



Global Data Systems, Inc.

MSPVerify Level 3 – Report

Report on Compliance with the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers® Version 3

Tested through

March 1, 2024, to February 28, 2025

Table of Contents

SECTION 1: INTRODUCTION 2

SECTION 2: REPORT BY MANAGEMENT 5

SECTION 3: INDEPENDENT ACCOUNTANT'S REPORT 7

SECTION 4: DESCRIPTION OF THE CLOUD AND MANAGED SERVICES ENVIRONMENT 10

- Global Data Systems, Inc. Background 11
- Services Offered 11
- Services Verified Under Cyber Verify™ Report 13
- Events Subsequent to the Cyber Verify™ Period of Review 13
- Explanation of the Cyber Verify™ Certification Table 13

SECTION 5: CYBER VERIFY™ CERTIFICATION TABLE 14

- UCS Domain 1 – Expertise: Summary 15
- UCS Domain 2 – Trust: Summary 18
- UCS Domain 3 – Security: Summary 22
- UCS Domain 4 – Resilience: Summary 28
- UCS Domain 5 – Transparency: Summary 32

SECTION 6: UCS REPORT ADDENDUM 35

- SOC 2 Report Addendum 36

COMPANY INFORMATION 39

SECTION 1: INTRODUCTION

From MSPAlliance® Management: Description of the Tested UCS Environment

The Unified Certification Standard (UCS) for Cloud and Managed Service Providers® was developed by the MSPAlliance® as a Managed Service Provider (MSP) cybersecurity framework. The successful demonstration of the MSP internal controls aligned with the UCS extends compliance to all the major cybersecurity frameworks subsequent its inception in 2004.

These domains are then divided into objective categories containing specific requirements. Each requirement is evaluated based on its alignment with GDS's strategic objectives and represents the smallest unit of control. The requirements are assessed using the CORTEX scoring methodology, which assigns a numerical risk score in accordance with the UCS CORTEX scoring system.



During the Cyber Verify™ Certification process, the provider is examined by an independent third-party public accounting firm and must demonstrate it has successfully met the 5 applicable practice domains and underlying controls and requirements. The Cyber Verify™ examination must be renewed annually with gapless coverage to achieve the maximum tier in the CORTEX scoring system.

There are three levels of examination under the Cyber Verify™ framework: Level 1, Level 2, and Level 3.

Level 1 is self-attestation. This means that the service provider has self-attested to meeting the necessary requirements as of the specified date of its attestation.

Level 2 is a "point in time" examination. This means that the service provider met the necessary requirements as of the specified date of its examination.

Level 3 requires a minimum "period of review" of 3 months for first year examinations, while recurring Level 3 examinations typically cover a 12-month period of review. This means the third-party public auditing firm performed sampling and testing to verify that the objectives (and controls) were in place and operating effectively during the period of review.

This Cyber Verify™ report will describe each control objective, its purpose, and how the service provider has satisfied that control objective. While great care and detail went into the examination of the service provider, to protect the security of both the provider and its customers, some details of how the service provider delivers its services, including its security and privacy controls, are discussed here in general terms.

By using cloud computing and managed services from a verified provider, you are not only making a wise decision, but you are also helping to ensure that your service provider is abiding by the best practices and standards of a global community of service providers.

Thank you for helping us make the cloud computing and managed services community a safer place. If you have any questions about this report, you may contact your service provider. You may also request a call with the MSPAlliance® and its examination team if you have specific questions about how the examination was conducted.

Signed,

MSPAlliance® Management,

Las Vegas, Nevada

www.mspalliance.com/UCS

310 Laser Lane, Lafayette, LA 70507
Tel 888.435.7986 - Fax 337.291.9739
getinfo@getgds.com

SECTION 2: REPORT BY MANAGEMENT

310 Laser Lane, Lafayette, LA 70507
Tel 888.435.7986 - Fax 337.291.9739
getinfo@getgds.com

2. Assertion of GDS Management

We confirm, to the best of our knowledge and belief, that Global Data Systems, Inc. (GDS) maintained effective Internal controls over its IT Support and Helpdesk, IT Infrastructure, Network Design and Architecture, Managed Services, Managed Connectivity Services, Voice and Collaboration Services and Security Services referred to as its Managed Service Infrastructure, throughout the Period March 1, 2024, to February 28, 2025. We provide reasonable assurance that Global Data Systems, Inc. has met, in respect to the MSPAlliance® Cyber Verify™ Level 3 Program, based on the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers® Version 3, requirements of the following UCS Practice Domains:

Domain 1: Expertise
Domain 2: Trust
Domain 3: Security
Domain 4: Resilience
Domain 5: Transparency

The MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers® is available at www.mspalliance.com/ucs. The UCS Objective Summaries and Purposes, along with Management's description of its procedures for compliance therewith, are included in the attached Global Data Systems, Inc. Description of the Managed Service Infrastructure.

Signed,

GDS Management

July 21, 2025

SECTION 3: INDEPENDENT ACCOUNTANT'S REPORT

3. Independent Accountant's Report

To the Management of Global Data Systems, Inc. (GDS)

We have examined management of Global Data Systems, Inc. (GDS) assertion that the requirements in respect to the MSPAlliance® Cyber Verify™ Program based on the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers® Version 3 for the period March 1, 2024, to February 28, 2025, is presented in accordance with respect to the Cyber Verify™ Program based on the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers®. Global Data Systems, Inc.'s management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. 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 engagement.

The information included in Objective 10 Corporate Health provided by Global Data Systems, Inc. (GDS) is presented by Global Data Systems, Inc. management to provide additional information on the corporate health of Global Data Systems, Inc. While Corporate Health is part of Global Data Systems, Inc. description of its Cloud and Managed Service Environment and the Cyber Verify™ Certification Table made available to user entities for the period March 1, 2024, to February 28, 2025, the information about Global Data Systems, Inc. Corporate Health has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

The information included in Section 6: Report Addenda provided by Global Data Systems, Inc. is presented by GDS management to provide additional information and is not a part of GDS's description of its Cloud and Managed Service Environment or the Cyber Verify™ Certification Table made available to user entities for the period March 1, 2024, to February 28, 2025. Information about GDS SOC 2 Report Addendum have not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Management asserts that Global Data Systems, Inc. has met the requirements of the Cyber Verify™ Program, based on the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers® Version 3, including the following Domains:

- UCS Domain 1: Expertise
- UCS Domain 2: Trust
- UCS Domain 3: Security
- UCS Domain 4: Resilience
- UCS Domain 5: Transparency

In our opinion, management's assertion that, for the period March 1, 2024, to February 28, 2025, Global Data Systems, Inc. has met the requirements in respect to the MSPAlliance® Cyber Verify™ Level 3 in accordance with the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers® Version 3, is fairly stated, in all material respects.

