Whitepaper: Nuvolo Federal Government & IC Application Approval List Framework

Andrew Stribling
AMPSIGHT INC. | 22970 INDIAN CREEK DRIVE SUITE 100, STERLING VA 20166

AMPSIGHT

Contents

Introductions

Ampsight is a cybersecurity consulting company that supports the federal government including the Intelligence Community (IC). Ampsight specializes in Assessment and Authorization (A&A) consultation to ensure robust implementation of security controls and comprehensive risk assessments for Authority to Operate (ATO). Through meticulous analysis and tailored guidance, Ampsight enables clients to fortify the confidentiality, integrity, and availability of their vital information systems and applications. Ampsight's A&A team has collaborated with Nuvolo to evaluate the baseline security requirements for deploying their embedded software application, Connected Workplace, which is deployed into production on the ServiceNow platform. Nuvolo's enhanced software features leverage the ServiceNow platform for federal customers to complete their mission by knowing the risk acceptance decision has been managed throughout the in-scope application's development lifecycle. The multiple risk assessments from ServiceNow and Nuvolo's third-party assessment organizations (3PAO) clearly show that a Minor or Major Change to the ServiceNow ATO is not appropriate. Ampsight would advise our current federal customers already deploying ServiceNow to make their Risk Management/Acceptance decision based on their internal commercial off-the-shelf (COTS) software approval process.

The Federal Government and Intelligence Community consumers of the ServiceNow platform would benefit from a clear roadmap to deploy the Nuvolo application in a timely manner. Ampsight's Whitepaper will clarify the "challenges" of deploying Nuvolo solutions from the ServiceNow Federal Store:

- ServiceNow requires Independent Software Vendors to meet their certification process for being listed in the Federal Store to operate within its FedRamp Moderate or High ATO.
- Nuvolo applications are not stand alone and cannot receive a Software as a Service (SaaS) ATO.
- ServiceNow's approach in their "Terms of Use" does not accept any liability for installing applications they certified on their Federal Store.
- Federal Government and IC Customers have conditions for hardening commercial software in their environment and want confirmation if they need risk assessments through an ATO process or a COTS approval process to be FedRamp compliant.
- While the Request for Proposal is being evaluated, are the right stakeholders aware that the Nuvolo application relies on 87% of ServiceNow's ATO to be in production and the remaining 13% of the controls have their risk assessment through a "Request for Change" starting at the ServiceNow Federal Store?
- Nuvolo has the Body of Evidence (BOE) to answer granular NIST 800-53 Rev. 5 controls that are implemented for meeting ServiceNow's security requirements, and federal customers will use that BOE for a COTS software approval process, not a separate ATO or Minor/Major Change to ServiceNow's ATO.

Nuvolo Technologies Corporation

Nuvolo, the world's leading Connected Workplace Company, partnered with ServiceNow to create the Connected Workplace by expanding the ServiceNow platform into Facilities and Space management. Through the ServiceNow Build Program, Nuvolo has worked closely with ServiceNow as an "Advanced Platform Partner" to deliver Certified Applications meeting all security requirements.[1] The facility management teams' success is measured on their ability to see and act on data in new ways and ensure a consistent customer experience. Many teams are constrained by their legacy Enterprise Asset Management (EAM) and Computerized Maintenance Management Systems (CMMS). They are hard to maintain, offer limited flexibility and mobile capability, and hinder growth and productivity for the enterprise.

The Connected Workplace is all employees, all physical locations, all assets, and all business services – all aspects of enterprise service management for an organization – residing on one platform. ServiceNow provides IT, SecOps, Customer Service, and Human Resources service management to its customers. Nuvolo's Integrated Workplace Management System for facilities management platform extends the ServiceNow infrastructure into other areas of your operations to manage maintenance, assets, projects, capital planning, space, leases, real estate, sustainability, and OT Cyber Security. Nuvolo's facilities management platform helps teams create seamless digital workflows with IT with a single system of record, eliminating the need to continue relying on disparate systems to retrieve the data they need.[2]

Below is a high-level depiction of how Nuvolo is integrated into ServiceNow:

