Unified Certification Standard
For Cloud and Managed Services

2014 Certified & Accredited Company

MSPAlliance®
Int'l Assoc. of Cloud & Managed Service Providers

# UCS Level 2 Report Issued to

MAINSTREAM TECHNOLOGIES
MANAGED SERVICES • CUSTOM SOFTWARE • HOSTING

MSPAlliance®
Int'l Assoc. of Cloud & Managed Service Providers

Welcome to the UCS report which stands for Unified Certification Standard for Cloud & Managed Service Providers. The UCS represents nearly a decade of work on the part of the MSPAlliance to bring standards and best practices to the cloud and managed services profession.

This report, along with every UCS report, is issued only after the service provider has satisfied the control objective requirements of the UCS. The UCS is comprised of control objectives (described within this report). Each control objective has individual controls which must be met in order for the larger objective to be satisfied.

This UCS report will describe the control objective, what its purpose is, and how the service provider has satisfied that control objective. While great care and detail went into the examination of the service provider, in order to protect the security of both the provider and its customers, some details of how they deliver their services, including their security and privacy controls, are discussed here in general terms.

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 independent accounting firm if you have specific questions about how the examination was conducted.

By using cloud computing and managed services from a UCS certified and accredited service 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.

Charles Weaver
Chief Executive Officer
The International Association of Cloud & Managed Service Providers

HoganTaylor LLP
CERTIFIED PUBLIC ACCOUNTANTS

**INDEPENDENT ACCOUNTANT'S REPORT**

Board of Directors
Mainstream Technologies, Inc.
Little Rock, Arkansas, United States of America

HoganTaylor LLP has examined management's assertion that Mainstream Technologies, Inc. (Mainstream), throughout the period April 1, 2013 to March 31, 2014, maintained effective controls over its Managed Hosting, Managed Virtual Hosting, Collocation services, Full Service IT and GetIT Back services environment, referred to as its Cloud and Managed Services Environment (Services), to provide reasonable assurance that Mainstream has met, in respect to the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers – Level 2, requirements of the following objectives:

- Objective 1: Provider Organization, Governance, Planning and Risk Management,
- Objective 2: Provider Policies and Procedures,
- Objective 3: Configuration and Program Change Management,
- Objective 4: Event Management,
- Objective 5: Logical Security,
- Objective 6: Data Privacy, Security and Integrity,
- Objective 7: Physical and Environmental Security,
- Objective 8: Service Level Agreements, Customer Reporting and Billing, and
- Objective 9: Corporate Health.

Management is responsible for Mainstream's compliance with those requirements. Our responsibility is to express an opinion on management's assertion about Mainstream's compliance based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and International Standard on Assurance Engagements established by the International Federation of Accountants and, accordingly, included examining, on a test basis, evidence about Mainstream's compliance with those requirements and performing such other procedures as we considered necessary in the circumstances. We believe our examination provides a reasonable basis for our opinion. Our examination does not provide a legal determination on Mainstream's compliance with specified requirements. Our examination did not include completing an audit of Mainstream's financial statements.

In our opinion, management's assertion that Mainstream complied with the aforementioned requirements for the period April 1, 2013 to March 31, 2014, is fairly stated, in all material aspects.

HoganTaylor LLP

September 9, 2014

*688 E. Millsap, Suite 203, Fayetteville, AR 72703-4095*
***P*** *479.521.9191* ***F*** *479.521.2817*
***www.hogantaylor.com***

325 West Capitol Avenue, Suite 200
Little Rock, Arkansas 72201-3552
501.801.6700

MAINSTREAM TECHNOLOGIES
MANAGED SERVICES • CUSTOM SOFTWARE • HOSTING

**REPORT BY MANAGEMENT ON THE SERVICES ENVIRONMENT BASED ON THE MSPALLIANCE UNIFIED CERTIFICATION STANDARDS FOR CLOUD AND MANAGED SERVICE PROVIDERS – LEVEL II**

