Unified Certification Standard for Cloud and Managed Service Providers® 3.0 (UCS)

Domains, Objectives and Requirements

Overview

The following UCS (Unified Certification Standard) Domains, Objectives and underlying Requirements will be used by the independent auditor to perform the necessary verification procedures to issue a report on the MSP/Cloud organization seeking certification. In addition to being used by the independent auditor, these requirements can be used by the MSP to anticipate specific documentation and verification requirements that will likely arise during the examination process. In the context of the UCS requirement text an **organization** is the Company seeking certification. The organization is referred to as Organization Seeking Certification or (OSC)

This version of the UCS became effective on November 1st, 2024.

UCS Domains

The UCS is divided into five Domains: Expertise, Trust, Security, Resilience, and Transparency. These Domains are a collection of ten Objectives working in unison to create a framework that ensures MSP/Cloud organizations comply with rigorous standards. Each Domain includes specific Objectives and Requirements that need to be fulfilled to obtain certification. Achieving certification under the UCS demonstrates a commitment to excellence and a dedication to upholding the highest industry standards. Each of these Domains is designed to ensure that the organization maintains a high standard of service, trust, and reliability.

Service Providers using an MSP

While originally designed for MSPs and Cloud service providers, the UCS can also be extended to the Customers of a certified Organization in a shared responsibility matrix. This matrix ensures that the majority of services provided by the customer rely heavily on either an MSP, MSSP, or Cloud service provider to manage their IT infrastructure. By leveraging a suite of SaaS or Cloud-hosted tools, these service providers offer comprehensive solutions that cater to the specific needs of their clients.
The UCS framework helps these certified organizations maintain high standards in service delivery, trust, and reliability, thereby creating a harmonious relationship between the service providers and their customers. This shared responsibility approach allows customers to benefit from cutting-edge technology and expert management without the burden of maintaining the infrastructure themselves. As a result, customers can focus on their core business activities while ensuring that their IT systems are robust, secure, and resilient. The UCS certification demonstrates the organization's commitment to excellence and adherence to rigorous industry standards. This ensures that both the service providers and their customers are aligned in their goals and expectations, fostering a collaborative environment that promotes innovation and continuous improvement. The UCS Domains of Expertise, Trust, Security, Resilience, and Transparency collectively contribute to this dynamic partnership, ultimately driving growth and success for all parties involved.

Expertise

This domain involves an OSC's capacity to proactively manage their scope of services within an organization. An OSC that demonstrates proficiency in the Expertise domain will understand the client's business model and provide technical solutions tailored to the client's specific requirements. Effective strategic planning and software management are crucial to any organization's success. By developing and communicating clear strategic plans and priorities, companies can prevent scope creep and avoid unprofitable and unsustainable revenue channels. Managing legal and financial risks associated with software audits or third-party intellectual property claims requires maintaining an inventory of in-scope SaaS vendors. Configuration data for managed or monitored objects should be documented before management begins, ensuring that modifications are evaluated and approved by the customer. This guarantees that changes are updated systematically following implementation to reflect the current customer configuration. Vendor-supplied software and hardware patches must be applied following standardized procedures, with non-critical patches evaluated for issues before release and critical patches applied promptly. Application changes to information systems should follow a formal process, including requesting, logging, approval, testing, and acceptance before implementation in production environments. The secure monitoring and management of organization and customer managed environments are ensured through the effective use of the operations center.

Periodic internal reviews of tickets and operational events, coupled with continual upper management assessments of resource access, help maintain appropriate restrictions to authorized personnel. Regular backup data restoration and recovery testing procedures, with results logged and monitored, are vital for ensuring data integrity. The presence of signed Master Service Level Agreements (MSA) between organizations and customers, along with financial reports demonstrating profitability or access to necessary funds for operation, is essential for business stability. Tracking the retention of customers and employees guarantees business continuity, further solidifying the organization's flexibility and long-term success. The Expertise domain ensures that OSCs maintain high standards in service delivery, trust, and reliability. This fosters a collaborative environment that promotes innovation and continuous improvement, driving growth and success for all parties involved.