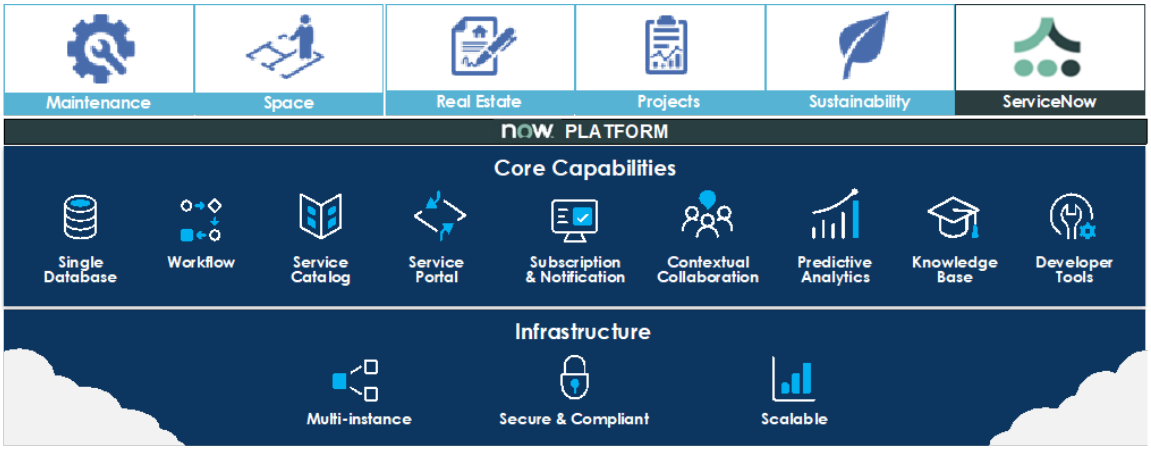

Figure 1 Connected Workplace Technical Architecture Overview

[1] Nuvolo Technologies Corporation (servicenow.com)

[2] Extending the ServiceNow Platform to Facilities and Space Management (nuvolo.com)

Evaluation Results

Ampsight can attest to the additional steps Nuvolo has taken to meet the ServiceNow FedRamp ATO standards as if they were included in the appropriate ATO and proving those security controls are implemented on their own. The NIST 800-145 Definition of Cloud Computing does not define an Independent Software Vendor (ISV) and only mentions it as part of the PaaS Service Model; “acquired applications created using programming languages, libraries, services, and tools supported by the provider. (This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.).” This allows ServiceNow to include what is “supported by the provider” in their ATO and leave ISV “from other sources” to be a shared responsibility of making Nuvolo accept the risk of developing the in-scope application, ServiceNow accept the risk of certifying the in-scope application in the Federal Store, and the Federal customer accepting the risk of installing the in-scope application that maintains ServiceNow’s confidentiality, integrity, and availability information security requirements.

Ampsight wants to empower the Authorizing Official to direct their cyber security team to be prepared for an off-the-shelf software approval task versus an out-of-scope approach to evaluating a minor application change of an ATO based on the 13% of Nuvolo controls applicable for a risk assessment. Nuvolo’s architecture overview clearly leaves the boundary and data unaffected on the ServiceNow platform with the necessary settings customized for FedRamp compliance on each ServiceNow instance. An important BOE artifact from Nuvolo is the ServiceNow Certified Application package that documents ServiceNow’s approval that Nuvolo is not introducing additional risks or vulnerabilities outside of the platform’s boundary as embedded software. The ServiceNow Store TOU effectively points the liability of Nuvolo’s customer support to just Nuvolo and the federal customer, but ServiceNow cannot deny the BOE satisfying the risk management to being a minimal risk.

With the ServiceNow and Nuvolo combined risk management frameworks clarified, Federal customers are able to accept justification that FedRamp standards are being met during the request for proposal phase, and upon contract award, they will only be spending the weeks necessary for a Commercial Off-the-Shelf/Change Management Request type approach to receive an approval for the Nuvolo Connected Workplace to be installed from the ServiceNow Federal Store.