Mainstream Technologies, Inc. (Mainstream), maintained effective controls over its Cloud and Managed Services Environment (Services) throughout the period April 1, 2013 to March 31, 2014, to provide reasonable assurance that Mainstream has met, in respect to the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers – Level 2, requirements of the following objectives:

- Objective 1: Provider Organization, Governance, Planning and Risk Management,
- Objective 2: Provider Policies and Procedures,
- Objective 3: Configuration and Program Change Management,
- Objective 4: Event Management,
- Objective 5: Logical Security,
- Objective 6: Data Privacy, Security and Integrity,
- Objective 7: Physical and Environmental Security,
- Objective 8: Service Level Agreements, Customer Reporting and Billing, and
- Objective 9: Corporate Health.

The MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers is available at www.mspalliance.com/ucs and as an appendix to this report.

The attached Mainstream Description of the Services summarizes those aspects of this environment covered by our assertion.

Johnny Burgess
President
Mainstream Technologies, Inc.
Little Rock, Arkansas, United States of America

March 31, 2013

# Mainstream Description of the Cloud and Managed Services Environment

## Mainstream Background

Mainstream Technologies, Inc. (Mainstream) is a managed service provider based in Little Rock, Arkansas, that provides a full suite of managed information technology (IT) services to User Organizations (Customers). Established in 1996, Mainstream began offering managed services in 2003 in response to Customer demand. Mainstream is a privately owned company providing services to Customers throughout the United States.

## Overview of Services

Mainstream provides full service IT support, managed hosting, managed virtual hosting, collocation, disaster recovery and software development services to Customers seeking to improve and secure their IT environments, while also decreasing costs. Mainstream delivers customized solutions for national and regional businesses through four distinct service lines:

- Managed Hosting, Managed Virtual Hosting and Collocation – Through its data center, Mainstream provides Customers managed hosting, managed virtual hosting and collocation services. These services provided by Mainstream include, but are not limited to:

  - Managed Hosting
    - ✓ Collocation services in addition to:
      - Server management and administration,
      - Hardware setup,
      - Patch management,
      - Backup management, and
      - System and network monitoring.
  - Managed Virtual Hosting
    - ✓ Shared, Mainstream provided hardware:
      - Secure virtual server provisioning,
      - Application hosting accessibility,
      - Server management and administration,
      - Patch management,
      - Backup management, and
      - System and network monitoring.
  - Collocation
    - ✓ Secured rack or cage storage within the data center,
    - ✓ Environmentally controlled and monitored areas,
    - ✓ Redundant power and data connectivity, and
    - ✓ Ad-hoc hourly "hands-on-site" IT support.

- GetITback Disaster Recovery – Service offering that provides remote business continuity and disaster recovery to Customers. The service offering includes:

  - File and system level off-site backup services,
  - Backup data set retention,
  - System state backups in conjunction with the Managed and Managed Virtual Hosting services, and
  - Secure transmission and storage of data.

- Full Service IT Support – Mainstream provides server, infrastructure, desktop and end user support services on-site and remotely to Customers. The support services include the assessment,

planning, implementation, monitoring and proactive maintenance of Customer systems by Mainstream personnel. This line of service is provided to ensure Customer maintained environments are configured to an acceptable standard while also supporting system availability.

- Software Solutions – Mainstream employs a staff of programmers and developers to provide its Customers technology environmental solutions that will improve the efficiency and effectiveness of their business. This line of service includes, but is not limited to the following solutions:

  - Custom Software Design and Development,
  - Business Process Analysis,
  - Sunset Application Support and,
  - Collaborative Chief Technology Officer.

