A-LIGN

A-LIGN.com

# Type 2 SOC 3

Prepared for:
Nuvolo Technologies Corporation

Date:
2025

nuvolo

# SOC 3 FOR SERVICE ORGANIZATIONS REPORT

## June 1, 2024 to May 31, 2025

## Table of Contents

# SECTION 1

# ASSERTION OF NUVOLO TECHNOLOGIES CORPORATION MANAGEMENT

## ASSERTION OF NUVOLO TECHNOLOGIES CORPORATION MANAGEMENT

June 20, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Nuvolo Technologies Corporation's ('Nuvolo' or 'the Company') Software Development of Connected Workplace Product and Components Services System throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Nuvolo's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Nuvolo Technologies Corporation's Description of Its Software Development of Connected Workplace Product and Components Services System throughout the period June 1, 2024 to May 31, 2025" 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 June 1, 2024 to May 31, 2025, to provide reasonable assurance that Nuvolo's service commitments and system requirements were achieved based on the trust services criteria. Nuvolo'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 "Nuvolo Technologies Corporation's Description of Its Software Development of Connected Workplace Product and Components Services System throughout the period June 1, 2024 to May 31, 2025".

Nuvolo uses ServiceNow, Inc. ('ServiceNow' or 'subservice organization') to provide data center hosting, monitoring, backup, and encryption services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nuvolo, to achieve Nuvolo's service commitments and system requirements based on the applicable trust services criteria. The description presents Nuvolo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nuvolo's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Nuvolo's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Nuvolo's controls.

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 June 1, 2024 to May 31, 2025 to provide reasonable assurance that Nuvolo's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Nuvolo's controls operated effectively throughout that period.

Jason Siegrist
VP, Head of Security & Compliance
Nuvolo Technologies Corporation

# SECTION 2

# INDEPENDENT SERVICE AUDITOR'S REPORT

## INDEPENDENT SERVICE AUDITOR'S REPORT

To Nuvolo Technologies Corporation:

*Scope*

We have examined Nuvolo Technologies Corporation's ('Nuvolo' or 'the Company') accompanying assertion titled "Assertion of Nuvolo Technologies Corporation Management" (assertion) that the controls within Nuvolo's Software Development of Connected Workplace Product and Components Services System were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Nuvolo's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Nuvolo uses ServiceNow to provide data center hosting, monitoring, backup, and encryption services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nuvolo, to achieve Nuvolo's service commitments and system requirements based on the applicable trust services criteria. The description presents Nuvolo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nuvolo's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nuvolo, to achieve Nuvolo's service commitments and system requirements based on the applicable trust services criteria. The description presents Nuvolo's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Nuvolo's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

*Service Organization's Responsibilities*

Nuvolo 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 Nuvolo's service commitments and system requirements were achieved. Nuvolo has also provided the accompanying assertion (Nuvolo assertion) about the effectiveness of controls within the system. When preparing its assertion, Nuvolo 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.

Our examination included:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

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

*Independence and Ethical Responsibilities*

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

*Opinion*

In our opinion, management’s assertion that the controls within Nuvolo’s Software Development of Connected Workplace Product and Components Services System were suitably designed and operating effectively throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Nuvolo’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Nuvolo’s controls operated effectively throughout that period.

The SOC logo for Service Organizations on Nuvolo’s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

*Restricted Use*

This report, is intended solely for the information and use of Nuvolo, user entities of Nuvolo’s Software Development of Connected Workplace Product and Components Services during some or all of the period June 1, 2024 to May 31, 2025, business partners of Nuvolo subject to risks arising from interactions with the Software Development of Connected Workplace Product and Components Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
June 20, 2025

# SECTION 3

# NUVOLO TECHNOLOGIES CORPORATION’S DESCRIPTION OF ITS SOFTWARE DEVELOPMENT OF CONNECTED WORKPLACE PRODUCT AND COMPONENTS SERVICES SYSTEM THROUGHOUT THE PERIOD JUNE 1, 2024 TO MAY 31, 2025

## OVERVIEW OF OPERATIONS

### Company Background

Nuvolo was founded in October 2013 as an innovation and subscription software company and began operations in January 2014. The company was founded with the single mission of transforming the enterprise asset management (Connected Workplace) market dominated by legacy technology companies.