Nuvolo’s Risk Acceptance Challenge

Nuvolo solutions are developed to be secure by design, installed within ServiceNow, and used by ServiceNow users. Nuvolo has been an innovator in the ServiceNow platform regardless of which sector their customers operate in. Nuvolo has updated their products in accordance with

ServiceNow security requirements to be installed wherever ServiceNow is deployed. Nuvolo as an Independent Software Vendor is left in a unique position to be certified meeting all the security measures for the ServiceNow Cloud, Platform, and Application layers, but is not provided an avenue to be ServiceNow certified at the Instance level. Nuvolo faces this software development challenge of meeting ServiceNow's FedRamp ATO requirements to be listed as a certified application in the Federal Store, and they are not directly developing "Nuvolo Federal Solutions." By serving ServiceNow as their first customer, but not being included in the paperwork for the individual agency ATOs, Nuvolo must pick up with each federal customer where ServiceNow leaves them at the Federal Store for installation.

The challenge of developing in-scope applications built to configure ServiceNow platform functions is that Nuvolo:

1. Has to meet the security measures as an organization doing business as a ServiceNow Technology Partner, which will not change the cloud infrastructure.
2. Depends on the ServiceNow Platform security measures for customer data.
3. Has to be a certified application to be listed in the commercial ServiceNow Store.
4. Has to have an additional security review for the Federal Store on FedRamp information systems.
5. The final step is missing, since there is no risk assessment ServiceNow conducts to list authorized applications at a customer's "instance" level.

Other prominent Platform as a Service (PaaS) have taken steps to include "authorized applications" as part of the app store model of deploying approved in-house and third-party vendors that are included in their ATO. One benefit of including all authorized applications is to remove confusing interpretations of "third-party" or "independent" vendor that leave some Authorizing Officials (AOs) questioning all the "Parent Controls" implemented by the platform that the Nuvolo code is embedded in. Next the challenging "Stand Alone Application" question gets asked causing CISOs to ask why is this SaaS not going through an ATO process? The IaaS, PaaS, and SaaS risk assessment questions are all answered in the ServiceNow FedRamp ATO, so for Nuvolo's embedded software, it can only satisfy specific control families of the NIST 800-53: Awareness and Training Incident Response, Personnel Security, System and Services Acquisition, and System and Information Integrity.

The Frequently Asked Questions cycle starts right where ServiceNow left it, and it is a fair place to leave the Risk Acceptance choice at the Instance level. ServiceNow and Nuvolo will never be the Data Controllers, so the choice to do a software approval request at the instance level is appropriate. Per the ServiceNow Store Terms of Use (TOU)[3] in context of the Government Community Cloud for all available applications:

[3] Store_TOU (04232021SNv1).pdf https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0564067 (Internal ServiceNow CORE link)

> **12. U.S. Government Community Cloud ("GCC") and National Security Cloud ("NSC").** The following applies exclusively to the extent that the App will be provisioned to a ServiceNow instance hosted in ServiceNow's GCC or NSC:: you agree and acknowledge that ServiceNow's FedRAMP High, Impact Level 4, and Impact Level 5 ("IL5") Provisional Authorizations to Operate ("P-ATOs") do not apply to the security, privacy or any other attributes of any App. YOU AGREE TO ASSUME ALL RISK AND RESPONSIBILITIES OF SUCH INSTALLATION AND USE OF THE APP IN THE GCC OR NSC INSTANCE AND RELEASE SERVICENOW FROM ALL LIABILITY RELATED TO SUCH INSTALLATION AND USE.

Nuvolo has matured through countless rounds of Frequently Asked Questions to help customer system owners and cybersecurity teams better understand how far ServiceNow will vouch for a certified independent product developed on their ServiceNow platform and where customers must start accepting risk for their own instance level customizations of ServiceNow. The customer is not authorizing Nuvolo as a standalone application affecting the information system boundary with ServiceNow clearly stating it is an individual instance level decision. Nuvolo has completed the FAQ cycle for 35 federal agencies to arrive at the essential question that ServiceNow leaves unanswered: If ServiceNow makes a customer "agree to assume all risk and responsibilities of such installation and use of the App in the GCC or NSC Instance"[4], what risk is left to accept if you trust the ServiceNow Federal Store on your Information System? The TOU focuses on two different paths forward that previously produced a challenge. Do you start from scratch with "All Risks and Responsibilities" creating an extensive list of NA/Inherited controls satisfied by ServiceNow, or do you start with "All Liability" and assess the controls Nuvolo has already satisfied for ServiceNow?