## UCS Control Objective Summaries and Purposes

### UCS Objective 1: Provider Organization, Governance, Planning, and Risk Management

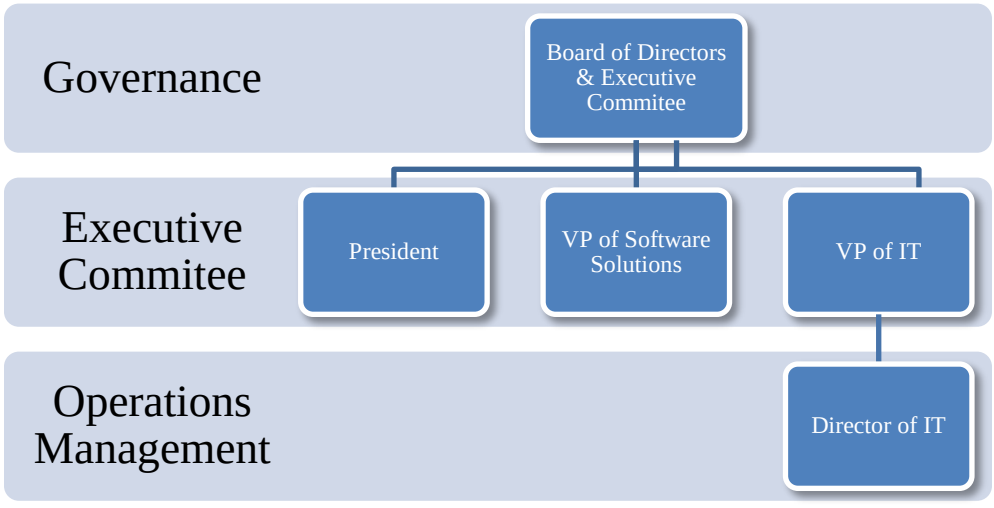
***UCS Objective Summary and Purpose:*** *The goal of the Provider Organization, Governance, Planning and Risk Management Objective is to provide assurance to the Customer that the provider has established a corporate and organizational structure designed to maximize efficiency, minimize risk, and provide sufficient oversight and accountability with regards to the services delivered.*

**Mainstream Organizational Reporting Structure**

The governance of Mainstream is the responsibility of the Board of Directors (Board) and the Executive Committee (EC). Membership of the Board consists of the members of the EC and an outside director. The Board meets monthly to review and approve internal financial statements and discuss both short- and long-term strategic plans and priorities.

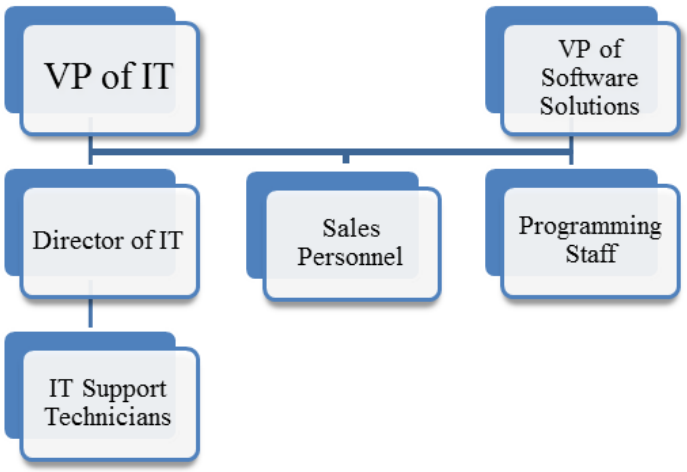
The EC is responsible for the daily operations and management of the organization. The EC consists of the President, Vice President (VP) of Software Solutions and VP of IT. The EC handles the oversight of operations management, the review and approval of policies and procedures, supervision of ongoing projects and discussion and resolution of current issues and events regarding Mainstream. See Figure 1 below for a summary of Mainstream's organizational governance.

***Figure 1 – Organizational Governance***



Mainstream's reporting hierarchy is organized and designed to segregate personnel and management by service line and organizational responsibility. Members of the EC are designated responsibility for specific functions and service lines within Mainstream. The President is responsible for marketing and overall supervision and management of Mainstream, while the VP of IT manages the Managed Hosting, Managed Virtual Hosting and Collocation, and Full Service IT service lines, and the VP of Software Solutions manages the Software Solutions service line. Sales for each area, IT and Software Solutions, report to those VPs, respectively. See Figure 2 below for the organizational management break down by service line.

