Compliance-as-a-Service

Managed Cloud Service Offerings

Rev. 03.20.2025

Managed Cloud Services Offerings	CaaS
Cloud CMMC Compliance-as-a-Service	✓
Endpoint Management, Security Monitoring & Protection	✓
Compliance Assessment Portal	✓
Exchange Online	✓
OneDrive & SharePoint	✓
Security Threat Detection and Remediation	✓
Reports & Alerts	✓

Table of Contents

Description of Services

Cloud CMMC Compliance-as-a-Service

Nimbus Logic has engineered a secure cloud-based service to expedite the process of compliance with CMMC 2.0 L2. This service utilizes the Microsoft cloud stack of technologies and includes all the following:

- Setup & configuration of Microsoft 365 baseline security compliance policies in GCC/H tenant that includes
    - Microsoft Entra Identity Management and Secure Access Policies
    - Implementation of Intune device configuration profiles, compliance policies, app protection & attack surface reduction policies, as part of your device security baseline.
    - Configuring Microsoft Information Protection in your tenant with baseline Sensitivity Labels tailored for CUI
    - Conditional Access & Compliance policies
    - “Customer-Key” encryption, to ensure only your organization holds the encryption keys
    - Setup of Microsoft Sentinel as the SIEM system to log all events within last 90 days and for the analysis of events for incident monitoring
- Onboarding of devices, such as workstations & mobile devices, to Microsoft Intune to enforce baseline security and compliance policies
- Security threat reporting and remediation for any incidents identified in the Microsoft cloud or enrolled endpoints
- Compliance monitoring & automated alert tracking
- Scheduled tasks required by policy, including regular security scans & threat attack simulations
- Gap assessment documentation portal with following features
    - Efficiently perform your NIST SP 800-171 R2 & CMMC 2.0 L2 self-assessment through a guided assessment by answering questions and providing the artifacts necessary
    - Assign assessment items to your colleagues
    - Automated SPRS score generation
    - Automated gap identification & remediation task creation
    - Assist with POA&M generation

- Assist with System Security Plan (SSP) generation
- Includes over a dozen pre-built documentation templates to help meet CMMC maturity and NIST SP 800-171 requirements

Endpoint Management, Security & Protection

All cloud services and onboarded endpoints will have ongoing real-time monitoring for threats & vulnerabilities using Microsoft Defender and Microsoft Sentinel.

The onboarded endpoints, including Windows workstations and any mobile devices, are evaluated in real-time for compliance based on compliance policies established in Intune. If a device falls out of compliance, appropriate notifications are sent to the end-user and a ticket will automatically be logged with the Nimbus Logic help desk for further assistance. After a period of non-compliance, the device will be locked out.

User Management

Microsoft Entra ID will used for all identity and access management. Support will be provided for all functions associated with user account authentication as they relate to Entra ID.

All user additions, changes or deletions will be performed by Nimbus Logic to ensure compliancy procedures are met.

Exchange Online

All aspects of Exchange Online will be supported and maintained by Nimbus Logic. Exchange Online will be configured with a security baseline as defined by our CMMC Compliance-as-a-service documentation.

OneDrive & SharePoint

Support for use as an individual or group-based file share system and includes security setup as it dictated by compliance policy.

Security Threat Detection and Remediation

Nimbus Logic provides real-time managed threat detection and remediation services to uncover and address malicious attacks against all endpoints. In the case that a medium or high-level severity incident alert is detected, a support ticket will be opened with Nimbus Logic support staff automatically and a Nimbus Logic compliance support technician will investigate and remediate.

Reports & Alerts

As part of our Compliance-as-a-Service, all client services and devices are configured in Microsoft Sentinel, which serves as a central SIEM system. All incidents will have email alerts triggered.