ID	Title	Description
01.02	Strategic Planning	Strategic plans and priorities have been developed and communicated to the management of the company.
01.04	Software Management	Process for managing and determining legal and financial risk of software audits or third-party intellectual property claims. Inventory of in scope SaaS vendors is maintained.
04.01	Configuration Documentation	Configuration data for objects managed or monitored is documented based on level of service before management of the object.
04.04	Customer Change Tracking	Modifications to Customer object configurations are documented to ensure changes are evaluated and approved by the Customer before implementation. Configuration data is updated following implementation to reflect the current Customer configuration.
04.06	Patch Management	Vendor-supplied software and hardware patches are applied to managed objects and environments following standardized procedures. Non-critical patches are evaluated

		for issues before release and applied during planned or accepted maintenance windows. Critical patches are applied as soon as possible.
04.07	SaaS Special Requirement: Application Development Procedures	Application Changes to information systems follow a formal process that requires the requesting, logging, approval, testing, and acceptance of changes before being implemented into production.
05.01	Centralized Operations Center	MSOC/NOC/SOC is used to provide effective and secure monitoring and management of Organization and Customer managed environments.
05.05	Operations Monitoring	Organization management performs a periodic internal review of tickets and operational events.
06.07	Continuous Review of Access Rights	Access to information systems, as well as the underlying customer systems and data, is continually reviewed by the Organization's upper management to ensure that resource access is appropriately restricted to authorized personnel.
07.03	Data Recovery Testing	Backup data restoration and recovery testing procedures are conducted periodically, with the results of tests being logged and monitored by the Organization.
09.01	Signed Contracts and Agreements	Signed Master Service Level Agreements (MSA) are in place between the Organization and Customers.
10.01	Operational Sustainability	Financial reports demonstrate profitability of a minimum of 6 of the previous 12 months, or sufficient access to funds necessary to keep the Organization operational for a 12-month period of time.
10.06	Customer and Employee Retention Tracking	The Organization maintains records to track the retention of customers (both voluntary and involuntary) and employees (both voluntary and involuntary) to ensure business continuity.

Trust

Trust is essential in the relationship between the organization and its customers. This domain evaluates the measures in place to ensure the integrity and reliability of services provided. The goal of the MSP is to become a trusted partner for their customers by advising them on technical solutions while also understanding their unique environments and suggesting improvements to their technology stack. The Trust domain illustrates how they can achieve this role. The trusted partner will conduct internal audits at planned intervals to provide information on whether internal systems meet control criteria and implement documented policies for the safe transfer of IT management to another provider, including signed agreements for transition services.

Through the UCS, the OSC monitors the capacity of managed objects and environments, managing and proactively planning capacity requirements either internally or with the customer. A problem management system ensures operational events that are not part of the organization's standard operations are recorded, analyzed, and resolved in a timely manner. Problems and incidents are categorized to allow for event correlation and eliminate false positives, ensuring proper resolution and

documentation. Resolutions are reported to both organization and customer management. Trust is earned, not given, so the OSC will track and monitor remote access to customer information systems. The OSC manages this process by restricting access using a VPN or Zero Trust Network Access (ZTNA) configurations. Remote access is monitored, logged, and reviewed following a Remote Access Policy to ensure systematic operations during each connection. Environmental safeguards in NOCs and/or data centers protect against disruptive events, and environmental and maintenance services are performed and tested regularly following a standardized and documented process. Physical access to collocation hardware maintained in facilities is restricted to individuals designated by the customer and authorized organization personnel.

The OSC provides reporting metrics to customers following signed contracts and demonstrates that a sustainable gross profit margin is realized on managed service/cloud offerings. Additionally, the organization shows that most of its customers and revenue come from relationships that last at least a year or longer. Finally, the organization maintains errors and omissions, professional liability, cyber security, and any other applicable insurance policies necessary to mitigate against business disruption. Trust is the cornerstone of any successful relationship between an organization and its customers. Through systematic processes such as internal audits, capacity management, problem resolution, and secure remote access, the OSC can effectively demonstrate their reliability and integrity. By adhering to standardized policies and maintaining robust insurance coverage, the OSC ensures continuity and safeguards against disruptions. Ultimately, it is the commitment to continuous improvement and adherence to standards that solidifies the OSC's role as a trusted partner, fostering long-term relationships and sustainable growth.

