Information Base version 2 (MIB2), Hyperic, OpenNMS, et al.).

## Security

Navisite understands that customers have entrusted the Company with sensitive data stores. The Company's highest priority is to safeguard sensitive customer information. Protecting against unauthorized data access is an ongoing process. Navisite is acutely aware that those individuals desiring to exploit data stored in computer systems for personal means are constantly changing and improving their access strategies. The fluid nature of external and internal attacks requires Navisite to continuously analyze, review and enhance its security infrastructure blueprint. The Company considers this its number one priority.

Navisite has a dedicated Governance, Risk, and Compliance (GRC) team responsible for the management of information security, data privacy and service management throughout the organization. The team is responsible for developing, maintaining and enforcing Navisite's information security policies, procedures, and work instructions. The Information Security Policy is reviewed annually by the Chief Information Security Officer (CISO) & Senior Vice President (SVP) of Managed Services. The security and compliance management framework is based on the following standards:

- ISO 9001:2015
- ISO 20000-1:2018
- ISO 27001:2022
- ISO 22301:2019
- ISO 27017:2015
- ISO 27018:2019

Navisite has implemented enterprise-wide risk management in line with ISO 31000:2009. A benefit of implementing risk management is improved reduction, mitigation and/or elimination of business and technical risk. It also helps to acknowledge that identified risks are within the organization's risk criteria and tolerance and further improve the stakeholder's confidence and trust.

## Connectivity

Navisite does not require customers to use a specific connectivity mechanism. Because of its large customer base, the Company has strong expertise in configuring and using a number of different connectivity products. Navisite's infrastructure and support teams work with each customer to tailor connectivity, account privileges and authentication mechanisms that adhere to the client's internal security controls and ensure the Company is able to securely and effectively monitor, administer and secure their environments.

Navisite has created a robust, secure connectivity architecture that utilizes virtual desktops and servers. The virtual environments allow Navisite to tailor a connectivity desktop platform that allows its support team members to quickly and securely connect to all supported systems. The architecture enables Navisite to create customer-specific desktop environments with all connectivity mechanisms, security controls, support information and administrative tools required to support each customer's unique needs.

### Monitoring

Navisite completed an extensive evaluation of various industry-leading monitoring products and has selected to partner with Zabbix to provide a robust monitoring offering to its customers. Zabbix's Server and Application Monitor (SAM) deliver comprehensive application and server monitoring software for alerting, reporting, and management.

SAM provides full visibility into the database application stack and delivers contextual awareness of performance issues across applications, server hardware and storage infrastructure. It provides Navisite monitoring specialists with the ability to quickly identify and troubleshoot application issues that can occur from any of the layers. SAM provides a customer-monitoring portal that allows the customer to "see what Navisite sees."

### *Software*

Navisite utilizes the following software applications to provide services to its customers:

- ServiceNow - Navisite's ITIL-compliant incident and work request management system. (See Work Request Management section above for more information on ServiceNow.)
- Zabbix SAM - Navisite's production monitoring platform. (See Monitoring section above for more information on Navisite's SAM monitoring architecture.)
- Customer Wiki - Navisite maintains a secure customer Wiki that provides all information necessary to provide high-quality customer support. The Wiki contains customer contact, notification and escalation information.
- Connectivity Software - Because Navisite does not dictate to its customers the type of connectivity mechanism it uses to gain access to their environments, the Company uses a wide range of solutions. Navisite's Administration team works with each customer to define and agree upon the mechanisms and baseline security standards for outside connectivity that Navisite will be required to adhere to.
- Secret Server/Enterprise Random Password Manager (ERPM) Secure Password Vault - To protect sensitive information, Navisite uses Secret Server, which allows Company security personnel to control access to critical accounts and passwords in one centralized, encrypted repository. The software provides users with secure access to passwords and other privileged information.
- Windows Security Update Server - Microsoft's automated patching server ensures that all Windows operating systems and Microsoft applications receive the latest security updates.

- Sophos Virus Scan - Navisite has created a comprehensive virus management solution using Sophos virus protection software to prevent virus infections and automate the virus definition update process. These tools scan servers for viruses, and infected files are automatically quarantined unless the system cannot be automatically cleaned. Navisite maintains current virus signature updates to ensure networks and systems are protected from newly developed threats. The Company's antivirus software is configured to receive automatic updates, perform periodic scans and log antivirus events. All events are routed to a central logging solution.
- ELK Log Aggregation Software - Logging enables Navisite to track user access to all systems, as well as the actions they perform. Logging is enabled on all systems where feasible, which includes databases, servers, users' desktops, applications, networking equipment, and wireless access points, etc.