Sensiba LLP

San Jose, California

July 21, 2025

SECTION 4: DESCRIPTION OF THE CLOUD AND MANAGED SERVICES ENVIRONMENT

Global Data Systems, Inc. Background
Global Data Systems (GDS) is a full-service Managed IT company that, for more than 30 years, has helped people strategically grow their businesses by implementing first-class end-to-end IT services and solutions. GDS provides Managed Secured Connectivity, Voice and Collaboration, Managed IT, Security Services, and Cloud solutions for commercial customers in the Healthcare Services, Oil and Gas, Marine Transportation, and Industrial Construction industries, but it's GDS' passion for Serving People and Making IT Simple that empowers GDS' customers to reach their potential. You have enough to worry about, so GDS simplifies IT so you can focus on your business.

Services Offered
GDS provides an alternative to the traditional "on-premise" IT teams and infrastructures. GDS also provides strategic planning and consulting to optimize Customer technology ecosystems. GDS provides the following:

IT Support and Helpdesk: GDS monitors and manages network and connected devices through its redundant Network Operation Centers (NOC) 24x7x365. The GDS team of solutions-specific engineers provides proactive management and alert resolution while delivering the highest customer satisfaction ratings in the industry. GDS IT support and helpdesk services are available in a model that fits a variety of business needs and budgets through the following:

- 24x7x365 United States (US)-based
- On-Alert Support
- Onsite Support
- Remote Support
- US-based Helpdesk Tiers 1-3

IT Infrastructure: GDS provides turnkey solutions for IT infrastructure needs, from procuring and provisioning hardware and software to managing Customer maintenance and licensing contracts:

- Hardware Procurement
- Software Licensing
- Third-Party Vendor Management

Network Design & Architecture: GDS maintains and improves Customer network design and architecture, develops an IT roadmap, and delivers senior-level IT strategy through the following:

- Office365 Migrations
- Network Refresh
- Remote Site Implementations
- IMAC&D's
- IT Strategy Development

Managed Services: GDS provides a suite of managed services to support IT organizations and business stakeholders. From infrastructure and messaging to critical business applications, GDS works to make it easier to manage IT and deliver the technology that runs Customer businesses.

- Office365 Implementations
- Unified Email Management
- Managed Firewall and Antivirus

- Managed Data Center Infrastructure
- Managed Route/ Switch
- Managed Desktop
- Patches and Updates
- Managed Fax
- Email Spam Filtering

Managed Connectivity Services: GDS provides a suite of managed secured connectivity solutions. Whether it's a corporate office, a branch office, or remote work sites, GDS has a secured connectivity solution to run customers' businesses.

- Managed Secured SD-WAN (NGC)
- Managed Secured Wireless Communications (NOMAD, NOMAD-2-GOM)
- Managed Secured Satellite Communications (NOMAD VOYAGER & NOMAD EXPLORER)
- Managed Mobility

Voice and Collaboration: GDS provides customers with a full suite of voice and collaboration services to provide businesses with the necessary tools to operate their business from anywhere.

- nCONTACT™ Hosted VoIP
- Voice
- Voicemail
- Chat
- Meetings
- Video
- Collaboration
- Cloud Contact Center
- Managed SIP Trunking

Security: With an ever-changing threat vector and cyber criminals gaining sophistication daily the need for Security Services has never been greater. GDS offers a full suite of security services to prevent, detect, and respond to threats in real time.

- Core Infrastructure Assessments
- Penetration Testing
- End-User Security Services
- Email Security Services
- Web Security Services
- Implementation Services
- On-Going Strategic Planning
- Multifactor Authentication
- Server Security
- Firewall Security
- Security Foundation Services
- Security Awareness Training

Services Verified Under Cyber Verify™ Report
This Cyber Verify™ report has been prepared to provide information on GDS's compliance with the MSPAlliance® Unified Certification Standard v.3.0. The scope of this Cyber Verify™ report is on GDS IT Support and Helpdesk, IT Infrastructure, Network Design and Architecture, Managed Services, Managed Connectivity Services, Voice and Collaboration and Security Services, in the context of the Cyber Verify™ report, Customers are defined as entities utilizing these services.

Events Subsequent to the Cyber Verify™ Period of Review
Through its membership in the MSPAlliance®, GDS completed a Systems and Organization Control (SOC 2) Type 2 Report subsequent to December 31, 2024. Included in an appendix to this report, GDS has provided the mapping of the criteria reported on in its SOC 2 report to the UCS objectives and requirements utilized in this report.

External Service Providers Not in Scope of Report
GDS leverages a third party datacenter as a subservice organization provider, leaning on their infrastructure and security measures to ensure data integrity and availability. GDS relies on the encryption controls and physical security measures of their cloud-based applications for data storage. Details about the services provided by these subservice providers can be found in the relevant sections of this report. However, this examination did not include an assessment of the policies and procedures of the subservice providers used by GDS.

Explanation of the Cyber Verify™ Certification Table
In the following Cyber Verify™ Certification Table, GDS has disclosed its assertion of compliance with the Objectives and the underlying Requirements of the MSPAlliance® Unified Certification Standard (UCS) for Cloud and Managed Service Providers® Version 3. GDS's assertion of compliance with the UCS Domains and underlying Requirements is communicated through the use of the following symbols:

-  - Overall compliance with the UCS Objective has been verified,
- ✓ - GDS asserts its compliance with the underlying Requirement,
- ! - GDS asserts its compliance with the underlying Requirement but has not yet demonstrated full compliance with the UCS best practices.
- x - GDS asserts its compliance with the underlying Requirement is not fully met.
- * - GDS asserts its compliance with the underlying Requirement is not applicable to either the services provided by GDS or is not within the scope of the examination.

As part of the Cyber Verify™ process, GDS is improving their controls and the underlying policies and procedures. While complete compliance with all Requirements is the goal of the examination, no system is perfect. Therefore, non-compliance with a minimal number of Requirements does not prevent overall compliance with the UCS Domain. For instances of noncompliance or a non-applicable Requirement, a summary is provided by GDS to communicate its mitigation of the root causes for noncompliance.

SECTION 5: CYBER VERIFY™ CERTIFICATION TABLE



UCS Domain 1 – Expertise: Summary

The Expertise domain emphasizes the Service Providers' proficiency in managing service scopes and tailoring technical solutions to client needs. Effective strategic planning, software management, and risk mitigation are crucial. Procedures for software updates, configuration documentation, change management, secure monitoring, and backup testing ensure high service delivery standards. Internal reviews, management assessments, financial stability, and retention tracking further solidify business continuity and success.