The AO will be asking their internal ServiceNow Administrator, what should I assess to trust Nuvolo as much as ServiceNow trusts Nuvolo to be promoted as a ServiceNow Certified Application? The next step will look similar to a "Request for Change" from a user to request access to a commercial off-the-shelf software that must be analyzed and approved. Nuvolo's body of evidence including product details and applicable compliance documentation from the ISO 27001, SOC Type 2, ServiceNow Design Document Report, and the ALIGN FedRamp Independent Software Vendor (ISV) Report will be researched and verified.

ServiceNow can state that "All Liability" belongs to the customer, but eventually the Federal Store would have to be disabled if ServiceNow kept certifying applications that do not meet their Government Community Cloud FedRamp requirements. When the Nuvolo FAQ cycle ends with a customer assuming "All Liability" to install or not to install Nuvolo from the ServiceNow Federal Store, they end up asking: isn't ServiceNow already assuming "Most of the Liability" for Nuvolo anyways? The answer is yes from an ATO point of view, and your software analyst will review the Nuvolo ISO, SOC, FedRamp, CMMC, and ServiceNow Reports to satisfy the remaining "Request for Change/COTS" security controls. All these FAQs and ServiceNow Certified

[4] Store_TOU (04232021SNv1).pdf
https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0564067 (Internal ServiceNow CORE link)

Application steps clarify the unique relationship ISVs have with ServiceNow, that any application installed from the ServiceNow Federal Store must get the risk acceptance processed as a "Request for Change" individually. Nuvolo will continue to innovate as a ServiceNow Technology Partner developing more certified applications to be installed *individually* from the Federal Store and Nuvolo federal customers should reference this whitepaper when they ask: what did we do last time?

Please review the Control Mapping Diagram for the remaining FedRamp security controls satisfied by Nuvolo as embedded software.