ID	Title	Description
02.04	Internal Audit	Conduct internal audits at planned intervals to provide information on whether internal systems are meeting control criteria.
02.08	Service Transition Continuity	Documented policy containing procedures for effectuating the safe transfer of IT management to another provider. Uses signed agreements with specific provisions for addressing transition services.
04.05	Capacity Planning	Monitors the capacity of managed objects and environments. Manages and proactively plans capacity requirements internally or with the Customer.
05.02	Support and Problem Logging	A problem management system (help desk / ticketing system) has been implemented to ensure that operational events that are not part of the Organization’s standard operations are recorded, analyzed and resolved in a timely manner.
05.03	Categorization and Correlation	Problem/incident documentation is categorized to allow for event correlation and the elimination of false positives.
05.04	Support and Problem Resolution	Problems and/or incidents identified in the Customer’s environment are properly resolved and documented. Resolution is reported to both Organization and Customer management.
06.08	Restricted Secure Remote	Remote access to information systems is protected by

	Access	restricting access using a VPN or Zero Trust Network Access (ZTNA) configuration. Remote access is monitored, logged, and reviewed following a Remote Access Policy.
08.05	Data Center Environmental Controls	Environmental safeguards in NOC(s) and/or data center(s) to protect from disruptive events.
08.06	Data Center Maintenance	Environmental and maintenance services are performed and tested regularly following a standardized and documented process.
08.07	Data Center Colocation	Physical access to collocation hardware maintained in facilities is restricted to individuals designated by the Customer and authorized Organization personnel.
09.03	Report Availability	Reporting metrics are available to Customers following signed contracts.
10.03	Sustainable Profit Margin on Services	Demonstrates that a sustainable gross profit margin is realized on managed service/cloud offerings.
10.04	Customer Commitments	The Organization shows that most of its customers and revenue come from relationships that last at least a year or longer.
10.05	Insurance	Maintains errors and omissions, professional liability, cyber security and any other applicable insurance policies necessary to mitigate against business disruption.

Resilience

This domain assesses the organization's resilience to disruptions, emphasizing risk management and business continuity. It includes a formal management structure with executive oversight and a comprehensive risk management strategy. The OSC formally documents its policies to ensure resilience and address incident responses for data breaches, ransomware, and cyber-attacks. Employees of the MSP undergo rigorous onboarding processes, receive regular cybersecurity training, and must comply with confidentiality, privacy, and security standards. Management conducts background checks, requires signed confidentiality agreements, and tracks application versions.

The UCS values employees as a key asset but notes that improper onboarding can cause harm. To ensure security, access to information systems is separated by functional area, provisioned, elevated, and revoked systematically. This approach maintains real-time security and traceability in case of incidents.

Data backup schedules provide continuous protection, and business continuity plans are thoroughly documented and regularly tested to ensure effectiveness. Employee access to facilities is systematically revoked upon termination to prevent unauthorized entry and safeguard sensitive information. Overall, the organization showcases a robust framework for resilience by implementing rigorous risk management strategies and comprehensive data protection measures, ensuring resilience and safeguarding data integrity. This proactive approach not only mitigates potential disruptions but also fortifies the organization's ability to respond swiftly and effectively to various incidents, thereby maintaining operational continuity and security.

ID	Policy/Procedure	Description
01.01	Organizational Structure	Formal management structure with executive steering committee/board of directors responsible for management and supervision.
01.03	Risk Management	A risk management strategy is established by the organization. Risks are logged and communicated to management to ensure adequate and timely analysis. A risk treatment strategy is in place and followed.
02.02	Incident Response Policies and Procedures	Incident Response policy documented; addresses data breaches, ransomware payments, and cyber-attacks.
02.06	Training and Orientation	Orientation/training and continuing education programs for ethical, integrity, confidentiality, privacy, security, and acceptable use standards.
02.07	Security Awareness Training	Employees receive essential cybersecurity and information security training.
03.01	Employee Background Checks	Background checks conducted on personnel following policies and procedures.
03.02	Employee Confidentiality and Privacy Acceptance	Employees sign and attest to understanding and adherence to confidentiality and privacy policies.
04.08	SaaS Special Requirement: Version Tracking and Code Maintenance	The Organization has a process for tracking application versions.
04.09	SaaS Special Requirement: Development Segregation of Duties	Segregation of duties exists between the development and promotion of application changes to the production environment.
06.04	Revocation of Access	Logical access to information systems and Customer systems/data revoked for terminated and departing employees.
06.06	Segregation of Access	Access to information systems separated by functional area to ensure segregation of duties.
07.01	Customer Data Backup and Replication	Customer data backup schedules documented and followed; backups monitored and errors handled; data encrypted.
07.02	Organization Data Backup and Replication	Organization data backups completed and monitored; errors handled; data encrypted.
07.04	Disaster and Business Continuity Planning	Business continuity plans documented and tested periodically to ensure data integrity.
08.04	Revocation of Physical Access	Upon termination, employee access to facilities is revoked.