Navisite accommodates organizations that need to adhere to FIPS compliance by using FIPS 140-2 compliant algorithms.

- Secured Password Vault - Navisite uses Delinea Secret Server and the ERPM (Enterprise Random Password Management) tool for password management of all Company-managed servers and their respective user accounts. Account passwords get rotated at every checkout/check-in operation performed in ERPM.
- Sophos XDR and MTR - Navisite utilizes Sophos Extended Detection and Response (XDR) coupled with Managed Threat Response (MTR) to provide robust endpoint protection, detection, and response capabilities, including ransomware protection, antivirus, anti-malware, antispam, website filtering, email protection, application control, and removable media restrictions.

### Technology Summary

<b>Platform</b>	<b>Technology</b>
<b>Network</b>	Cisco, Fortinet, F5, Citrix
<b>Storage</b>	IBM, Dell, Pure, HP, Infini, Netapp, Brocade
<b>Computer Hardware</b>	Cisco UCS, IBM Flex, IBM Power, Dell, HP, Fujitsu
<b>Virtualization</b>	VMware, OVS, KVM, Hyper-V
<b>OS</b>	Windows, Linux, AIX, IBM, CentOS, Solaris, HP-UX, Ubuntu
<b>Backups</b>	Bacula, NetBackup, Symantec, Commvault
<b>Disaster Recovery</b>	Zerto, Mimix, Double Take, Veeam
<b>Monitoring</b>	Zabbix, Checkmk
<b>Security</b>	Alert Logic, Qualys, Sophos

### *People*

Personnel supporting Navisite's remote administrative services, systems and solutions include, but are not limited to, the following:

Executive Management and the Apex Committee - Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.

- Navisite's Executive Management consists of the following:

- Business Unit Chief Executive Officer (CEO)
- CISO & SVP of Managed Services
- Chief Growth Officer
- Senior Corporate Counsel
- SVP, Managing Director, India
- SVP of Customer Success
- SVP, Strategic Accounts
- SVP, Transformation & Methodology
- SVP, Global Infrastructure Services
- SVP, Professional Services
- SVP, Delivery and Operations
- Managing Director, Europe, the Middle East and Africa (EMEA)

### *Processes and Procedures*

Navisite has operational and security procedures in place to ensure its security, availability, confidentiality, and privacy commitments can be met.

Navisite's Apex Committee is committed to maintaining a formal Information Security and Compliance Program consisting of the policies, procedures and controls that govern the security of Navisite's IT infrastructure. The Information Security and Compliance Program is based on industry best practices (ISO/IEC 27002) and is designed to protect Navisite's internal systems and client environments.

### *Data and Data Classification*

All data stored on Navisite's computing resources must be assigned a classification level by the information owner or creator. This level is used to determine which users are permitted to access the data. Navisite uses the following categories to classify data:

- **Restricted: Confidential** - Highly sensitive data. Information protected by statutes, regulations, policies or contractual language, and/or any data identified by Government regulation to be treated as confidential.
- **Confidential: Proprietary** - Information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a civil statute requiring this protection.
- **Internal Use** - Information that is not deemed critical or confidential but has not been approved for general circulation outside of Navisite. Internal Use Only data is information that is restricted to members of Navisite who have a legitimate purpose for accessing such data.
- **Public Data** - Information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage.

## Integrity and Ethical Values

The Navisite and Accenture executive teams stress the importance of integrity and ethical values. The management team reinforces those values by ensuring that a high level of commitment to excellence is the standard for all employees. Through staff meetings, training sessions, and on-the-job coaching, management constantly monitors and evaluates employee actions, decisions, and the general performance of assigned duties to maintain its commitment to integrity and ethical behavior.

## Organization Structure

Navisite has an organizational structure within which operations are planned, executed, monitored, and controlled. Navisite has defined key areas of responsibility and established appropriate lines of reporting, which are significant aspects of the organizational structure. The organizational structure allows for the segregation of responsibilities among employees. Navisite Global Services represents a combination of team members, processes, and technologies used to deliver consistent and high-quality customer experience across all locations in which Navisite operates.

The entire organization follows a philosophy of customer intimacy as a means of achieving high levels of customer satisfaction. The delivery side of the organization works closely with the Sales team to ensure that customer requirements are understood and fulfilled from the outset of the relationship.

From a functional standpoint, the organizational structure permits interaction, where appropriate, while eliminating potential conflicts of interest through proper segregation of duties and facilitating appropriate checks and balances for strong internal controls.



**SCHNEIDER DOWNS**

Big Thinking. Personal Focus.

[www.schneiderdowns.com](http://www.schneiderdowns.com)