To achieve its objectives, Nuvolo pioneered enterprise application development on the ServiceNow Platform (NOW). In 2015, Nuvolo became the first enterprise application globally to be fully certified on the ServiceNow platform. With the certification process complete, the next generation Connected Workplace in the cloud was born. In November 2015, as a recognition of its growth and market leadership, Nuvolo became the flagship portfolio company of ServiceNow Ventures and the first company in ServiceNow history to serve as both a global partner and portfolio company.

In June 2017, Nuvolo announced Series A funding which included the participation of New Enterprise Associates (NEA) and ServiceNow Ventures. Worth noting that NEA is a $16B+ fund and was also the original investor in both Salesforce.com and Workday and they have deep institutional expertise in helping cloud companies grow.

Nuvolo’s technical teams are segmented into Innovation (including product management and Quality Assurance (QA)), Delivery, and Customer Care.

Nuvolo has 320+ full-time employees in the United States, Canada, Europe, and India.

### Description of Services Provided

Nuvolo is a software company providing Software Development of Connected Workplace Product and Components Services, including enterprise asset management (EAM), Integrated Workplace Management System (IWMS) and Operational Technology (OT) Security on a single platform, built natively on ServiceNow. Nuvolo Connected Workplace includes solutions for maintenance, space, real estate, projects, sustainability, dispatch, and OT security. Nuvolo Connected Workplace solutions deliver significant value for healthcare, life sciences, financial services, public sector, retail, and many other enterprise industries. In August of 2021, Nuvolo was named a leader by International Data Corporation (IDC) in their Worldwide Software-as-a-Service (SaaS) Facility Management Applications and Worldwide SaaS computerized maintenance management system (CMMS) Applications. Also, in October 2021, Nuvolo was included in Gartner’s Market Guide for IWMS.

Nuvolo develops, delivers, and maintains its products through a set of services related to software development, service delivery, customer care, and success. These services are comprised of people, processes, and technologies that support the organization's mission to deliver fully Connected Workplace solutions to its customers. Nuvolo products are developed on the NOW platform and hosted within the ServiceNow platform using a subscription-based licensing model.

### Principal Service Commitments and System Requirements

organizational and cultural commitment to updates and constant feedback. A short or immediate resolution is what Nuvolo’s customers want, more than anything, as well as transparency and visibility into status and progress. While more of a qualitative measurement, Nuvolo has an organizational and cultural commitment to ensuring that customers are informed and understand when they should expect an issue to be resolved. Regular, open, transparent, and informed interaction during problem resolution and meeting the service level agreement commitments are core objectives of Nuvolo.

A crucial commitment to the customers is to develop, deliver and maintain Nuvolo solutions securely and protect customer and company information. Nuvolo has established organizational requirements and a Digital Security Program (DSP) that supports the commitment to the customers. The program contains technical and organizational controls in the domain of Information Security and aims to support the organization in achieving objectives and commitments regarding Information Security. The DSP includes security policies, standards, standard operating procedures, and guidelines that operationalize the requirements the company will comply with. The DSP also aims to link to any external regulatory or contractual security and privacy requirements that the organization may be required to comply with.

**Components of the System**

*Infrastructure*

The primary infrastructure used to provide Nuvolo's Software Development of Connected Workplace Product and Components Services System includes the following:

| **Primary Infrastructure** | | |
|---|---|---|
| **Hardware** | **Type** | **Purpose** |
| End-user computing | HP EliteBook 840/850 | Providing Nuvolo staff the capabilities to develop, deliver and maintain products, and communicate within the organization / customers |
| | HP ZBook FireFly 840/850 14" | |
| | Dell Latitude 7450 | |
| | MacBook 13.3"/14" | |
| | iPad mini | |
| Wi-Fi and Virtual Private Network (VPN) Infrastructure | Cisco Meraki | Provides wireless connectivity within Nuvolo offices and secured VPN channel connectivity for remote workers |