Transparency

Transparency is an essential pillar of the organization's commitment to its customers and stakeholders. The UCS sets forth guidelines that underscore the importance of clear communication and openness. Adhering to these standards, the organization strives to provide accurate and timely information regarding its services and performance. This approach not only builds trust but also fortifies relationships, fostering an environment where customers and employees feel valued and informed.

Documenting policies and procedures is crucial for guiding daily operations and preparing the OSC to withstand any disruptions. The UCS mandates that these documents be reviewed and updated annually, ensuring they reflect the current operational landscape and regulatory requirements. Employees are required to sign and attest to their understanding and adherence to these policies, reinforcing the organization's dedication to maintaining a high standard of operational integrity as prescribed by UCS.

The OSC has implemented comprehensive policies to govern the identification, disclosure, and management of data geolocation, both internally and through external service providers, in line with UCS standards. Service levels are accurately categorized, and invoices are generated in alignment with signed Master Service Level Agreement contracts. The OSC finishes this practice domain with financial transparency, achieved through strategic revenue distribution management. The organization ensures a balanced income from its customers, thereby safeguarding financial stability and promoting sustainable growth. This comprehensive framework, adhering to UCS guidelines, supports the organization's long-term objectives.

ID	Title	Description
02.01	Documentation of Policies and Procedures	Policies and procedures formally documented to guide daily operations. The sequence of employee onboarding and org layout will contribute to the ability for the MSP to withstand any disruptions
02.03	Periodic Review and Approval	Policies and procedures reviewed and updated annually for approval and implementation. The sequence of employee onboarding and org layout will contribute to the ability for the MSP to withstand any disruptions
02.05	Employee Acceptance	Employees sign and attest to understanding and adherence to policies and procedures. The sequence of employee onboarding and org layout will contribute to the ability for the MSP to withstand any disruptions
03.04	Organization Data Geolocation Disclosure	Policies and procedures are implemented to govern the identification and disclosure of the geolocation of managed data.
03.05	External Service Provider Geolocation Disclosure	Policies and procedures are implemented to govern the identification and geolocation disclosure of external service provider managed data.
03.07	External Service Provider Access Disclosure	Policies and procedures have been implemented to govern the communication and disclosure of external service provider access to Customer information systems and data.
04.02	Service Level Categorization	Service levels are adequately categorized and identified within Organizational systems.

09.02	Accuracy of Service Invoices	Organization invoices are generated following signed Master Service Level Agreement contracts.
10.02	Significant Customer Risk	The Organization demonstrates sufficient managed services revenue distribution so that the largest Customer does not represent more than 20% of total managed services revenue and the five largest Customers do not represent more than 50% of total managed services revenue.

Security

Security is a cornerstone of UCS operations. External service providers for cloud and managed services are carefully evaluated and approved by designated employees. Confidential or private internal or customer data is encrypted, and where encryption is unavailable, other security practices safeguard the data. This rigorous approach ensures that sensitive information is protected from unauthorized access and potential threats.

Access by external providers to organizational and customer systems is strictly controlled, monitored, and documented. This access is limited to necessary occasions and follows documented policies and procedures. Additionally, changes to internal configurations are documented, ensuring that they are requested, reviewed, and approved through a consistent process. Access control policies restrict system access to authorized personnel, utilizing unique IDs and passwords, which are stored securely. Administrator IDs for critical systems are limited to a few approved personnel, ensuring that access to sensitive information is tightly controlled. Networks are fortified by leveraging a suite of threat management tools. Email and environments are scanned for malware, and EDR systems protect network devices, ensuring that the organization's information systems remain secure. The wireless network is segregated, keeping organizational and guest networks separate to enhance security. Physical security at work locations includes periodic reviews of access rights, visitor logs, and restricted access to sensitive areas such as operations centers, data centers, and server rooms. Visitor logs are maintained at each facility, with visitors required to sign upon entry. Physical access to sensitive areas is restricted to authorized personnel, ensuring that only those with proper clearance can enter.

The UCS demonstrates a robust commitment to operational sustainability and customer protection through comprehensive security measures, including stringent access control, encryption, network security, and physical security protocols. These measures reflect OSC's dedication to safeguarding data, resources, and environments from potential threats, ensuring a secure and reliable operational framework.