***Figure 2 – Segregation of Duties and Management***




*Communication*

Mainstream has implemented various methods of communicating with employees, including, but not limited to, new hire training, management's continuous training of employees, employee handbooks, e-mail and voice messages to communicate time sensitive information and an Information Security Policy that communicates the formal policies and procedures of Mainstream. Management also conducts quarterly meetings with personnel to communicate important company announcements, discuss process improvement suggestions a000nd update personnel on the financial health of Mainstream.

## UCS Objective 2: Provider Policies and Procedures

***UCS Objective Summary and Purpose:*** *The purpose of the Provider Policies and Procedures Objective is to ensure that the Provider has documented the necessary policies and procedures in order to maintain effective data privacy, service delivery levels, as well as to minimize deviation from those established policies and procedures.*

### Mainstream Policies and Procedures

Mainstream maintains a documented Information Security Policy that identifies and addresses the following topics:

- Information Security Communication,
- Acceptable Use,
- Network Documentation,
- Logical Security,
- Service, Protocol and Port Documentation,

- Network Change and Configuration Testing/Approval,
- Network Perimeter Control Review,
- Anti-Virus,
- Security Patch Management Installation,
- Programming Change Control,
- Data Control and Access,
- Unique Identification (ID) and Authentication Methods,
- Proper Authentication and Password Management,
- Media Distribution and Classification,
- Security Log Review,
- Audit Trail History and Log Retention,
- Risk Assessment,
- Information Security Responsibility,
- Service Provider Management,
- Incident Response Plans,
- Security Awareness Program, and
- Physical Access Control.

Within the Information Security Policy topics listed above, specific procedures have been documented, approved and implemented to cover:

- Customer configuration management,
- Service level monitoring, and
- Incident and event management.

An Information Security Committee, consisting of select IT Support personnel and EC members, is charged with reviewing and updating the Information Security Policy quarterly.

**UCS Objective 3: Configuration and Program Change Management**

***UCS Objective Summary and Purpose:*** *The goal of the Configuration and Program Change Management Objective is to ensure the Provider has configuration change management documentation that is under formalized change controls. Such change management documentation may include, if applicable, capacity planning and modification to Provider and Customer configurations. Customer change management policies are documented based on the level of services delivered to the Customer by the Provider.*

**Mainstream Configuration Change Requirements**

Configuration data for managed service Customers is initially documented by IT Support personnel using a standardized information gathering form that is stored in a centralized folder on the Mainstream network. Sales tickets are submitted by sales personnel within the trouble ticketing system to initiate the new Customer configuration setup following the signing of an SLA. To ensure Customer tickets are clearly identified and pertinent Customer configuration data is documented, Customers are identified by name within the trouble ticketing system and the configuration documentation requirements vary by the level of managed services used by the Customer.

Modifications to initial SLAs are tracked within the trouble ticketing system to ensure Customer configuration data is updated in accordance with documentation requirements. Further, patch and update management services are provided to managed services Customers to ensure virtual and managed environments are updated with Mainstream tested and approved services. Planned changes and modifications to Customer environments are communicated to Customers prior to implementation for approval. Changes and modifications required to resolve outage situations are performed as needed and communicated to Customer for documentation purposes. Upon approval, tickets are generated within the

trouble ticketing system to track and monitor the Customer approval and documentation of the configuration changes.

Configuration data for new and existing Customers is analyzed by the Director of IT and IT Support personnel to ensure capacity needs for virtual and managed environments are monitored and achieved in accordance with SLA requirements.

