



Compliance-as-a- Service

Managed Cloud Service Offerings

Rev. 02.11.2022



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



Table of Contents

Managed Cloud Services Offerings	2
Table of Contents	3
Description of Services	4
GAP Analysis Process Overview	8
Service Response Times	9
Compliance Services Requirements	10

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 the DFARS interim rule, and subsequently CMMC. This service utilizes the Microsoft cloud stack of technologies and includes all the following:

- Initial assessment of client technologies and inventory
- Setup & configuration of Microsoft 365 baseline security compliance policies in your GCC High tenant that includes
 - Azure Active Directory Identity Management and Secure Access Policies
 - Configuring Microsoft Information Protection (MIP) in your tenant and
 - Data Loss Prevention (DLP), Conditional Access & Compliance policies
 - App Protection & Attack Surface Reduction (ASR) policies
 - “Customer-Key” encryption, to ensure only your organization holds the encryption keys
 - SIEM (Azure Sentinel) system setup to log all events within last 90 days and analysis of events for incident monitoring
- Onboarding of devices, such as workstations & mobile devices, to Microsoft Endpoint Manager to enforce endpoint security policies
- Compliance Accelerator documentation portal with following features
 - Efficiently perform your NIST SP 800-171 & 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
 - Automated gap 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

- 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
- Ongoing compliance guidance
- Annual Gap Analysis review & assessment
- NIST 800-171 compliance
- Secure handling of CUI data by authorized personnel

Endpoint Management, Security & Protection

All endpoints and cloud services will have ongoing real-time monitoring for compliance, threat & vulnerabilities for a complete Managed Detection and Response (MDR) solution. Compliance policies for endpoint include, but are not limited to, MFA, OS updates, anti-virus, disk encryption & data loss prevention policies.

Once a device falls out of compliance, CSP will automatically log a ticket and send the appropriate notifications out. After a period of non-compliance, the device will be locked out.

User Management

Azure Active Directory will be used for all identity and access management. Support will be provided for all functions associated with user account authentication as they relate to Azure AD.

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

Cloud Infrastructure

Nimbus Logic will provide support for all cloud infrastructure that is contained within Microsoft Azure for up to 8 hours for each month. Support that exceeds the 4-hour monthly allotment will be billed at the hourly rate of \$175.

In addition to infrastructure support, cloud migration assessments, consults and project plans will be provided at no extra charge. Projects will then be billed at the regular hourly rate of \$175 per hour.

Exchange Online

All aspects of Exchange Online will be supported and maintained by CSP. 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.

Cloud-based Backup

Nimbus Logic utilizes Azure backup for all cloud and on-site servers and workstations. Setup and management is included in the cost of the support, however the licensing and storage are an additional fee.

Backup schedule to be developed in coordination with Client preferences and includes AES-256-bit DOD Level Encryption of all data. Clients must have a 5 megabyte or higher Internet connection (both upload and download).

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.

Reports & Alerts

As part of our Compliance-as-a-Service, all client services and devices are configured in Azure Sentinel, which serves as a central SIEM system. Any and all incidents will have email alerts triggered. Compliancy reports are also built and configured to execute on the desired schedule.

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 reduced hourly rate of \$175.

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

Projects that are beyond the scope of this Agreement will be billed separately at CSP's then hourly rate for service, currently \$175.

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	Response Time Off Hours
Service not available or significant degradation of service (large number of users or business critical functions affected)	1	Remote within 2 hours	Remote within 4 hours
Limited degradation of service (limited number of users or functions affected, business process can continue)	2	Remote within 8 hours	Remote within 8 hours
Small service degradation (business process can continue, one user affected)	3	Remote within 24 hours	Remote within 24 hours

Compliance Services Requirements

1. Microsoft 365 E5 GCC High license required for all users plus an administrative license for 100% compliance
2. Azure Sentinel (SIEM) license required
3. PC's (laptops/desktops) in excess of 5 years in age that fail will need to be replaced by the client with a new machine or one that is less than 5 years in age.
4. All Servers, Desktop PC's and Notebooks/Laptops with Microsoft Windows or Apple operating systems must be running an operating system supported by Microsoft or Apple with support expected to continue 12 months or more with the latest service packs and critical updates installed. As Microsoft or Apple 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. MSP 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.