1.02	**Strategic Planning**	✓
1.04	**Software Management**	*
4.01	**Configuration Documentation**	✓
4.04	**Customer Change Tracking**	✓
4.06	**Patch Management**	✓
5.01	**Centralized Operations Center**	✓
5.05	**Operations Monitoring**	✓
6.07	**Continuous Review of Access Rights**	✓
7.03	**Data Recovery Testing**	✓
9.01	**Signed Contracts and Agreements**	✓
10.01	**Operational Sustainability**	✓
10.06	**Customer and Employee Retention Tracking**	✓

Strategic Planning
The Executive Team led by the President is responsible for the company's strategic plans. The CTO is accountable for the engineering, documentation, and development of the plans. The Executive Team meets quarterly at which time the VTO is reviewed, updated if necessary, and approved by the Executive team members. Once archived using the EOS software, prior VTO's are available for review.

Software Management
Not Applicable - GDS does not offer IaaS to customers.

Configuration Documentation
Standard onboarding MOP is used for new managed services Customers. A checklist is followed as detailed in MOP for initial onboard. Then tickets are generated in the PSA to ensure consistent onboarding of assets and initiating service delivery.

The technical and procedural documentation for new Customers is stored within the documentation application. This information is populated by manual entry and via automated synchronization with the RMM. Information regarding Customer contacts and service types are documented within the PSA.

Service requests are funneled via ticketing system/CRM. Client must submit an approval via quote signature. Completion is Managed ticket created in the standard service deployment via playbooks and workflow.

Customer can send in notification of cancellation via service ticket or by notification to account manager. Ticket in the PSA will be used to track removal of services.

Customer Change Tracking
GDS uses a change management process for the request, approval, and processing of changes to customer environments. These changes are tracked in PSA tickets. All Change Management tickets are reviewed by the GDS Change Management Board.

GDS tracks all customer change requests in a Change Management ticket. These changes are tracked in PSA tickets. All Change Management tickets are reviewed by the GDS Change Management Board. Customer notification and approval are documented in these CM tickets. Tickets include a MOP documenting the changes/steps being made.

Patch Management
GDS provides Patch Management for their Customers on servers and workstations. GDS utilizes an RMM for patch management, testing, and logging. GDS has a Patch Management Policy to govern the delivery of these services.

Patches are tested internally prior to being applied. GDS has a test group, pilot group, and production group to organize patches. If a patch fails to apply in the testing phase an alert is automatically created to resolve the issue. If a patch causes an issue in the Customer environments, the Customer will submit a ticket. Tickets will also be automatically generated for devices that are not reporting patch data or are missing patches.

GDS has a standard standing maintenance window for non-mission critical server patches. For mission critical servers GDS coordinates with the Customer(s) and internal resources to perform patches during scheduled maintenance windows. The dates and times for server maintenance windows will vary by Customer and are documented in the RMM. The maintenance windows for workstations are followed by an ad hoc reboot notification that allows the Customer to reboot at the time of their choosing within 30 hours of the patch implementation. GDS has a daily scan of accessible monitored/managed internal and Customer devices.

Centralized Operations Center
The GDS Network Operations Center (NOC) & Service Desk are staffed by employee personnel to monitor, log, and resolve reported/identified problems, incidents, or service requests.

The GDS NOC is staffed 24/7/365 with additional on-call personnel for escalated support. The Service Desk's standard business hours are 7:00 am to 6:00 pm Central time Monday thru Friday (excluding holidays). Service Desk personnel are available on an on-call basis outside of standard business hours. The on-shift NOC employee will contact the appropriate NOC or Service On-Call representative via previously determined appropriate phone numbers.

Operations Monitoring
Reviews are documented via a ticket which is automatically generated weekly. GDS reviews tickets SLAs weekly using reports. NOC/Service Desk Management performs the reviews and requests follow-ups where needed.

Continuous Review of Access Rights
GDS utilizes a recurring PSA ticket that has a set of tasks assigned to GDS Service Desk & NOC Managers and primary engineer to review user listings AND access rights for internal applications, company intranet, data center logical/physical access, and active directory twice per year. The application owners and personnel enter their notes in the ticket, and it is reviewed by the Director of Operations & Infrastructure.

Data Recovery Testing
Backup data restoration and recovery testing procedures are conducted for internal and customer backups on a bi-annual basis using scheduled backup jobs. The initiation and results of the testing procedures are documented in a PSA ticket.

Signed Contracts and Agreements
Service contracts for managed services relationships exist between both GDS and each Customer. These contracts are signed by both parties. GDS also uses a master service agreement in conjunction with its service agreements.

Each Customer signed proposal is countersigned by GDS for managed services. Each Customer acknowledges the MSA as part of the T&Cs referenced in each proposal.

Operational Sustainability
GDS was incorporated/formed in 1985 and has been providing services to Customers for over 35 years. As of the date of this report, GDS' financials showed that its operations were profitable over the previous 12 months. This profitability indicates operational sustainability and fiscal responsibility.

Customer and Employee Retention Tracking
Over the last fiscal year, GDS has a managed services retention rate that fits the UCS best practice.



UCS Domain 2 – Trust: Summary

Trust is essential in the relationship between an organization and its customers, evaluated through measures ensuring integrity and reliability. To become a trusted partner, MSPs advise on technical solutions, understand unique environments, and suggest technology improvements. Trust is illustrated by conducting internal audits, managing capacity requirements, resolving problems, and locking down remote access. Environmental safeguards protect against disruptions, and physical access to hardware is restricted to authorized personnel. Reporting metrics demonstrate sustainable profits and long-term customer relationships. Robust insurance policies mitigate business disruption, solidifying the MSP's role as a trusted partner and ensuring continuity and growth.

2.04	**Internal Audit**	✓
2.08	**Service Transition Continuity**	✓
4.05	**Capacity Planning**	✓
5.02	**Support and Problem Logging**	✓
5.03	**Categorization and Correlation**	✓
5.04	**Support and Problem Resolution**	✓
6.08	**Restricted Secure Remote Access**	✓
8.05	**Data Center Environmental Controls**	✓
8.06	**Data Center Maintenance**	✓
8.07	**Data Center Colocation**	✓
9.03	**Report Availability**	✓
10.03	**Sustainable Profit Margin on Services**	✓
10.04	**Customer Commitments**	✓
10.05	**Insurance**	✓

Internal Audit

GDS performs an annual internal audit of their controls following a standardized checklist. This audit is tracked in a recurring ticket, and the completed checklist and remediations resulting from the audit are documented in the ticket notes.

VP Operations is responsible for reviewing and approving the internal audit report upon completion. This approval is documented. approved, and dated via the e-signature application.

The scope and criteria of GDS' internal audit are documented in the internal audit checklist to guide the performance of the internal audit.

Audit support documents and results are stored in GDS documentation tool Audit section.