**UCS Objective 4: Event Management**

***UCS Objective Summary and Purpose:*** *The goal of the Event Management Objective deals with how service organizations learn about and respond to IT related events that could impact services delivered to the Customer. In this section, the UCS covers Network Operations Center (NOC), Trouble Ticketing systems and Service Desk operations specifically related to event management policies and procedures.*

**Mainstream Event Management**

Incidents and events outside of normal operations that occur within the hosted and physical environments managed by Mainstream are logged and analyzed within the trouble ticketing system. Incidents and events can be submitted through an automated notification from a monitoring application, by a Customer via the ticketing system's web portal, or by a member of the IT Support Department following an alert or notification by the Customer or an ancillary application or system. Within the ticketing system, event and incident tickets are reviewed for impact and severity and prioritized appropriately to ensure the timely addressing and resolution of these instances.

Trouble tickets are monitored and analyzed by the IT Service Manager. Based on the categorization and analysis of outstanding and resolved tickets, the IT Service Manager is able to identify and correlate related incidents and events in an effort to standardize the resolution process and to implement processes or procedures to prevent the reoccurrence of the instance. Further, based on the Customer impact of the incident or event, the IT Service Manager will communicate the issues to the Director of IT and VP of IT and, if necessary, the Customer.

**UCS Objective 5: Logical Security**

***UCS Objective Summary and Purpose:*** *The goal of the Logical Security Objective is to ensure the Provider has taken the appropriate precautions to implement necessary controls in order to effectively govern access to Customer and other sensitive data, networks and systems that may compromise security of both the Provider and the Customer.*

**Mainstream Logical Security**

Mainstream's Information Security Policy defines the logical access control requirements for its internal network and in-scope applications.

These policies and procedures specifically define the following with regard to personnel access to the Mainstream network and managed service environments:

- Password length, complexity, expiration and reuse requirements,
- Security administration requirements,
- Network User ID requirements, and
- Mainstream domain and service support and monitoring applications access rights.

Access to the monitoring, management, and ticketing systems, as well as the domain Administrator IDs is restricted to the Director of IT and select IT Support personnel. EC and Software Solutions personnel do not have access to the managed service applications and limited access on the Mainstream domain.

Network vulnerability testing is completed on a quarterly basis by Mainstream.

## UCS Objective 6: Data Privacy, Security and Integrity

***UCS Objective Summary and Purpose:*** *The goal of the Data Privacy, Security and Integrity Objective is to ensure that Provider has sufficient policies and procedures operating effectively and being reviewed, updated, approved and communicated to Provider personnel annually. This includes data backup and retention policies (both for Provider and Customer data, if applicable), data security and privacy, including location of sensitive data, encryption of data, and management of third-party providers who have access to the data.*

### Mainstream's Data Privacy, Security and Integrity

*Customer Privacy and Confidentiality*
Mainstream relies on competent personnel with the necessary knowledge and experience to ensure services are provided to Customers effectively and efficiently, with an emphasis on the protection of Customer privacy and confidentiality. To support Mainstream's commitment to privacy and confidentiality, personnel are subject to background checks and must sign confidentiality/nondisclosure agreements during the new hire process.

*Data Backup and Integrity*
Mainstream has formal data backup and retention policies and procedures in place that define the backup and retention requirements of internal and managed data. Backup procedures are monitored with backup logs and notifications being monitored to ensure the complete and valid backup of data. Backup restoration testing and recovery procedures are conducted quarterly by IT Support personnel and monitored by the Director of IT. Mainstream has a HIPAA policy in place to define private and confidential information and how the information should be handled.

The GetITback Disaster Recovery services are implemented as a master grid of redundant processors and disk storage located at a third-party data center. The grid is accessible via the internal Mainstream network or authorized Customer accounts. Data is encrypted and compressed in transit and added to the grid. Data is transmitted between the data center and the Customer sites via static virtual private network (VPN) tunnels. Restoration of file and system level data is performed by IT Support personnel and monitored by the Director of IT.

Creation of new backup media was discontinued during the period of review with the transition to virtual storage systems for system backups. Remaining archival backup media is stored in a secure, off-site warehouse by an independent third party in accordance with Mainstream data retention policies.