*Software*

The primary software used to provide Nuvolo's Software Development of Connected Workplace Product and Components Services System includes the following:

| **Primary Software** | | |
|---|---|---|
| **Software** | **Operating System** | **Purpose** |
| Sophos Central | SaaS + endpoint agents | Endpoint protection, anti-malware solution, web filtering |
| ServiceNow Vens | SaaS | Develop Nuvolo products |
| ServiceNow SMB | | Host Nuvolo SMB offerings |
| ServiceNow NuResolve | | Information Technology Service Management (ITSM) and Governance, Risk, and Compliance (GRC) |
| ServiceNow NuSD | | Customer care and success |
| Okta | | Identity Management, Application access provisioning |

| Primary Software | | |
|---|---|---|
| **Software** | **Operating System** | **Purpose** |
| Microsoft (MS) Endpoint Manager (Intune) | | Windows and Bring Your Own Device (BYOD) Mobile Device Management |
| Jamf Pro | | macOS and iPad Mobile Device Management |
| Area 1 Security | | E-mail Advanced Threat Protection |
| MS Sentinel | | Security Information and Event Management System (SIEM) |
| MS Office 365 | | E-mail, MS Teams, MS Office, SharePoint |
| Zoom Video Conferencing | | Video communication |
| Apollo Salesforce | | Nuvolo sales force management system |
| ADP Workflow | | Nuvolo Payroll and people management |
| Atlassian Jira | | Product Systems Development Life Cycle (SDLC) management |
| Atlassian Confluence | | Product SDLC Documentation |
| Azure DevOps | | Product SDLC process management |
| Atlassian BitBucket | | Nuvolo products code Repository |

*People*

Nuvolo has a staff of approximately 320 employees organized in the following functional areas:

- Executive leadership - Leading and managing the departments involved in Nuvolo software products development, delivery and maintenance, as well as management of staff in various locations
- Innovation - Staff that deals with software engineering and product management. They provide research and development services for Nuvolo products as well as software QA and release management
- Marketing and Sales - Staff engaged in activities related to brand positioning, product marketing and business development
- Legal and Privacy - Staff engaged in activities related to brand positioning, product marketing and business development
- Service Delivery - Staff providing the delivery of Nuvolo products to customers. They provide services in pre-sales, project management in professional delivery services and customer success
- Customer Success - Staff providing support services for Nuvolo products in the 'after-delivery' phase of products. They provide services in maintenance and support of the products with customers
- Information Technology (IT) Services - IT system administration, access management, unified communication, mobile device management:
  - Provide technical assistance to Nuvolo end users
  - Central identity and access management
- IT Security and Compliance - IT security operations, compliance, security monitoring, endpoint protection and security incident response:
  - Internal audit and compliance monitoring
  - Development and maintenance of DSP
  - Vendor risk management

    - Cybersecurity risk management
    - Monitoring of internal and external threats
- People team and Training - Staff dealing with hiring, culture and people development in the organization. They support the various departments by ensuring there’re cohesive professionals working for the organization
- Finance - Staff dealing with financial activities in the organization. Budgeting, financial resource management and financial forecasting are among the core activities provided by the Finance department

*Data*

Data, as defined by Nuvolo, constitutes the following:

- Client or employee personal data
- Employee related data
- Sales and Marketing data
- Networking and Infrastructure data
- Strategic financial data
- Operating financial data
- Product development-related data
- Research and development data
- Customer transaction data

<u>The Nuvolo Digital Security Program</u>

Formal information security documentation is comprised of five main parts:

- A core policy that establishes management’s intent
- Control objective that identifies the conditions that should be met
- Standards that provide quantifiable requirements to be met
- Procedures that establish how tasks will be performed to meet the requirements established in standards, and guidelines are recommended, but not mandatory

DSP Security Policies by domains:

- Asset Management (AST)
- Business Continuity and Disaster Recovery (BCD)
- Capacity and Performance Planning (CAP)
- Change Management (CHG)
- Compliance (CPL)
- Configuration Management (CFG)
- Cryptographic Protections (CRY)
- Cybersecurity Vendor Compliance Program (VCP ISO)
- Cybersecurity Vulnerability and Patch Management Program (VPMP)
- Cybersecurity Incident Response Program (CIRP)
- Data Classification and Handling (DCH)
- Endpoint Security (END)
- Human Resources Security (HRS)
- Identification and Authentication (IAC)
- Incident Response (IRO)
- Information Assurance (IAO)
- Maintenance (MNT)
- Mobile Device Management (MDM)
- Monitoring (MON)
- Network Security (NET)
- Physical and Environmental Security (PES)
- Privacy (PRI)

- Project and Resource Management (PRM)
- Risk Management (RSK)
- Secure Engineering and Architecture (SEA)
- Security and Privacy Governance (GOV)
- Security Awareness and Training (SAT)
- Security Operations (OPS)
- Technology Development and Acquisition (TDA)
- Third-Party Management (TPM)
- Vulnerability and Patch Management (VPM)
- DSP Appendix A: DATA CLASSIFICATION and HANDLING GUIDELINES
- DSP Appendix B: DATA CLASSIFICATION EXAMPLES
- DSP Appendix C: DATA RETENTION PERIODS
- DSP Appendix D: BASELINE SECURITY CATEGORIZATION GUIDELINES
- DSP Appendix E: DIGITAL SECURITY ROLES and RESPONSIBILITIES
- DSP Appendix F: RULES OF BEHAVIOR / USER ACCEPTABLE USE

Teams are expected to adhere to the Nuvolo DSP policies and procedures that define how services should be delivered securely. These are published in the Company's Knowledge space and can be accessed by any Nuvolo team member.