Service Transition Continuity
GDS ensures that Customer systems are properly reconfigured, and all prior or current MSP access has been removed during the onboarding and offboarding process, guided by its Service Transition Policy.

Capacity Planning
GDS monitors both internal and Customer storage capacity and availability with the scanning application. High consumption events trigger a service ticket, and the resolution can range from removal of temporary files to providing additional storage through the change order process. Utilization is reviewed with Customers during the EBR process. GDS also monitors the aggregate storage available to Customers and is tracked on a weekly basis for capacity management.

GDS monitors their SAN capacity continuously in a business intelligence reporting dashboard and reviews their SAN capacity on a weekly basis. The weekly review is tracked in GDS' Level 10 meeting standing agenda.

Support and Problem Logging
Customer support issues/requests are logged in the PSA. Tickets are categorized and prioritized by source (email, RMM, phone, manual generation), Customer, and level of impact/urgency.

Tickets are automatically generated into the PSA from the scanning application and RMM via an email connector. Tickets are also automatically generated from backup applications to RMM.

GDS auto-closes tickets by Customer request from VSAT telecommunications Customers after a set period of time. GDS does not delete tickets. For these, tickets are logged, remain open for a prescribed amount of time, and, barring subsequent events, are auto-resolved.

GDS has service level targets based on the severity of the incident and its impact on the Customer. While GDS typically tries to respond to all cases quickly, the SLA defines target response times for Customers (typically 15 minutes for Priority (P1) level cases, 30 minutes for Priority 2 (P2), 60 minutes for Priority 3 (P3), and 24 hours for Priority 4 (P4).

Categorization and Correlation
For monitoring generated tickets, the RMM tools provide info to PSA that denotes priority. This priority level is predetermined upon the configuration of the monitored item/asset. GDS also utilizes a categorization list for each ticket that is generated. For phone or email-generated tickets, GDS has a documented process that is followed for proper ticket priority and categorization.

In the event of a notification storm tickets are manually correlated as parent/child tickets in the ticketing system.

Support and Problem Resolution
GDS houses ticket documentation requirements in the documentation application. Some Customers request modified documentation requirements, these modifications are stored in the documentation application.

GDS has documented Customer communication in their NOC SOP's. This covers events identified in monitored environments.

Updates, closures, and engineer assignment are auto-communicated to the Customer from the PSA.

Restricted Secure Remote Access
GDS uses the remote access VPN client, specific routes utilizing site-to-site VPN, or the RMM to access customer networks.

Remote Desktop logs are kept on the server, and RMM logs every time a user connects remotely. Logs are only reviewed if issues are reported through tickets.

Data Center Environmental Controls
GDS has Smoke/Fire detectors monitored via third party monitoring platform. Waterless (FM200) Fire Suppression systems are also installed and inspected yearly. Redundant HVAC systems are monitored via the RMM and also alert if any water intrusion is seen under the raised floor. UPS systems are monitored via the RMM as are rack mounted PDUs. There is also a generator panel within the NOC which indicates line power or generator power as well as generator's health status using audible alerts. Datacenter temperature is monitored via the cloud infrastructure management environmental sensors which generate tickets automatically when conditions exceed configured thresholds.

Data Center Maintenance
GDS has Smoke/Fire detectors monitored via third party monitoring platform. Waterless (FM200) Fire Suppression systems are also installed and inspected yearly. Redundant HVAC systems are monitored via the RMM and also alert if any water intrusion is seen under the raised floor. UPS systems are monitored via the RMM as are rack mounted PDUs. There is also a generator panel within the NOC which indicates line power or generator power as well as generator's health status using audible alerts. Datacenter temperature is monitored via the cloud infrastructure management environmental sensors which generate tickets automatically when conditions exceed configured thresholds.

Maintenance contracts are maintained on the backup generator, HVAC systems, Uninterruptible Power Supplies, and FM200 suppression system per supplier recommendations.

Data Center Colocation
Physical access to colocation hardware maintained in GDS' facility is restricted to individuals designated by the Customer and authorized GDS personnel. The current list of Customer-authorized individuals is maintained within Contacts in the ticketing system and the authorized access forms are documented within the Customer's contact folder.

Report Availability
Periodic reporting is established based on Customer requirements. GDS creates one or two sample reports from different reporting platforms to illustrate the capabilities of each during the Customer onboarding process. Once the Customer experiences the reporting and identifies a few use cases, GDS configures recurring reports (scheduled, delivered by email) on their behalf. GDS will also perform a limited number of on-demand reports based on predefined manufacturer templates when a Customer requires an in-depth traffic review. GDS tracks report requests in a ticket.

Sustainable Profit Margin on Services
GDS maintains a positive gross profit margin on its services, which meets the UCS best practice of maintaining a positive gross profit margin. By meeting the best practice, GDS is operationally efficient in its costs of delivering services.

Customer Commitments
The majority of GDS contracts have a term of 2 to 5 years. GDS utilizes month-to-month contracts on a limited basis, with those contracts supporting specific services or service lines.

Insurance
GDS carries insurance coverage commensurate with UCS best practices, including cybersecurity, errors and omissions, professional liability, and key man life.



UCS Domain 3 – Security: Summary

Security is crucial for Managed Service Providers (MSPs) because they protect sensitive data. UCS exemplifies this by limiting access to authorized personnel, encrypting data, and assessing external service providers. Advanced threat management tools and physical security measures like segregated networks and controlled entry ensure the integrity of data centers and server rooms. These protocols maintain operational sustainability and protect customer information.

1.05	**External Service Provider Management**	✓
3.03	**Data Classification and Encryption**	✓
3.06	**External Service Provider Access**	✓
4.03	**Internal Change Tracking**	✓
6.01	**Controlled Access to Applications and Environments**	✓
6.02	**Super User and Administrator Access Security**	✓
6.03	**Unique Users and Passwords**	✓
6.05	**Strong Passwords**	✓
6.09	**Network and Endpoint Security Management and Monitoring**	✓
6.10	**Email Security**	✓
6.11	**Network and Endpoint Protection**	✓
6.12	**Wireless Network Security**	✓
6.13	**Network Security Review**	✓
6.14	**Security Logging**	✓
7.05	**Internal Data Destruction**	✓
7.06	**Customer Data Destruction**	*
7.07	**Device and Asset Management**	✓
8.01	**Organizational Physical Security**	✓
8.02	**Logging of Visitors**	✓
8.03	**Sensitive Area Security**	✓

External Service Provider Management
An initial risk analysis should be conducted for each potential vendor by members of the Executive team. At a minimum, the risk analysis will utilize the Vendor Risk Rating Matrix to assign a Vendor Risk Rating of Low, Medium, or High risk. A vendor is assigned a risk rating based on the highest risk level attributable to the contract, or sum of all contracts, with that vendor. Exceptions to the assigned risk rating may be granted as noted by the Risk Rating Matrix.