Code	Title	Description
01.05	External Service Provider Management	External service providers (contractors, third-parties, vendors) utilized by the Organization for delivery of cloud and/or managed services are evaluated and approved by a designated employee.
03.03	Data Classification, Data Protection and Encryption	Internal or Customer data classified as confidential or private is encrypted following applicable industry best practices or regulations. Where encryption is not available, inherent information security practices are in place to protect internal

		and customer data.
03.06	External Service Provider Management	External service providers only monitor or gain access to Organizations and Customers' information systems only when needed. This access is monitored, logged, and reviewed according to documented policies and procedures.
04.03	Internal Change Tracking	Modifications to internal object configurations are documented to ensure changes are requested, reviewed, and approved following a consistent process.
06.01	Controlled Access to Applications and Environments	Access to Organization and Customer systems and configuration data is restricted to authorized personnel following a documented Access Control Policy. All critical service delivery and internal applications have centralized access control mechanisms implemented.
06.02	Super-User and Administrator Access Security	Administrator IDs to information systems (network and in-scope critical systems) are restricted to a limited number of approved personnel.
06.03	Unique Users and Passwords	Users authenticate to Organizational information systems and the underlying Customer data using unique user account IDs and passwords.
06.05	Strong Passwords	User authentication password mechanisms are implemented and require minimum standards for password length, complexity, expiration, reuse, and account lockout for failed attempts. Organization passwords are stored in a secure password repository.
06.09	Network and Endpoint Security Management and Monitoring	Local and wide area networks are secured through the use of managed firewalls and other devices and software. Where applicable, MDR/EDR/XDR controls and security information and event management (SIEM) systems are utilized to monitor and secure the Organization’s network.
06.10	Email Security	The Organization has implemented applications and/or systems to scan and protect email and environments from email attacks and malware/viruses.
06.11	Network and Endpoint Protection	Organization has implemented an EDR (Endpoint Detection and Response) system on the network’s connected devices and traffic (web and email) to scan and protect its environment.
06.12	Wireless Network Security	The Organization's wireless network is segregated from its guest wireless network.
06.13	Network Security Review	Network security reviews (including security assessments, scans, penetration tests, etc.) of the Organization’s network are conducted periodically.
06.14	System Logging	The Organization has a formal process for tracking, retaining and reviewing audit logs.
07.05	Internal Data Destruction	Objects containing internal data are handled and destroyed following end-of-life policies.
07.06	Customer Data Destruction	If data destruction services are delivered to Customers,

		objects containing Customer data are handled and destroyed following end-of-life policies.
07.07	Asset and Device Management	Assets and devices are maintained in a centralized inventory list. A device management policy and supporting security measures shall be adopted to manage the risks of all devices and assets. The Organization is using an active discovery tool when managing customer assets.
08.01	Organizational Physical Security	Physical security controls are implemented by the Organization with respect to all work locations. Access rights of personnel are reviewed and approved by Organization upper management on a periodic basis.
08.02	Logging of Visitors	Visitor logs are maintained at each facility by the Organization. Visitors are required to sign the log upon entering the building.
08.03	Sensitive Area Security	Physical access to the sensitive areas (including operations centers, data centers, and server rooms) is restricted to authorized personnel.

UCS Objective 1: Governance

UCS Objective Summary and Purpose: *The goal of the Governance Objective is to provide assurance to the Customer that the Organization has established a corporate structure designed to maximize efficiency, minimize risk, provide sufficient oversight and accountability with regard to the services delivered. This objective also addresses external service provider management protocols of the Organization.*

01.01 Organizational Structure – The Organization has a formal management structure, with an executive steering committee/board of directors responsible for the management and supervision of the company.

01.02 Strategic Planning – Strategic plans and priorities have been developed and communicated to the management of the company.

01.03 Risk Management – A risk management strategy is established by the organization. Risks are logged and communicated to management to ensure adequate and timely analysis. A risk treatment strategy is in place and followed.

01.04 Software Management – For infrastructure, platform, or software as a service being delivered, the Organization has a process for managing and determining their legal and financial risk of software audits or third-party intellectual property claims. An inventory of in scope SaaS vendors is maintained by the organization.

01.05 External Service Provider Management – External service providers (contractors, third-parties, vendors) utilized by the Organization for delivery of cloud and/or managed services are evaluated and approved by a designated employee.

UCS Objective 2: Policies and Procedures

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

02.01 Documentation of Policies and Procedures – Policies and procedures have been formally documented to guide the daily operations of the Organization.

02.02 Incident Response Policies and Procedures – An Incident Response policy has been formally documented. Policies and procedures to address data breaches, ransomware payments, and cyber-attacks impacting the daily operations of the Organization are established and tested, and if applicable, it's Customers.

02.03 Periodic Review and Approval – Policies and procedures are reviewed and updated at least annually to ensure any modifications are approved and implemented.