Endpoint, Hardware & Networking Support

Help desk support, maintenance and support for existing on-premises hardware and software that is outside the scope of compliance-as-a-service and the services defined above will be billed separately at the prevailing professional services rate set by Nimbus Logic. A client will be provided a statement of work to be signed off on prior to work.

Projects that are considered outside the scope of our compliance service offerings are billed separately and can include, but not limited to:

- Any changes to on-premises hardware or network for compliance purposes
- Firewall and/or router setup and configuration
- System changes expanding beyond what is currently in use in the network
- Evaluation of on-premises systems for compliancy

GAP Analysis Process Overview

1) **Interview and Assessment**
   Nimbus Logic will coordinate a set of conversations with your team based on groupings of the controls and assessment questions that need to be answered. We will provide you a security baseline policy definition document that will outline and define all of the security policies we will be setting up for your cloud & endpoint configurations.

2) **Cloud Configuration & Endpoint Enrollment**
   Nimbus Logic will then begin the setup & configuration of your Microsoft 365 baseline security compliance policies in your GCC High tenant. This will include the onboarding of devices, such as workstations & mobile devices, to Microsoft Endpoint Manager to enforce endpoint security policies.

3) **Written Policy & Documentation Review**
   Nimbus Logic will provide pre-filled policy for each control family and all documentation templates necessary for the NIST 800-171/CMMC self-assessment. You will be required to review or provide additional policy items that are outside the boundary of the Microsoft cloud.

4) **Self-Assessment & SPRS Scoring**
   Once the cloud configuration and policy review is completed, we will begin the self-assessment phase which will ultimately generate your SPRS score. The Nimbus Logic Compliance Accelerator Portal will provide for a guided assessment of each control, where you will be answering questions and providing artifact documents.

   Nimbus Logic will be responsible for all controls and artifacts that relate to your Microsoft Cloud security baseline configuration.

5) **Development of Plan of Action with Milestones (POAM)**
   After a score is calculated, the compliance accelerator tool will provide a list of all tasks that require remediation. This will drive the generation of the POAM document.

6) **Generation of System Security Plan (SSP)**
   You will be provided a template SSP with all Microsoft Cloud systems referenced, including all policies, practices, assessments & plans. You will be required to provide the additional detail for anything outside the cloud boundary.

Service Response Times

Trouble	Priority	Response Time 8am-7pm ET Weekdays
Service not available or significant degradation of service (large number of users or business critical functions affected)	**1**	Remote within 2 hours
Limited degradation of service (limited number of users or functions affected, business process can continue)	**2**	Remote within 8 hours
Small service degradation (business process can continue, one user affected)	**3**	Remote within 24 hours

Compliance Services Requirements

1. Microsoft 365 G5 GCC (Community/High) license required for all users for 100% compliance. A combination of G3 and G5 licenses with the appropriate security and compliance add on can be used depending on the level of security required.

2. Microsoft Sentinel (SIEM) license required

3. PC's (laptops/desktops) with a minimum of Windows 10 Pro and running TPM 2.0.

4. All Servers, Desktop PC's and Notebooks/Laptops with Microsoft Windows operating systems must be running an operating system supported by Microsoft with support expected to continue 12 months or more with the latest service packs and critical updates installed. As Microsoft stops supporting an operating system Client must update their operating system or remove it from any access to the network.

5. Clients will maintain service/support contracts for hardware such as routers, firewalls and switches and specialty software applications.

6. If a client has software particular to its business which is installed on its network, the client is responsible to obtain installation, training and continuing technical support from the software provider. CSP technicians are able to assist with network support but they are not experts in all software applications and rely on the software manufacturer to provide software support at Client's expense.

7. All server and desktop software must be genuine, licensed and vendor-supported.

8. Cloud-based azure backup solution requires internet connectivity at all times.

9. All wireless data traffic in the environment must be securely encrypted.

At the time of initiating service for Client, CSP will evaluate Client's network and determine whether all Compliance Services Requirements are in place and if not in place will install the required services for an additional cost.