## UCS Objective 7: Physical and Environmental Security

***UCS Objective Summary and Purpose:*** *The goal of the Physical and Environment Security Objective is to ensure the Provider has documented policies governing physical access to the Provider's assets, including visitor/guest logs at applicable facilities. Provider must demonstrate sufficient physical security controls at each facility, including controls such as card key, CCTV, on-site security and other effective security controls. The Provider also has documented controls governing terminated and/or employees changing positions and their access to Provider and/or Customer facilities.*

### Mainstream Physical and Environmental Security Controls

Mainstream operates a hardened and conditioned data center with a separate Network Operations Center (NOC). Both the data center and NOC are located in Mainstream's corporate office in Little Rock, Arkansas. The NOC is utilized during emergency situations to monitor and access systems and data located within the data center. Mainstream does not house Customer systems or data within the NOC.

Access to the Mainstream corporate office is secured by an access security system with proximity badge controllers restricting access into the exterior entrances of the building outside of business hours and with proximity badge and biometric reader controllers on the entrances to the Mainstream offices. The access security system allows Mainstream to control access to the building, office area and data center based on the badge holder's assigned access rights. During regular business hours, access to the building housing the corporate offices and data center is unrestricted, with access to the office area restricted to Mainstream personnel.

After-hours access to the building is restricted to authorized cardholders, with access being monitored by an independent security firm. The data center is physically split into two separately secured areas; the "escorted" area, which houses Mainstream's Virtual hosting environment, certain collocated Customer environments and all ISP connections, and the "24x7" area, which houses certain collocated Customer environments contained in individually secured cabinets or secured suites of cabinets. Access to the escorted area of the data center is restricted at all times to a restricted number of authorized Mainstream personnel. Access to the 24x7 area of the data center is restricted at all times to a restricted number of authorized Mainstream personnel plus approved and individually designated representatives of the Customers occupying the 24x7 area, who are provided with proximity badges and who access the 24x7 area via entrances to the building and data center restricted by biometric reader controllers.

Mainstream has implemented the following controls to ensure the corporate offices (including the data center and NOC) are physically secured:

- Proximity badge and biometric security controls on corporate office entrances,
- Proximity badge on internal data center entrances,
- Intrusion detection system, and
- Security cameras with DVR covering all external entrances, internal entrances and throughout the data center.

Visitor access to the Mainstream office and data center is restricted at all times. Access to collocation cages and areas are restricted to Customer approved individuals. A visitor log is maintained by the receptionist for all visitors to the Mainstream office. Visitors to the escorted area of the data center are required to be escorted at all times by either the VP of IT, Director of IT or Mainstream IT Support personnel. Access to the 24x7 area of the data center by Customer approved individuals is logged in access security system and recorded to DVR via security cameras.

Mainstream has implemented the following environmental controls to ensure availability for its hosted and collocation Customers:

- Uninterruptible Power Supply (UPS),
- Backup diesel generator,
- Raised flooring,
- Redundant HVAC cooling and humidity control air units,
- Constant air filtration units,
- Nonsprinkled fire suppression (FM-200),
- Fiber Data Connection with capacity, and
- VLAN support with network bandwidth rate control.

Maintenance contracts and equipment warranties are in place to ensure the reliability of environmental controls. Environmental conditions within the data center are continuously monitored by the IT Director and IT Support personnel through automated notifications and warnings.

## UCS Objective 8: Service Level Agreements, Customer Reporting and Billing

***UCS Objective Summary and Purpose:*** *The purpose of the Customer Reporting and Billing Objective is to ensure the Provider is accurately monitoring, reporting, and issuing reports and invoices to Customers in accordance with the SLAs signed by both parties.*

### Mainstream Service Level Agreements, Customer Reporting and Billing Controls

Mainstream provides services to Customers through signed SLAs. The SLA utilized by Mainstream was developed and approved by the EC and reviewed by outside legal counsel. Customer SLAs must be signed by both Mainstream and Customer representatives prior to services being rendered. Modifications to the terms of a Customer's SLA are handled via signed addendums.