02.04 Internal Audit – The Organization shall conduct internal audits at planned intervals to provide information on whether their internal systems are meeting their control criteria.

02.05 Employee Acceptance – Employees are required to sign and attest to their understanding and adherence to Organizational policies and procedures.

02.06 Training and Orientation – New employee orientation/training and continuing education programs for existing employees are implemented to address the ethical, integrity, confidentiality, privacy, security, and acceptable use standards developed by the Organization.

02.07 Security Awareness Training – Organization employees receive essential cybersecurity and information security training.

02.08 Service Transition Continuity – The Organization has a documented policy containing procedures for effectuating the safe transfer of IT management to another provider. The Organization uses signed agreements which contain specific provisions for addressing transition services in situations where the client is changing providers.

UCS Objective 3: Confidentiality, Privacy and Service Transparency

UCS Objective Summary and Purpose: *The goal of the Confidentiality and Privacy Objective is to ensure the Organization has sufficient policies and procedures related to the protection and disclosure of Customer data, specifically protocols safeguarding confidentiality, privacy, geolocation of managed data (including external service provider managed data) and identification of applications utilized to deliver services.*

03.01 Employee Background Checks – Background checks are conducted on personnel following Organization policies and procedures.

03.02 Employee Confidentiality and Privacy Acceptance – Employees are required to sign and attest to their understanding and adherence to Organizational confidentiality and privacy policies.

03.03 Data Classification, Data Protection and Encryption – Internal or Customer data classified as confidential or private is encrypted following applicable industry best practices or regulations. Where encryption is not available, inherent information security practices are in place to protect internal and customer data.

03.04 Organization Data Geolocation Disclosure – Policies and procedures are implemented to govern the identification and disclosure of the geolocation of managed data.

03.05 External Service Provider Geolocation Disclosure – Policies and procedures are implemented to govern the identification and geolocation disclosure of external service provider managed data.

03.06 External Service Provider Management – External service providers only monitor or gain access to Organizations and Customers' information systems only when needed. This access is monitored, logged, and reviewed according to documented policies and procedures.

03.07 External Service Provider Access Disclosure – Policies and procedures have been implemented to govern the communication and disclosure of external service provider access to Customer information systems and data.

UCS Objective 4: Change Management

UCS Objective Summary and Purpose: *The goal of the Change Management Objective is to ensure the Organization has formalized change management policies and procedures that may include, if applicable, the modification of Organization and Customer configurations, capacity planning and patch management. Customer change management policies are documented based on the level of services delivered to the Customer by the Organization.*

04.01 Configuration Documentation – Configuration data for objects managed or monitored is documented based on level of service before management of the object.

04.02 Service Level Categorization – Service levels are adequately categorized and identified within Organizational systems.

04.03 Internal Change Tracking – Modifications to internal object configurations are documented to ensure changes are requested, reviewed, and approved following a consistent process.

04.04 Customer Change Tracking – Modifications to Customer object configurations are documented to ensure changes are evaluated and approved by the Customer before implementation. Configuration data is updated following implementation to reflect the current Customer configuration.

04.05 Capacity Planning – The Organization monitors the capacity of managed objects and environments. If applicable, the Organization manages and proactively plans (both internally or with the Customer) and prioritizes capacity requirements.

04.06 Patch Management – Vendor-supplied software and hardware patches are applied to managed objects and environments following standardized procedures. on-critical patches are evaluated for issues before release and applied during planned or accepted maintenance windows. Critical patches are applied as soon as possible to both Customer and internal environments.

UCS Objective 5: Service Operations Management

UCS Objective Summary and Purpose: *The goal of the Service Operations Management Objective deals with how the Organization identifies and responds to IT (Information Technology) related events that could impact services delivered to the Customer. In this UCS objective, the examination covers the Organization's Network Operations Center ("NOC"), Trouble Ticketing systems and Service Desk operations specifically related to event management policies and procedures.*

05.01 Centralized Operations Center – A Managed service/Network/Secure Operation Center (MSOC/NOC/SOC) is used to provide effective and secure monitoring and management of Organization and Customer managed environments.

05.02 Support and Problem Logging – A problem management system (help desk / ticketing system) has been implemented to ensure that operational events that are not part of the Organization's standard operations are recorded, analyzed and resolved in a timely manner.

05.03 Categorization and Correlation – Problem/incident documentation is categorized to allow for event correlation and the elimination of false positives.

05.04 Support and Problem Resolution – Problems and/or incidents identified in the Customer's environment are properly resolved and such resolution is documented and reported to both Organization and Customer management.