Physical Security

The infrastructure services supporting Nuvolo's Software Development of Connected Workplace Product and Components Services System are operated entirely within the SaaS platforms. Nuvolo relies on the SaaS providers to be responsible for the physical security of the infrastructure. Nuvolo reviews SaaS vendors' compliance reports and certifications annually to ensure that sufficient controls are in place and operating effectively.

ServiceNow hosts the in-scope system and supporting infrastructure. As such, ServiceNow is responsible for the physical security controls for the in-scope system. Refer to the 'Subservice Organizations' section below for controls ServiceNow manages.

Logical Access

Nuvolo is an entirely cloud SaaS-oriented company. Resources, including business applications and information systems, are contracted through SaaS providers.

The company uses Role-Based Access and Zero-trust security architecture and requires users and devices of the system to be identified, authenticated, and authorized prior to the use of any system resources. Resources are protected using native system security and add-on software products that identify and authenticate users and devices and validate access requests against the users' authorized roles in access matrices depending on a job role or position, adhering to the “need-to-know” and” least privilege” principles.

Resources are managed in the asset inventory system, and each asset has assigned an owner. Owners are responsible for approving access to the resource and performing regular reviews of access by role.

Employees and approved vendor or contractor personnel sign in to the Nuvolo business applications using an Okta ID, password using Single Sign-On (SSO) and a second factor of authentication. Users are also required to separately sign in to any systems or applications that do not use or support the Single Sign-On functionality of the Okta IAM solution. Passwords conform to defined password standards and are enforced through parameter settings in the Okta SSO solution. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system(s) and components after a specified number of unsuccessful access attempts, and lock workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees and/or contractors accessing Nuvolo business applications use an additional authentication factor through a mobile app. Business applications and information systems support Secure Sockets Layer (SSL) / Transport Layer Security (TLS) connectivity encryption for web-based and API connections.

Computer Operations - Backups

The data relating to Nuvolo's Connected Workplace Products is backed up entirely within ServiceNow or by the SaaS providers of the other SaaS platforms which the company uses. Nuvolo and its customers rely on ServiceNow to be responsible for the backups of the data. Nuvolo reviews ServiceNow's compliance reports and certifications annually to ensure that sufficient controls are in place and operating effectively.

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, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Change Control

Nuvolo maintains documented SDLC policies and documentation to guide personnel in documenting and implementing application and product code changes. Change control policies include standards defining requirements about changes and how to be documented and tracked. This includes documentation requirements, development practices, QA testing requirements and required approvals.

An ITSM system is utilized to document and track the change requests' lifecycle for changes in the business applications and the implementation of the new changes. Nuvolo product changes are subject to an established and documented SDLC process and procedures, including an agile methodology of collection, review, prioritization, design, development and release of changes triggered by functional enhancements, bugs or defects.

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

Data Communications

Nuvolo functions as an organization capable of operating entirely remotely. However, the company offices provide employees and visitors with wireless network connectivity which is encrypted and secure. The network access is segregated to Guest and Employee wi-fi network access, which allows segregation between non-managed devices connected to the network and the company-managed computing devices provided to employees.

The data communication network is managed through a central management cloud-based platform provided by the network equipment vendor.

Internet connectivity redundancy is ensured through a second communication line provided by an alternative provider for every of the office facilities the company occupies.

Employees have access to a VPN service, which provides a secure communication channel to the cloud-based business applications whenever they travel or are connected to a non-secure network.

**Boundaries of the System**

The scope of this report includes the Nuvolo Software Development of Connected Workplace Product and Components Services System performed at the Wellesley, Massachusetts facility.

This report does not include the data center hosting, monitoring, backup, and encryption services that ServiceNow provides at multiple facilities.