Customers are invoiced for the services rendered by Mainstream in accordance to signed SLAs. Time spent by IT Support personnel to support Customers outside of the terms of the SLA is retrieved from the Time Entry application and uploaded into the ticketing system for invoicing. Invoicing is performed by an independent bookkeeping firm, with invoices being reviewed for adherence to the terms of the SLA by the VP of IT prior to issuance. Customer issues or questions regarding the services provided by Mainstream are addressed and resolved by either the responsible sales representative or the VP of IT.

## UCS Objective 9: Corporate Health

***UCS Objective Summary and Purpose:*** *The purpose of the Corporate Health Objective is to ensure sufficient corporate and financial health on the part of the Provider so that all of its Customers are adequately protected. Technical proficiency is only part of the Provider's value to the Customer. The Provider must be on firm financial footing, as well as risk averse in a variety of areas unique to managed services and cloud in order to effectively deliver its services to the Customer.*

### Mainstream Corporate Health

Mainstream was incorporated in 1996 in Arkansas and is managed by the by-laws and articles of the corporation. The organization has been in business over 18 years. During the 18 years of operation, there has been limited turnover on the Board and EC.

Mainstream's business model and operations have been carefully implemented and managed to ensure financial stability while providing outstanding service to its Customers. To obtain this stability, Mainstream has a revenue stream that is diversified across its service lines to a base of long-term customers while also being refreshed with new Customers. This diversity ensures that the majority of revenue is not tied to one particular Client or a small concentration of Customers. Further, the majority of revenue is generated from Customers of SLAs that cover multi-year service terms with minimal utilization of month-to-month SLAs.

# Unified Certification Standard for Cloud and Managed Service Providers: Controls and Guidelines

## Overview

The following control objectives are used by the independent accounting firm to perform the necessary testing to issue a report on the MSP, Cloud, or hosting service provider seeking certification. In addition to being used by the independent examiner, these controls can be used by the Service Provider to anticipate specific documentation and testing requirements that will likely arise during the examination process.[1]

## Level 1 Certification

The Unified Certification Standard (UCS) for Cloud and Managed Service Providers, Level 1 Certification provides service providers, end-user organizations, and external examiners, with a public report that has a wide range of information about the service provider without compromising the security and/or integrity of the organization.

The UCS Level 1 report provides readers with assurance that "as of" a specific date, the necessary controls have been observed to be in place and operating effectively by the independent examiner.

## Level 2 Certification

The Unified Certification Standard (UCS) for Cloud and Managed Service Providers, Level 2 Certification provides service providers, end-user organizations, and external examiners, with a public report that has a wide range of information about the service provider without compromising the security and/or integrity of the organization.

The UCS Level 2 report provides readers with assurance that over a minimum period of at least 90 days, the necessary controls have been observed to be in place and operating effectively by the independent examiner. This report offers greater assurance than a Level 1 report since the independent examiner or must ensure that the applicable controls have not only been established but have been in place for the 90 day period of time.

[1] In the event that a particular control objective does not apply to a Service Provider's business model, and if the independent examiner and the MSPAlliance both agree that the control objective does not negatively impact the Service Provider's ability to safely deliver their services to the end-user, the independent examiner may decide to perform the examination without applying that particular control objective.

## UCS Process

Step 1) Service Provider completes the application

Step 2) Service Provider is given a UCS data gathering document listing the controls and control objectives that will be examined.

Step 3) MSPAlliance schedules a series of calls to assist the Service Provider in completing the UCS data gathering form. MSPAlliance will assist service provider in UCS preparation and documentation (i.e., description of the Service Delivery environment)

Step 4) UCS data gathering document is reviewed by MSPAlliance and the independent examiner. At this time, additional information may be requested from the service provider.

Step 5) Level 2 - Independent examiner will visit the service provider's physical locations to perform on-site testing of the applicable controls[2]. The independent examiner will perform testing to ensure that the applicable controls are in place and have been operating effectively for the necessary period of time.