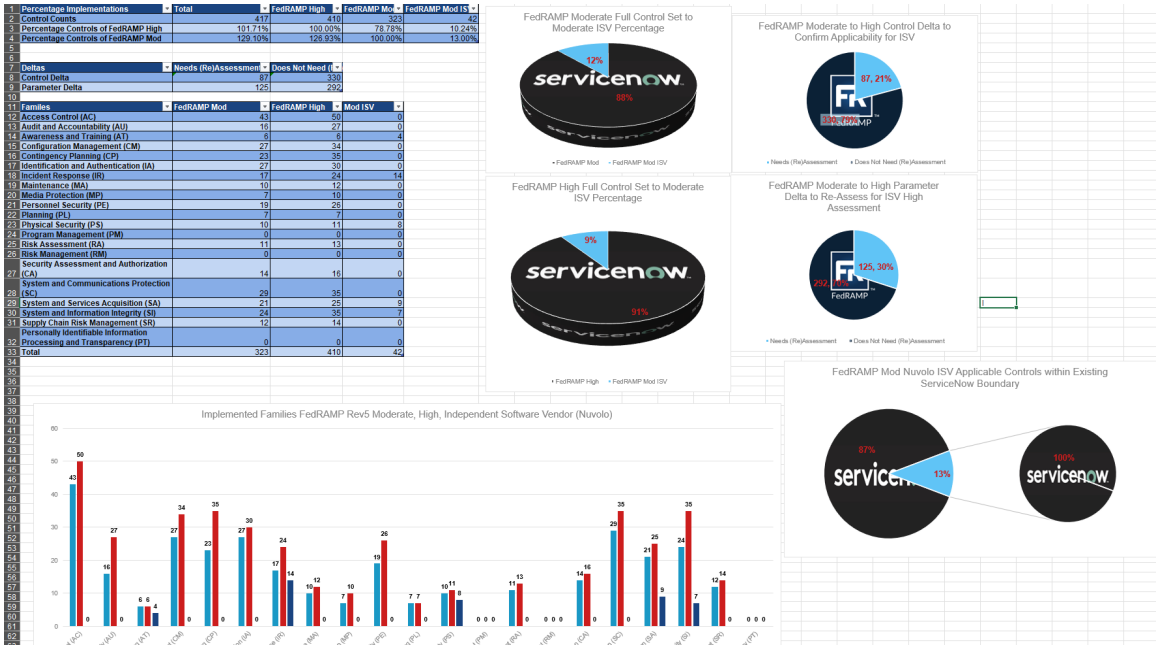

Figure 2 FedRamp_Mod_High_ISV_Delta_Nuvolo_Graphic

Approval Starting Point

The minimal steps required to have the Nuvolo Connected Workplace application enabled to be installed starts with clearly identifying that the security requirements for the ServiceNow platform have already been approved and the boundary/data will not change. The application will not change the Data Controller aspect of the IC customer having the only access to their data. The additional code for the software is the only evaluation left to be done by the agency's ISSOs/engineers. Nuvolo has compiled layers of security requirements at their organizational level while developing the in-scope application to include static and dynamic code scanning at the ServiceNow level. This allows for the Certified Application to be available for installation on the Authorized Platform boundary and pursue multiple assessments against ISO, SOC, CMMC, FedRAMP ISV, which are the appropriate NIST SP 800-53 rev 5 controls for in-scope applications.

After the purchase of the Nuvolo Connected Workplace, the Government Point of Contact/Contracting Officer gives the green light to deploy Nuvolo on the Information System

and begins the following software approval steps, which are different from the initial ATO process that approved the ServiceNow Platform:

- An authorized user submits a “Change Management Request” with a justification that the ServiceNow Platform has the embedded Nuvolo software ready to be enabled and made available to download. The Nuvolo application is required to fulfill their job duties and needs to be approved to install the application. The appropriate screenshots of software version, manufacturer details, release notes, read me files, and compliance BOE are collected and submitted.
- The Configuration Change is received by the respective Program Office/Contracting Officer’s Technical Representative (COTR) for approval. The software approval can then proceed to the security assessment.
- Foreign ownership is established and can be routed to a Foreign Ownership, Controlling, or Influence (FOCI) threat assessment, or if ownership is on an approved list, it can go to the next approval step.
- The appropriate cyber security team and a software analyst will begin the evaluation and verification using their agency specific approval criteria.
- An assessment using Nuvolo’s BOE is completed by the analyst/engineer/ISSO and recommended for Approval to the AO or Designated Authorizer.
- With approval published, the appropriate internal ServiceNow administrator will enable the available Nuvolo software to be visible on the Platform for installation. The Nuvolo products are already part of the ServiceNow Federal Store, but the option is hidden until ServiceNow is contacted to make it available on your instance.
- The implementation team/consultant will assist the system administrator with the custom settings within the ServiceNow Platform to adjust endpoints if tables/libraries need to be hosted internally. The content delivery network (CDN) and dynamic link library (DLL) functions would be customized in the settings before installation is completed.
- The Information System now has an Approved Software assessment that could be used for whitelisting the product with the change advisory board (CAB)/agency.
- Nuvolo Connected Workplace is now deployed with improved functionality for the agency, while the minimal risk has been managed starting where the Platform Authorization hands off the application security layers to the in-scope application’s responsibility.

Nuvolo Software Application Approval Process

Ampsight has researched the correct categorization of the Nuvolo Connected Workplace Application as embedded software on the ServiceNow Platform. The Nuvolo Connected Workplace can only be deployed on an information system through an agency’s instance of the ServiceNow platform, which can be enabled from the ServiceNow Store. Without changing the cloud boundary for ServiceNow, the Nuvolo products would be prepared to be submitted as a change request similar to the Commercial Off-the-Shelf (COTS) process. After the required product information is submitted, the request flows through four to six personnel for approval.

The respective agency software analyst/Information System Security Officer (ISSO) would start their research process with the security control selections that are the software's responsibility, having already acknowledged the inherent security controls established by the ServiceNow Platform.

Each Federal agency will have unique additional software approval criteria, and Nuvolo has continuously proven their commitment to compliance by getting the Nuvolo Connected Workplace application approved at over 30 Federal Agencies based on the thorough secure-by-design documentation and evaluation by those respective Security Operations Centers (SOCs). Once the decision has been made to achieve mission goals utilizing the Nuvolo application, the clarification must be made such that an AO or Chief Information Security Officer (CISO) will be preparing for the software approval process to install the Nuvolo product from the ServiceNow Platform. The containerized certified application downloaded from the ServiceNow Store will not affect the information system boundary allowing for the minimal required documentation to be submitted for the software approval process.