05.05 Operations Monitoring – Organization management performs a periodic internal review of tickets and operational events.

UCS Objective 6: Information Security

UCS Objective Summary and Purpose: *The goal of the Information Security Objective is to ensure the Organization has implemented necessary controls to effectively govern access to managed data, networks and systems that may compromise security of both the Organization and the Customer. This includes remote access policies, user account administration, authentication, wireless access, segregation of duties, network security scans and assessments, and the monitoring of access to Customer systems.*

06.01 Controlled Access to Applications and Environments – Access to Organization and Customer systems and configuration data is restricted to authorized personnel following a documented Access Control Policy. All critical service delivery and internal applications have centralized access control mechanisms implemented.

06.02 Super-User and Administrator Access Security – Administrator IDs to information systems (network and in-scope critical systems) are restricted to a limited number of approved personnel.

06.03 Unique Users and Passwords – Users authenticate to Organizational information systems and the underlying Customer data using unique user account IDs and passwords.

06.04 Revocation of Access – Logical access to the Organization's information systems (Organization LAN (Local Area Network) and web portals) and Customer systems and data is revoked and reviewed for terminated and departing employees.

06.05 Strong Passwords – User authentication password mechanisms are implemented and require minimum standards for password length, complexity, expiration, reuse, and account lockout for failed attempts. Organization passwords are stored in a secure password repository.

06.06 Segregation of Access – Access to information systems (including Customer systems and data) is separated by functional area to ensure segregation of duties.

06.07 Continuous Review of Access Rights – Access to information systems, as well as the underlying customer systems and data, is continually reviewed by the Organization's upper management to ensure that resource access is appropriately restricted to authorized personnel.

06.08 Restricted Secure Remote Access – Remote access to the Organization and Customer information systems is protected by restricting access to the Remote Access Tool using a VPN or Zero Trust Network Access (ZTNA) configuration. Remote access is monitored, logged, and reviewed by Organization management following a Remote Access Policy.

06.09 Network and Endpoint Security Management and Monitoring – Local and wide area networks are secured through the use of managed firewalls and other devices and software. Where applicable, MDR/EDR/XDR controls and security information and event management (SIEM) systems are utilized to monitor and secure the Organization's network.

06.10 Email Security – The Organization has implemented applications and/or systems to scan and protect email and environments from email attacks and malware/viruses.

06.11 Network and Endpoint Protection – Organization has implemented an EDR (Endpoint Detection and Response) system on the network's connected devices and traffic (web and email) to scan and protect its environment.

06.12 Wireless Network Security – The Organization's wireless network is segregated from its guest wireless network.

06.13 Network Security Review – Network security reviews (including security assessments, scans, penetration tests, etc.) of the Organization's network are conducted periodically.

06.14 System Logging – The Organization has a formal process for tracking, retaining and reviewing audit logs.

UCS Objective 7: Data and Device Management

UCS Objective Summary and Purpose: *The goal of the Data Management Objective is to confirm the Organization has sufficient policies and procedures to ensure the integrity and availability of managed Customer and Organization internal data in the event of natural disasters, cyber-attacks (i.e., ransomware), and user error or malfeasance. This includes the implementation of data backup as well as encryption, security, retention, and restoration of managed Customer and Organization internal data.*

07.01 Customer Data Backup and Replication – Where applicable, Customer data backup schedules are documented and followed following contractual service agreements, with backups being monitored, with any errors being handled following operations management policies and procedures. Customer backup and/or replicated data is encrypted following contractual requirements.

07.02 Organization Data Backup and Replication – Organization data backups are being completed and monitored following backup schedules, with any errors being handled following operations management policies and procedures. Backup and/or replicated data is encrypted following Organization policies and procedures.

07.03 Data Recovery Testing – Backup data restoration and recovery testing procedures are conducted periodically, with the results of tests being logged and monitored by the Organization.

07.04 Disaster and Business Continuity Planning – Business continuity plans are documented and tested periodically to ensure the integrity of Organization and, if applicable, Customer data.

07.05 Internal Data Destruction – Objects containing internal data are handled and destroyed following end-of-life policies.

07.06 Customer Data Destruction – If data destruction services are delivered to Customers, objects containing Customer data are handled and destroyed following end-of-life policies.

07.07 Asset and Device Management – Assets and devices are maintained in a centralized inventory list. A device management policy and supporting security measures shall be adopted to manage the risks of all devices and assets. The Organization is using an active discovery tool when managing customer assets.