GDS has a documented Vendor Management Policy. Part of the policy is to identify the risk profile of all vendors and significant third parties based on business impact, customer contact, contract term, and access to data.

GDS evaluates Vendors with a Vendor Risk Analysis before they are on-boarded.

Data Classification and Encryption
GDS has a Data Classification & Data Handling Document that contains Data Classifications and covers both internal and Customer data.

All data stored on GDS storage devices are encrypted at rest and in transit for Customers receiving backup services.

External Service Provider Access
Service Provider personnel receive temporary access only by request. Some Customers request that their vendor be granted access to GDS systems in this case GDS grants temporary access.

External service providers that request access to GDS or Customer systems are tracked within tickets. Management approves the access request. GDS does not currently monitor the third party vendor's activities, however access request tickets are only reviewed when requested by Customers.

Internal Change Tracking
Internal Change requests are treated and handled as change management requests.

GDS has a documented Change Management Policy that outlines rules to be followed in the change management process. Employees can submit a request for a change as an internal change ticket, which is tracked as a Change Management ticket type. Once submitted, the change is reviewed during the daily Change Committee meeting, where committee members document the approval or rejection of the change. The implementation of the change is tracked in a new ticket or project, depending on the size and scope of the change.

Controlled Access to Applications and Environments
GDS has deployed RBAC policies using AD to confirm personnel have network access based on defined roles and responsibilities by job role and the GDS security group naming convention matches job roles for easy access. Access to GDS internal applications is also granted by the job role. Customer system and data access are restricted to GDS technical personnel by job role.

All service delivery systems are secured by AD and the 2FA/MFA application.

When onboarding a new employee, A service ticket is created by the GDS HCM platform with the onboarding tasks listed as to-do items. Physical access and application access are determined by the RBAC title role assigned to the new employee. Employee, employee role, and access are documented in AD.

When an employee changes roles, GDS HR sends a role change request to the support desk. A service ticket is created to track the work.

The current RBAC role assigned to the employee is removed and the new RBAC role is applied in AD.

Requests for access not included in the assigned RBAC role must be approved by the employee's manager before being applied in AD.

All access rights MACD's are reviewed through GDS change management.

Super User and Administrator Access Security
Passwords for administrator accounts are documented in the documentation application with access being limited to authorized employees. Some administrator accounts are shared between authorized employees. The documentation application tracks authorized employee access to the shared administrator passwords via logs.

Access is controlled by RBAC policies in AD. Any modifications are approved through GDS change management.

Unique Usernames and Passwords
All GDS employees are given a unique username and password on the active directory management Domain. Usernames are the employee's first name and last initial unless this is already in use by another employee. If this is the case, the employee is given a username that consists of the first initial last name.

Service accounts are separated into their own OU in AD. Passwords are stored in the documentation application. Access is restricted and logged. Service accounts are given the minimum necessary permissions. All service account access is logged and monitored.

GDS tech resources access customer domains using unique accounts except where shared access is required by customers.

Shared access accounts are secured in the documentation application and access is granted based on role.

Guest accounts are only utilized in the application suite and are restricted to accessing the specific documents shared with them. GDS does not utilize guest accounts in AD or any other applications.

Strong Passwords
GDS' password policy is a minimum of 10 characters, one upper case and one lower case letter, one number, and one special character. It must be changed every 90 days and employees are notified to change it. It cannot be reused within 24 passwords and the account will lockout after 10 failed attempts.

Where applicable, GDS links the delivery services to AD, so that AD enforces the passwords. For applications not integrated with the AD, GDS enforces password policies to the extent possible. The passwords are enforced through the individual platforms and documented in the platform by the manufacturer. For applications that have their own authentication and are not linked to AD, the user must use the corporate password policy when creating passwords. In the event the application password strength is greater than the corporate password strength, GDS employees use the application's password policy.

Network and Endpoint Security Management and Monitoring
The GDS Corp network is protected by the firewall application utilizing the firewall with network AMP. The firewall provides IPS, web content filtering, and malware protection. The endpoint protection application protects the GDS Corp network and mobile users at the DNS layer. The endpoint protection application provides email filtering, spam, fishing, and virus protection for email. The 2FA/MFA application provides MFA for all Corp user access to desktops, laptops, and servers. It is also implemented on mission-critical applications and software. A SIEM is used to gather security logs from across the enterprise. It is then configured to create alerts on malicious or concerning security activities. The SIEM takes in SIEM data, threat intelligence, and other telemetry meaningful for security analysts. Playbooks are created to identify, investigate, and mitigate security threats found.

GDS uses the security endpoint protection application for endpoint protection. The security endpoint protection application continuously scans endpoints for malicious files and activity. Endpoint protection protects the GDS Corp network at the DNS level for malicious traffic activity. All laptops have an endpoint protection application roaming client that protects users off the GDS network. The 2FA/MFA application protects as MFA protection against stolen credentials. The SIEM agents monitor and gather endpoint logs that are sent to the SIEM for analysis.

Device health is managed through the RMM platform. All security logs and alerts are sent to the SIEM.

All changes on firewall are managed through change management tickets and change management board approval. All firewalls have been properly configured, and their configurations are exported and backed up when a commit is made to the device, and they are backed up nightly.

The cloud infrastructure management security appliances, wireless switches, Access points, and Cradle points devices utilize a multitenant platform. Firewall appliances are managed on a customer-by-customer basis.

Firewall baseline configs utilize security best practices. The customer requested changes follow security best practices. Each Customer's fire configuration is customized to the Customer's specifications, with changes to the firewall configurations being handled and logged as part of the company's change management procedures. All firewalls have been properly configured, and their configurations are exported and backed up as part of the nightly backup process. The health status of the firewalls is monitored in the RMM.

GDS provides SIEM as a service, but it can be wholly separated and independent from other service lines such as firewall management or monitoring services. SOC Analysts monitor the SIEM for alerts which are correlated into cases by the SIEM and triage them accordingly.

Email Security
The email security application is utilized to monitor and protect emails internally by scanning incoming emails for potentially harmful links and attachments. In the event of blocked messages or stripped attachments, GDS users open a ticket with support for investigation. Alerts are generated in the event of issues related to the delivery of the service.

When applicable to the version sold under contract to a client the ESA is monitored for health and up time.

Network and Endpoint Protection
GDS uses the endpoint protection application to monitor all endpoints including laptops, desktops, and servers. The alert/threat data is sent to the SIEM, from the security endpoint protection application. Then automation processes take place to create a case out of the alert data, as well as create a PSA ticket to associate with that case. Once automation is completed, our analysts work those cases to closure in the SOAR, and the PSA ticket is updated accordingly.