### 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 review period.

### Incidents in the Last 12 Months

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

### Criteria Not Applicable to the System

All Common/Security and Confidentiality criteria were applicable to Nuvolo's Software Development of Connected Workplace Product and Components Services System.

### Subservice Organizations

This report does not include the data center hosting, monitoring, backup, and encryption services ServiceNow provides at multiple facilities.

*Subservice Description of Services*

ServiceNow is a cloud-based workflow automation platform that enables Nuvolo to improve its operational efficiencies by streamlining and automating routine work tasks. ServiceNow provides data center hosting, monitoring, backup, and encryption services at multiple facilities.

*Complementary Subservice Organization Controls*

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

The following subservice organization controls should be implemented by ServiceNow to provide additional assurance that the Trust Services Criteria described within this report are met:

| **Subservice Organization - ServiceNow** | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria / Security | CC2.1 | Data that entered the system, processed by the system, and output from the system is protected from unauthorized access. |
| | CC4.1, CC7.1, CC7.2 | ServiceNow has established procedures and designated teams to monitor site availability and resolve availability incidents. |
| | | ServiceNow monitors resource availability and capacity within the ServiceNow production environment. |
| | | ServiceNow has implemented tools to monitor site availability for ServiceNow services. Alerts are escalated to on-call personnel as necessary. |

| Subservice Organization - ServiceNow | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | CC4.1, CC4.2, CC7.1 | Authenticated and unauthenticated network vulnerability scans are performed on a real-time basis. Vulnerabilities identified are documented within ServiceNow's internal ticketing system. |
| | | Penetration tests are performed from a third-party annually in ServiceNow environment. Vulnerabilities identified are evaluated and documented and remediation plans are implemented as needed. |
| | CC6.6, CC6.7, CC7.1, CC7.2 | ServiceNow has implemented an intrusion detection system (IDS) that protects against unauthorized access to ServiceNow's production tenants. |
| | | Firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Changes to traffic policies are documented and approved. |
| | CC6.8, CC7.1, CC7.2 | ServiceNow deploys file integrity monitoring (FIM) on ServiceNow's production tenants. Alerts are generated and followed up on. |
| | CC6.1 | Logical access control to in scope operating systems and databases is managed by the subservice organizations. |
| | | ServiceNow has established a Logging and Monitoring Policy which includes purpose, scope, processes and procedures around logging and monitoring security events and activities, and a list of auditable events. ServiceNow's Logging and Monitoring Policy is reviewed and approved annually. |
| | | A ServiceNow instance generates detailed log and audit information regarding activities which take place within it. ServiceNow's application logging capabilities include verbose transaction, client, event, e-mail, and system logs. |
| | CC6.4, CC7.2 | Physical access to ServiceNow facilities is restricted to authorized ServiceNow personnel. A list of authorized users is maintained within the facility's badge access system. |
| | | Physical access to ServiceNow facilities is reviewed monthly and users no longer requiring access are removed. |
| | | Physical access to ServiceNow facilities is revoked in a timely manner upon termination of a user. |
| | CC6.6, CC6.7 | The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel. |
| | | Encryption technologies are used for defined points of connectivity. |
| | | Firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Changes to traffic policies are documented and approved. |
| | | Communication between ServiceNow and the client is encrypted using TLS 1.2. Mobile devices can connect through the use of secured, encrypted connections. |

| Subservice Organization - ServiceNow | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | | Data at rest in ServiceNow is encrypted and protected by 256-bit Advanced Encryption Standard (AES). |
| | | Backup copies are maintained in an encrypted format in a backup facility. ServiceNow does full backups weekly and differential backups daily. The incremental backups are retained for 7 days, and full instance backups are retained for 30 days. |

Nuvolo 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, Nuvolo performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing the subservice organization's attestation reports over services provided by the vendor.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

## COMPLEMENTARY USER ENTITY CONTROLS

Nuvolo's 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 of the Trust Services Criteria related to Nuvolo's services to be solely achieved by Nuvolo control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Nuvolo's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services 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 Nuvolo.
2. User entities are responsible for managing logical access to data stored in Nuvolo or ServiceNow provided applications' databases.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Nuvolo products by their personnel.
5. User entities are responsible for immediately notifying Nuvolo (when subscribed for SMB or OEM offering) of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
6. User entities are responsible for notifying Nuvolo of changes made to technical or administrative contact information.
7. User entities are responsible for developing policies and procedures to protect their systems from unauthorized or unintentional use, modification, addition, or deletion.