UCS Objective 8: Physical Security

UCS Objective Summary and Purpose*: The goal of the Physical Security Objective is to ensure the Organization has documented policies and procedures governing physical access and environmental security of the Organizational assets. The Organization must demonstrate sufficient physical security controls at each facility, including controls such as physical access administration, card key, CCTV, on-site security, visitor/guest logs and other effective security and environmental controls.*

08.01 Organizational Physical Security – Physical security controls are implemented by the Organization with respect to all work locations. Access rights of personnel are reviewed and approved by Organization upper management on a periodic basis.

08.02 Logging of Visitors – Visitor logs are maintained at each facility by the Organization. Visitors are required to sign the log upon entering the building.

08.03 Sensitive Area Security – Physical access to the sensitive areas (including operations centers, data centers, and server rooms) is restricted to authorized personnel.

08.04 Revocation of Physical Access – Upon termination, employee access to the Organization's facilities is revoked.

08.05 Data Center Environmental Controls – The Organization has environmental safeguards in their NOC(s) and/or data center(s) to protect from disruptive events.

08.06 Data Center Maintenance – Environmental and maintenance services are performed and tested regularly following a standardized and documented process.

08.07 Data Center Colocation – Physical access to collocation hardware maintained in the Organization's facilities is restricted to individuals designated by the Customer and authorized Organization personnel.

UCS Objective 9: Billing and Reporting

UCS Objective Summary and Purpose: *The goal of the Billing & Reporting Objective is to ensure the Organization is accurately monitoring service delivery, reporting, and invoicing for Customers following SLAs (service level agreements) signed by both parties.*

09.01 Signed Contracts and Agreements – Signed Master Service Level Agreements (MSA) are in place between the Organization and Customers.

09.02 Accuracy of Service Invoices – Organization invoices are generated following signed Master Service Level Agreement contracts.

09.03 Report Availability – Reporting metrics are available to Customers following signed contracts.

UCS Objective 10: Corporate Health

UCS Objective Summary and Purpose: *The goal of the Corporate Health Objective is to ensure sufficient corporate and financial health on the part of the Organization so that all of its Customers are adequately protected. Technical proficiency is only part of the Organization's value to the Customer. The Organization 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.*

10.01 Operational Sustainability – Financial reports demonstrate profitability of a minimum of 6 of the previous 12 months, or sufficient access to funds necessary to keep the Organization operational for a 12-month period of time

10.02 Significant Customer Risk – The Organization demonstrates sufficient managed services revenue distribution so that the largest Customer does not represent more than 20% of total managed services revenue and the five largest Customers do not represent more than 50% of total managed services revenue.

10.03 Sustainable Profit Margin on Services – The Organization demonstrates that a sustainable gross profit margin is realized on its managed service/cloud offerings.

10.04 Customer Commitments – The Organization shows that most of its customers and revenue come from relationships that last at least a year or longer.

10.05 Insurance – The Organization maintains errors and omissions, professional liability, cyber security and any other applicable insurance policies necessary to mitigate against Organization business disruption.

10.06 Customer and Employee Retention Tracking – The Organization maintains records to track the retention of customers (both voluntary and involuntary) and employees (both voluntary and voluntary) to ensure business continuity.

Special Requirements

The following special requirements contain controls that are commonly associated with specific service lines and Customer industries. As such, these special requirements can be added to the Cyber Verify reports.

SaaS (Software as a Service) Special Requirements:

04.07 SaaS Special Requirement: Application Development Procedures – Application Changes to information systems follow a formal process that requires the requesting, logging, approval, testing, and acceptance of changes before being implemented into production.

04.08 SaaS Special Requirement: Version Tracking and Code Maintenance – The Organization has a process for tracking application versions.

04.09 SaaS Special Requirement: Development Segregation of Duties – Segregation of duties exists between the development and promotion of application changes to the production environment.

Helpful Definitions

A **Customer** refers to the clients of a company who receive professional services as defined in a service level agreement or comparable ongoing service-level document. Customers are the end-users who benefit from the services provided by the organization.

A **Vendor** is a company or individual that provides a product or performs a service for another company. Vendors can include consultants, banking service providers, software maintenance vendors, and auditors. They often have access to customers or other sensitive data and have a contractual commitment to the company.

An **External Service Provider (ESP)** is any Vendor or third party that provides a service for your company. This service could take many forms, such as an application, Infrastructure as a Service (IaaS), Software as a Service (SaaS), Hardware as a Service (HaaS), data destruction services, data centers/colocation services, etc. Continuous access refers to any access that is constant or permanent within an application or service.