Based on the version of the product sold under contract emails are generated for notification of alerts.

Wireless Network Security
The company has implemented the cloud infrastructure management access points to secure and manage wireless access points at the main office and branches which are protected by WPA2-Enterprise with PEAP authentication using AD a as an authentication source and the identity governance application for device filtering/management.

Guest wireless connectivity is available and secured with MAC based access control. The guest wireless network is a segmented untrusted network that does not have access to the company's internal network and is segregated by firewall rules in the Firewall applications, only allowing traffic directly out to the internet.

Network Security Review
GDS performs a monthly vulnerability assessment of internal and external networks. The GDS security team reviews the monthly vulnerability report based on NIST best practices, industry threat intelligence, and known malicious CVE from US-CERT. A ticket is generated each month for the activity. The Service Desk works to remediate those vulnerabilities that can be addressed. When issues are seen that SecOps considers being a potential risk to GDS, a FOCUS project is generated to discuss, evaluate corporate risk, and mitigate when directed.

Security Logging
GDS has configured its Active Directory, security applications, and internal systems to collect logs. These logs range from user activity logs, security event logs, error logs, access logs, and system logs. A SIEM has been implemented to scan these logs and raise alerts for identified events. Logs associated with an incident are retained for 365 days before being archived. Logs not associated with an incident are retained for 30 days before being archived. Archived logs are retained for a minimum of one year.

Internal Data Destruction
GDS has a documented internal data destruction policy that is located in GDS documentation tool. Device destruction is tracked in PSA tickets.

Customer Data Destruction
Not Applicable - GDS does not offer data destruction service to customers.

Asset and Device Management
GDS has a documented BYOD and Device policy, and it spells out “personal devices” which means any device not owned by GDS regardless of type.

GDS manages and monitors all internal assets through their RMM. Only internal devices loaded into this RMM by GDS. A list of all assets can be exported from this area of the RMM.

Organizational Physical Security
GDS employs a variety of physical security controls to ensure the flow of personnel is secure. All exterior doors remain locked at all times and access to the facility is by electronic card scanners. Employees are assigned their own security card during the onboarding process. The assignments of the GDS Access cards are managed and monitored in the Physical security – access management system.

There are also some restricted areas within the facility that are accessible by approved employee security cards. There are a number of cameras throughout the exterior of the facility strategically placed to cover the various entry portals. The camera feeds are fed into the NOC, Field Services Manager, Procurement, and Warehouse offices.

GDS maintains the facilities security systems as a matter of daily business. If there are any issues with the systems, they are reported to facilities management immediately for repair or remediation. The remediation efforts are created and tracked in the GDS ticket system.

Logging of Visitors
All non-GDS personnel must enter the facility through the reception area. The receptionist gathers the person's name and professional affiliation along with the time and date of entry to place into the Visitors Logbook. They are issued a name tag with the info that they must display on their outer wear until they leave the facility. At which time the receptionist retrieves the badge and logs them out of the facility in the logbook.

Sensitive Area Security
GDS employs card scanners that control door locks that will allow access to approved personnel into restricted areas. These areas include the NOC, Secure Warehouse area, and Data Center. Personnel that require access to these areas go through the approval process upon hire. Approval is determined by the hiring manager and is managed and monitored via the Genea Access Control software. Any unapproved personnel needing access to these areas must be accompanied by the appropriate GDS employee at all times. GDS reviews access rights to sensitive areas and tracks them through quarterly tickets.



UCS Domain 4 – Resilience: Summary

The UCS Domain on Resilience assesses the organization's capacity to handle disruptions through thorough risk management and business continuity strategies. Formal policies address incident responses for cyber threats, supported by executive oversight. MSP employees undergo comprehensive onboarding, regular cybersecurity training, and adhere to strict confidentiality standards. Security is ensured by managing access to information systems, systematic provisioning and revocation of access, and background checks. Real-time security and traceability are achieved through application version tracking. Continuous data backup schedules and tested business continuity plans provide robust protection against disruptions. Facility access is revoked upon employee termination to secure sensitive data. These measures demonstrate UCS's strong resilience and data protection, enabling effective incident response and ensuring operational continuity.

1.01	**Organizational Structure**	✓
1.03	**Risk Management**	✓
2.02	**Incident Response Policies and Procedures**	✓
2.06	**Training and Orientation**	✓
2.07	**Security Awareness Training**	✓
3.01	**Employee Background Checks**	✓
3.02	**Employee Confidentiality and Privacy Acceptance**	✓
6.04	**Revocation of Access**	✓
6.06	**Segregation of Access**	✓
7.01	**Customer Data Backup and Replication**	✓
7.02	**Organization Data Backup and Replication**	✓
7.04	**Disaster and Business Continuity Planning**	✓
8.04	**Revocation of Physical Access**	✓

Organizational Structure
GDS has an Executive Team responsible for the strategic planning and overall direction of the company and a Leadership Team responsible for specific department operations, managed services, and planning. The Executive Team is comprised of the President/CEO, COO, CFO, VP of Operations, VP of Human Resources.

The GDS Executive team has quarterly off site meetings and deliverables are documented in the EOS platform, our Executive team also meets weekly which is documented in the EOS platform for tracking and retention.

GDS has a two Owners. The composition of the Owners group consists of a President/CEO and CTO. Each owner possesses some company stock.

The Executive Team, except for the President/CEO, reports to the COO and meets weekly. The Executive Team members include the President/CEO, and CTO who are part of the governance structure. Additionally, the VP of Sales, CFO, COO, VP of Human Resources and VP of Operations are part of the Executive team. EOS software is used to guide the meeting, provide structure and document data and tasks.

FOCUS, chaired by the COO, consists of various department representatives. The mission of this committee is to facilitate communications throughout GDS, provide departmental perspective on all GDS projects, prioritize and define GDS projects and utilize GDS resources efficiently. The group evaluates PRF (Project Request Form) submissions, which may include new or revised Product or Services.

The FOCUS Project Administrator maintains project plans and detailed notes in the documentation tool for viewing by all GDS employees.

The GDS Operations team meets weekly to discuss tasks, to-dos, newsworthy company events, and ROCKS. The Change Management Committee meets each business day.

The organizational chart is updated as needed and is reviewed as part of the annual planning meeting agenda. The Executive team reviews the accountability chart annually, as part of their agenda.

The GDS organizational chart is maintained through an application that renders the chart from company directory information, which is updated upon every hire, separation, and organizational change. It is available to all company personnel within the company's associate portal intranet site.

GDS has documented job descriptions and requirements for all positions. Requirements such as education and certificates are noted and listed in any job posting. Further, GDS utilizes a tier progression chart that lines out all requirements for engineers to advance through GDS' tier system.