Ampsight has evaluated the relevant software development lifecycle and tailored control selection documentation that isolates the application layer security controls associated with certifying the Nuvolo products[5] This whitepaper will present the justification for the right-sized approach to avoid the confusion of the cloud computing ATO processes with the appropriate Request for Change process for installing in-scope applications on your information system.

IC IT Guiding Principles

As an in-scope application on the ServiceNow platform, Connected Workplace allows the development life cycle to focus on just the application software security principles. As attack surfaces shift focus down from the operating system level to the more granular application surface level, Nuvolo must be transparent in their commitment to trust and compliance. Nuvolo's CISO centrally manages the organization-wide management and implementation of cybersecurity and privacy controls through the related policies, procedures, and plans.

Ampsight's evaluation of the simultaneous approach of layered cybersecurity assessments conducted at Nuvolo has resulted in agreeing with the documentation of the Connected Workplace being secure-by-design equivalent to the FedRamp moderate and high baselines. The clear documentation of the Nuvolo applications being scoped applications designed to meet the ServiceNow security requirements allows clients to know the application and client data completely reside within the ServiceNow platform. The FedRamp Marketplace has ServiceNow approved with JAB Authorization as of August 12, 2019. Across the Federal government,

[5] Software Development Lifecycle (SDLC) POL0020097 Community Search - Community (nuvolo.com) (Internal Nuvolo Community Portal link)

ServiceNow has 80+ Authorizations, and the ATO packages are trusted enough to be used in the Reuse Authorization process 190+ times[6].

As potential clients have questions about at what point the authorized ServiceNow PaaS architecture hands off to the secure Nuvolo application functions, they need to understand that the Nuvolo software layer will not affect the PaaS boundaries or how the data is managed by the client as the Data Controller. Too often an IT department will scope the assessment beyond the application software layer and include the inherited/not applicable FedRamp authorized PaaS controls as the starting foundation. Ampsight advises potential clients to still reference the ServiceNow ATO package through the proper channels and focus the software analyst towards assessing the applicable 60 remaining controls for a "right sized" software application approval for Nuvolo Connected Workplace. Do not let the platform enhancing features for Nuvolo's end-users confuse any scoping decisions to make an assessment go beyond a basic approved product list evaluation by including the already approved platform boundary controls.

Ampsight

Executive Description

Ampsight is a cutting-edge technology company that specializes in providing advanced cybersecurity solutions to businesses looking to enhance the delivery of their products and services into more systems. The company is dedicated to helping organizations leverage the power of data to drive informed business decisions and gain a competitive edge in their respective markets. With its team of seasoned cybersecurity leaders and industry experts, Ampsight has developed a suite of proprietary tools and algorithms that enable businesses to extract valuable insights from their systems and services, identify key trends and patterns, and optimize their risk strategies for maximum impact. With the wide array of industry best practices, constantly revised standards, executive orders, and attainable certifications, Ampsight will demonstrate how one product can achieve multiple levels of risk management with the platform's foundational inherited controls making an authorization decision "right sized."

The remaining application-level controls have been assessed as satisfied and narrow that risk acceptance decision to a much smaller set of controls compared to the unique total functionality of the Nuvolo product. Through Nuvolo's Conformance Roadmap an AO will have clarity that their process to ATO the Nuvolo product will be starting at a "reusing Authorization" step or an Approved Product List step that will enable application software to be deployed off-the-shelf/ServiceNow Federal Store. This Whitepaper on the IC Approval List Framework will educate AO's who are not familiar with Nuvolo Connected Workplace on the implementation best practices to be able to recognize and utilize the secure-by-design lifecycle principles documented in the ServiceNow ATO package, which includes its Certified Applications, that has been authorized many times before. Ampsight recognizes the ServiceNow Platform being

[6] FedRamp Marketplace ServiceNow Platform Government Community Cloud | FedRAMP Marketplace

Authorized over 200 times across the Federal Government on FedRamp Marketplace and those inherited security requirements from the ServiceNow platform, plus the in-scope application security requirements to be listed in the ServiceNow Store, will be leveraged to show quicker authorization and deployment across the Intelligence Community to deliver mission success.