Step 6) Independent examiner will issue a report containing their findings to the MSPAlliance.

Step 7) MSPAlliance will issue the UCS Certification, along with the report, to the Service Provider.

## UCS Control Objectives Summaries and Purpose

## UCS Objective 1: Provider Organization, Governance, Planning, and Risk Management

***UCS Objective Summary and Purpose:*** *The goal of the Provider Organization, Governance, Planning and Risk Management Objective is to provide assurance to the Customer that the provider has established a corporate and organizational structure designed to maximize efficiency, minimize risk, and provide sufficient oversight and accountability with regards to the services delivered.*

[2] In some instances, the independent examiner may request physical access to (or documentation) locations that are not within the control of the service provider. For example, data centers, third-party NOCs, or help desk centers, etc.

## UCS Objective 2: Provider Policies and Procedures

***UCS Objective Summary and Purpose:*** *The purpose of the Provider Policies and Procedures Objective is to ensure that the Provider has documented the necessary policies and procedures in order to maintain effective data privacy, service delivery levels, as well as to minimize deviation from those established policies and procedures.*

## UCS Objective 3: Configuration and Program Change Management

***UCS Objective Summary and Purpose:*** *The goal of the Configuration and Program Change Management Objective is to ensure the Provider has configuration change management documentation that is under formalized change controls. Such change management documentation may include, if applicable, capacity planning and modification to Provider and Customer configurations. Customer change management policies are documented based on the level of services delivered to the Customer by the Provider.*

## UCS Objective 4: Event Management

***UCS Objective Summary and Purpose:*** *The goal of the Event Management Objective deals with how service organizations learn about and respond to IT related events that could impact services delivered to the Customer. In this section, the UCS covers Network Operations Center (NOC), Trouble Ticketing systems and Service Desk operations specifically related to event management policies and procedures.*

## UCS Objective 5: Logical Security

***UCS Objective Summary and Purpose:*** *The goal of the Logical Security Objective is to ensure the Provider has taken the appropriate precautions to implement necessary controls in order to effectively govern access to Customer and other sensitive data, networks and systems that may compromise security of both the Provider and the Customer.*

## UCS Objective 6: Data Privacy, Security and Integrity

***UCS Objective Summary and Purpose:*** *The goal of the Data Privacy, Security and Integrity Objective is to ensure that Provider has sufficient policies and procedures operating effectively and being reviewed, updated, approved and communicated to Provider personnel annually. This includes data backup and retention policies (both for Provider and Customer data, if applicable), data security and privacy, including location of sensitive data, encryption of data, and management of third-party providers who have access to the data.*

## UCS Objective 7: Physical and Environmental Security

***UCS Objective Summary and Purpose:*** *The goal of the Physical and Environment Security Objective is to ensure the Provider has documented policies governing physical access to the Provider's assets, including visitor/guest logs at applicable facilities. Provider must demonstrate sufficient physical security controls at each facility, including controls such as card key, CCTV, on-site security and other effective security controls. The Provider also has documented controls governing terminated and/or employees changing positions and their access to Provider and/or Customer facilities.*

## UCS Objective 8: Service Level Agreements, Customer Reporting and Billing

***UCS Objective Summary and Purpose:*** *The purpose of the Service Level Agreements, Customer Reporting and Billing Objective is to ensure the Provider is accurately monitoring, reporting, and issuing reports and invoices to Customers in accordance with the SLAs signed by both parties.*

## UCS Objective 9: Corporate Health

***UCS Objective Summary and Purpose:*** *The purpose of the Corporate Health Objective is to ensure sufficient corporate and financial health on the part of the Provider so that all of its Customers are adequately protected. Technical proficiency is only part of the Provider's value to the Customer. The Provider must be on firm financial footing, as well as risk averse in a variety of areas unique to managed services and cloud in order to effectively deliver its services to the Customer.*