Risk Management

Risk management activities are documented in weekly Level 10 (L10) meeting notes as they arise. A standardized risk assessment spreadsheet is utilized to log and identify risks on an annual basis. This spreadsheet has a recurring ticket that is automatically generated for management review.

Leadership holds primary responsibility for developing, maintaining, and updating the organization's risk assessment framework.

Incident Response Policies and Procedures

The incident response policies in GDS' Cyber Security Incident Response Plan directly address cyber, ransomware attacks, and provide incident response and communication services to any security breaches.

GDS will formulate a response for Customers that are affected by the data breach and communicate the next steps to the appropriate Customer point of contact.

GDS does not store Customer data.

GDS has procedures documented in the Cyber Security Incident Response Plan that cover the company's response and communication of the breach to the appropriate parties. However, it may differ from Customer to Customer; where appropriate.

GDS has not made any ransomware payments within the past 12 months.

Training and Orientation
GDS has a new hire onboarding (orientation/training) program. The framework is documented and can be modified for each position/role. GDS company and role-specific training are performed for all new hires. Both pieces of training are tracked in a standardized checklist following the new hire training documents.

GDS has continuing training and education programs for employees. These can be specific to each role and position and may involve internal or self-study or external training by an external service provider. Some of the courses are tracked by Learning Management System.

Security Awareness Training
GDS requires its employees to participate in security awareness training. An LMS is utilized to assign security modules monthly, with completion of the modules being tracked within the LMS.

Currently, GDS is looking for a new LMS to provide security training.

During this time GDS did have an LMS that handled security and non-security related training. We have since implemented a new system for the non-security training and are looking for a security related training system.

Employee Background Checks
All new hires are subject to background checks (7-year criminal history, SSN check, Motor Vehicle Report) and new-hire drug screening. The HR department orders and tracks the screenings and if a successful screening isn't acquired then the offer is rescinded.

GDS has a background checklist process. The background checklist includes criminal background checks, ID validation, and motor vehicle records if applicable to the position. The background checklist is used both for new hires. The completed checklist is attached and retained in the employee file folder.

Employee Confidentiality and Privacy Acceptance
The GDS Employee Agreement includes a "Confidential and Proprietary Information" section. All GDS employees are required to sign this Employee Agreement.

All GDS employees are required to sign and attest to their understanding and adherence to the company's confidentiality and privacy policies via the signing of an Employee Agreement and Employee Guidebook Acknowledgment as part of the new hire process.

Revocation of Access
Access revocation is documented in the ticket. GDS HCM creates a ticket with the offboarding tasks listed as to-do items.

Segregation of Access
Access is segregated based on employee roles using RBAC groups in AD to assign permissions. Access for an employee is reviewed and updated if their role changes.

GDS segregation of duties based on employee title. This is enforced by RBAC policies in Active Directory.

GDS has an Access Control Policy that contains a high-level explanation of the company's access segregation methodology.

Customer Data Backup and Replication
GDS contracts to provide backup and replication services to Customers. Each backup and replication policy is crafted to match the Customer's retention and backup requirements. These backup configurations are crafted during the Customer onboarding process. Changes to the backups are handled and tracked as part of the Change Management Process. This includes frequency for backups as well as retention time periods.

GDS encrypts the Customer's backup data while in transit and at rest. Per industry best practice GDS has instituted this as a standard as stated in their data classification policy.

Initial requirements are documented in the initial statement of work and subsequent changes are documented in Change Management tickets. Backups are automatically configured to encrypt while at rest & in transit within the backup application.

Organization Data Backup and Replication
GDS utilizes the following standard for internal backups: GDS performs Daily Backups on all servers. GDS utilizes a 14-day retention policy for all backups. GDS currently performs an initial full backup and then reverse incremental via the backup application standard configuration on a nightly basis. The GDS Internal Backup Policy covers all backups. GDS encrypts internal backup data while in transit and at rest utilizing the functionality built into the backup application.

Disaster and Business Continuity Planning
GDS has a Business Continuity Plan that is tested. GDS reviews the plan yearly and as we implement the plan during events requiring the plan to be placed into action, we perform analysis and update plan during next semi-annual meeting. The results of the test are documented in the minutes of the yearly meeting.

Revocation of Physical Access
As part of the GDS termination process the security card is electronically disabled. The revocation is tracked in our ticketing system as well as the HR Employee Information management system.



UCS Domain 5 – Transparency: Summary

Transparency forms the backbone of the UCS Domain, emphasizing the necessity of clear communication and openness to build trust and fortify relationships with customers and stakeholders. By adhering to annual reviews and updates of policies, the organization ensures operational integrity and compliance with current standards. Additionally, the meticulous management of data geolocation and financial transparency through strategic revenue distribution exemplifies the commitment to accuracy and sustainability. This comprehensive approach not only safeguards financial stability but also fosters an environment where employees and customers feel valued and informed, ultimately supporting the organization's long-term objectives in alignment with UCS guidelines.

2.01	**Documentation of Policies and Procedures**	✓
2.03	**Periodic Review and Approval**	✓
2.05	**Employee Acceptance**	✓
3.04	**Organization Data Geolocation Disclosure**	✓
3.05	**External Service Provider Geolocation Disclosure**	✓
3.07	**External Service Provider Access Disclosure**	✓
4.02	**Service Level Categorization**	✓
9.02	**Accuracy of Service Invoices**	✓
10.02	**Significant Customer Risk**	✓

Documentation of Policies and Procedures
GDS has an Employee Guidebook that covers the following topics:

- Building for the Future
- Mission
- Our Vision
- Our People
- Organizational Climate
- Quality
- Guidebook Purpose
- Employment
- Conduct and Behavior
- Compensation
- Benefits
- Health, Safety, and Security
- Workplace Guidelines
- Employment Separation

The following topics are addressed in the GDS Security Policy: Server Security, Network Security, Data Security and Physical Security.

HR policies and procedures are maintained on the documentation tool, where they are available to employees. The review of these policies and procedures with new hires is tracked with a new hire checklist.

Periodic Review and Approval
Policies are reviewed annually, usually meeting minutes are kept where changes are discussed. If a change is made the changes are tracked and approved before being published.

GDS management is responsible for the maintenance and administration of the Policies and Procedures Manual.

Employee Acceptance
As part of New Hire Orientation, all employees are required to read and sign the acceptance and acknowledgment page of the Employee Handbook. Company policies and procedures are sent electronically via email for attestation and tracking of all documentation.

When updates are made to the Employee Guidebook, which usually happens as needed - the updates are communicated to all employees via email and all affected acknowledgments are re-signed. These acknowledgments are stored in each employee's folder.

The last time GDS sent out a new guidebook was in 2023.