Federal Government & IC Approval List Framework Assessment

Ampsight has assessed Nuvolo's commitment to their trust and compliance strategy utilizing their extensive compliance documentation as a body of evidence. Nuvolo has taken their Risk Management Framework approach from the internal software development life cycle using the ISO 9001 and the ServiceNow Platform's stringent application certification requirements at their FedRamp Moderate and High ATO level. The Nuvolo Connected Workplace product is not capable of being a standalone application and is deployed as an embedded application within the ServiceNow platform. Connected Workplace is only available for installation through the ServiceNow Federal Store and does not affect ServiceNow's configuration enough for ServiceNow to require a Minor Change to their ATO. There is no way for Nuvolo to create its own boundary and be deployed outside of ServiceNow. This clear distinction in the Federal IC allows potential clients to quickly have the application assessed with their version of a change management request. This allows the respective cybersecurity team to right-size their level of effort to do the appropriate "software off-the-shelf risk assessment." As an extension of the ServiceNow Platform Nuvolo's product is already embedded in the ServiceNow ATO satisfying all controls a SaaS platform would have to meet, so the Approval process to install the application is streamlined to a familiar process with a COTS timeline and not a Cloud Service Offering ATO.

The Nuvolo Trust and Compliance group has provided the documentation through their Nuvolo Community portal. Portal access will be available to the federal customers doing the software analysis. Nuvolo's centrally managed Risk Management Program[7] requires annual Risk Assessments, Business Impact Analysis (BIA), Supply Chain Risk Management (SCRM), and Privacy Impact Assessments (PIA). As Nuvolo's Risk Management Program has identified and mitigated risks to the organization and products, they continue to align their security measures with best practices and defend against known vulnerabilities to be approved on more information systems in a shorter amount of time. Again, having reviewed the in-scope application as embedded software contained in the ServiceNow platform there could not be a

[7] Risk Management (RSK) - POL002002 - Risk Management (RSK) - POL0020024 - Community (nuvolo.com) (Internal Nuvolo Community Portal link)

path to an ATO, and the software analyst will easily verify the applicable security controls when it is assessed.

Nuvolo, having been approved at over 30 Federal agencies, has had limited requests for their extensive body of evidence as the agency analysts have been able to complete their processes in a matter of weeks. With the NIST Risk Management Framework (RMF) assessing against the standards from NIST Special Publication 800-53 rev 5, Nuvolo has been securely positioned to complete multiple audits for certifications at once. Nuvolo has achieved and maintains these certifications without any necessary Plan of Action and Milestone (POAM) conditions. Unique security questionnaires with additional criteria are often utilized by each federal agency for their sensitive data requirements that may result in conditions for certain settings having strictly internal connections. Nuvolo's robust approach to mitigating security vulnerabilities allows their documentation to easily crosswalk controls against multiple standards. Nuvolo has dedicated the time and resources to complete reports and certifications for the ISO 9001:2015, ISO 27001, SOC 1 Type 2, SOC 2 Type 2, and the FedRamp ISV Report that can be viewed individually to show the extensive security measures are satisfying multiple standards.

Nuvolo uses the ServiceNow GRC for their own successful risk management framework process that is used by current federal agencies with their ServiceNow platform. This level of detail in their self-assessments facilitates their ability to meet rigorous standards and easily implement their continuous monitoring. Nuvolo has high standards for their Peer Review process by checking code against best practices and standards. Automated tools like SonarCloud provide static and dynamic code vulnerability scanning, and ServiceNow must complete its own vulnerability scanning before listing the application in their Commercial or Federal store. By choosing companies like SonarCloud, that follow the NIST Secure Software Development Framework NIST SP 800-218, Nuvolo proactively meets the FedRamp security standards that they were built on within their ServiceNow partnership versus commercial software with security added at the end of the software development lifecycle (SDLC). As more agencies whitelist Nuvolo products as approved software at their current security standards, Nuvolo will move forward on their Roadmap to Conformance for High Baseline Information Systems that require additional Department of Defense Impact Level, NIST, and National Security Systems (NSS) scope of security controls for those more restricted systems.