Organization Data Geolocation Disclosure
All customer stored data is housed in the GDS Datacenter located in Lafayette, LA except for the data associated with customers who subscribe to our Geodiverse Secure Backup product. Customers are notified verbally in the sale process, and it is also noted in our Geodiverse Secure Backup Product Description.

External Service Provider Geolocation Disclosure
GDS will "leverage our relationships with industry-leading cloud providers to implement scale-out storage for offsite backups." This is inherent in this Secure Backup product.

GDS Customers are made aware of where their Geo backups are located. For the virtual data centers, the location is regional. Communication of this is verbal in the pre-sales process and Customers receive a Geodiverse Secure Backup Policy.

External Service Provider Access Disclosure
Once third-party or vendor access is approved via request, GDS tracks the third-party's access in a ticket. Customers are notified of third-party access via an automated email through the GDS ticket notification process. The email notification could go to a single requestor or a company distribution depending on how each individual Customer is configured.

Service Level Categorization
GDS uses a PSA application to classify and identify all new, existing, and former Customers. Companies are identified by Name, Company Type, Industry, Agreement Status, and Agreement Types. Every active Customer has an agreement corresponding to the product or service to which they subscribe. All companies with an active Managed Service Agreement are given a status of active in the PSA. This allows Service Delivery to process requests for these Customers. GDS has four ticket priorities that drive different response and resolution goals by priority. These priorities apply to all Customers. GDS does not offer different priorities or SLAs by Customer.

GDS sets global SLA and priority standards across all customers. Each customer's profile denotes customer name, type of industry, the status of service eligibility, and type of Customer.

Accuracy of Service Invoices
Invoices are generated the first of the month for recently completed work for recurring services and set up fees. Pricing is dictated by the Customer’s signed contract. Flat/fixed fee projects, like professional services, are billed upon completion. All out of scope work is billed per the standard rates.

Significant Customer Risk
GDS’ top five Customers represent less than half of total GDS revenue, which is the UCS best practice of 50% from the top five Customers. The largest GDS Customer represents 20% of total GDS revenue which is less than the UCS best practice of one Customer not representing more than 20% of total revenue. Due to this, GDS is considered to have minimal risk due to a loss of a significant Customer.

SECTION 6: UCS REPORT ADDENDUM

SOC 2 Report Addendum

MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers®

FOR GDS' SOC 2 MAPPING

This Cyber Verify™ Program report for Global Data Systems, Inc. (GDS) is based on the Practice Domains of the Unified Certification Standard for Cloud and Managed Service Providers® (MSPs) (UCS) Version 3. The UCS Practice Domains establish best practices for MSPs in the delivery of their services to customers. The UCS generally applies to most MSPs around the world, regardless of their vertical or market expertise and focus.

The UCS Practice Domains align with the Trust Services Criteria (TSC) for SOC 2. The UCS framework has compensating controls at over 200 points within Security, Availability, and Confidentiality criteria. Each TSC control maps to a UCS Practice Domain using its unique identifier.

ID	Domain	UCS Cross Mappings to Trust Services Criteria	Exceptions Noted
	Expertise	**36**	None
	Trust	**36**	None
	Security	**67**	None
	Resilience	**48**	None
	Transparency	**21**	None

A Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) is a report that describes how a Service Organization meets the criteria defined in a set of TSCs[1].

The following table represents the mapping of the GDS Cyber Verify™ report to their SOC 2 report[2]. This table was included in the issued and unqualified 2024 GDS SOC 2 Type 2 report on Security, Availability, and Confidentiality.

Trust Services Criteria for Security, Availability, and Confidentiality	UCS Practice Domains				
	01	02	03	04	05
CC 1.0 Common Criteria Related to Control Environments					
CC 1.1 The entity demonstrates a commitment to integrity and ethical values.					
CC 1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.					
CC 1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.					

[1] TSC section 100, *Trust Service Criteria for Security, Availability, and Confidentiality, 2017* (AICPA, *Trust Services Criteria With Revised Points of Focus – 2022*)

[2] The TSC does not address the requirements of UCS Objective 9: Billing and Reporting and UCS Objective 10: Corporate Health.

Trust Services Criteria for Security, Availability, and Confidentiality	UCS Practice Domains				
	01	02	03	04	05
CC 1.0 Common Criteria Related to Control Environments					
CC 1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.				∞	
CC 1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	♛		🔒	∞	👁
Trust Services Criteria for Security	**UCS Practice Domains**				
	01	**02**	**03**	**04**	**05**
CC 2.0 Common Criteria Related to Communications and Information					
CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		✓	🔒		👁
CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	♛	✓	🔒	∞	👁
CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	♛	✓	🔒	∞	👁
CC 3.0 Common Criteria Related to Risk Management					
CC 3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	♛		🔒	∞	
CC 3.2 The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	♛	✓	🔒	∞	
CC 3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.	♛	✓		∞	
CC 3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.				∞	
CC 4.0 Common Criteria Related to Monitoring Activities					
CC 4.1 The entity selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	♛	✓	🔒		
CC 4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	♛	✓	🔒		
CC 5.0 Common Criteria Related to Control Activities					
CC 5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	♛		🔒		
CC 5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.	♛		🔒		👁
CC 5.3 The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.	♛				👁
CC 6.0 Common Criteria Related to Logical and Physical Access Controls					
CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		✓	🔒	∞	
CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		✓	🔒	∞	
CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	♛	✓	🔒	∞	

Trust Services Criteria for Security	UCS Practice Domains				
	01	02	03	04	05
CC 6.0 Common Criteria Related to Logical and Physical Access Controls					
CC 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		✓	🔒	∞	
CC 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		✓	🔒		
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		✓	🔒	∞	
CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	♛		🔒	∞	
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	♛	✓	🔒	∞	
CC 7.0 Common Criteria Related to System Operations					
CC 7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	♛	✓	🔒		
CC 7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	♛		🔒	∞	
CC 7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	♛		🔒	∞	
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	♛			∞	
CC 7.5 The entity identifies, develops and implements activities to recover from identified security incidents.	♛				
CC 8.0 Common Criteria Related to Change Management					
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	♛		🔒	∞	
CC 9.0 Common Criteria Related to Risk Mitigation					
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	♛			∞	
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.			🔒		
A 1.0 Additional Criteria for Availability					
A 1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		✓			
A 1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		✓		∞	
A 1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	♛			∞	
C 1.0 Additional Criteria for Confidentiality					
C 1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			🔒	∞	👁
C 1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			🔒		

COMPANY INFORMATION

Examined Company:
GDS
310 Laser Lane
Lafayette, LA 70507
getgds.com

Independent Third-Party Auditor:
Sensiba LLP
101 Metro Drive, #160
San Jose, CA 95110

Examining Body:
MSPAlliance®
Phone: 800-672-9205
www.mspalliance.com