System Security Plan

Compliance Island

Version 1.0 • Sample For Public Release

Report Prepared by:

Island SYSTEMS

Date/Time Generated: 9/10/2021 2:09:13 PM

Author: Island Systems, LLC

Table of Contents

Glossary

Term	Type	Meaning
Abstraction	Relationship	Target element is an abstraction of the source element. Arrows run from source to target. Line style is solid, typically without arrows, but if arrows exist they are open.
Allocate	Relationship	Source element is applied (allocated to) the target element. Arrows run from source to target.
Association	Relationship	There is an unspecified relationship between source and target.
Call	Relationship	The source element triggers an action on the target element. Arrows run from source to target.
Defines	Relationship	The source element is responsible for determining the contents of the target element. Arrows run from source to target.
Deploys	Relationship	Operation of the source element results in the physical deployment of the target element. Arrows run from source to target.
Flow	Relationship	Information flows between source and target. Arrows indication the primary direction of flow but, for clarity, typically do not reflect acknowledgement return flows.
Generalization	Relationship	The target element is a more general, abstracted, or parent element of the source. Arrow runs from the more specific element to the more general requirement. Line style is solid with filled arrows.
Implements	Relationship	Operation of the source element results in the implementation of the target element. Arrow runs from source to target.
Manifest	Relationship	Operation of the source element causes the target element to come into existence. Arrows run from source to target.
Partly Satisfies	Relationship	Operation of the source element partially satisfies the requirements of the target element. Arrow runs from source to target.
Realization	Relationship	Source element implements or Realizes the target element. Arrows run from target to source. Line style is dashed with filled arrow.
Satisfies	Relationship	Operation of the source element satisfies the requirements of the target element. Arrow runs from source to target.
Trace	Relationship	There is an intangible relationship between the two elements but no direct dependency. Arrows typically run from source to target but may be bi-directional or target to source depending on the situation.
Use / Usage	Relationship	Source element makes use of the target element. Arrows run from source to target.

System Overview

Information System Identification

Information System Name: Compliance Island

Information System Abbreviation: CI

Throughout this document, references are made to the Organization Seeking Certification (OSC), {{Organziation}}, using the following abbreviations:
{{OrgAbbreviation}}
{{org}}

Leveraged Practices and Processes

{{Organization}} leverages the practices and processes of external organizations or service providers to operate the CI system. The external organizations or service providers leveraged by {{Organization}} are identified below and referenced throughout this System Security Plan:

Microsoft Corporation (MS)
Microsoft Azure (Azure)
Microsoft 365 (M365) a.k.a. Office 365 (O365)

Island Systems, LLC
Compliance Island (CI)

Contacts

Information System Owner (ISO)

The following individual is identified as the system owner or functional proponent/advocate for this system:

{{OrganizationPOC}}, {{OrganizationPOCTitle}}
{{Organization}}
{{OrganizationPOCAddress1}}
{{OrganizationPOCAddress2}}
{{OrganizationPOCCity}}, {{OrganizationPOCState}} {{OrganizationPOCZipCode}}
{{OrganizationPOCPhone}}
{{OrganizationPOCEmail}}

Authorized Information System Delegates (AISD)

The ISO, together with the following ISO authorized individual(s), collectively referred to as Authorized Information System Delegates (AISD), are authorized to direct the operation of the CI system:

{{OrganizationAISD}}

Technical Point of Contact (TPOC)

The following organization possesses in-depth knowledge of this system and/or its functions and operation:

Island Systems, LLC
+1 301-664-4049
https://islandsystems.net

Cloud Service Providers (CSP)

The following is the CI system cloud service provider contact information:

Microsoft Corporation
+1 (800) 642 7676

Primary support should be directed to Island Systems. Should the need arise to contact Microsoft, this can be done via the above phone number but is best achieved via the Azure or Microsoft 365 portals:

Azure Portal: https://portal.azure.us/
Microsoft 365: https://portal.office365.us/

Information System

This System Security Plan provides an overview of the security practices and processes for Compliance Island (CI) and describes the controls in place or planned for implementation to provide a level of security appropriate for Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) to be transmitted, processed or stored by the system. Information security is vital to the Defense Industrial Base and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the CI information system.
The security safeguards implemented for the CI system meet the policy and control requirements set forth in this System Security Plan.

Target CMMC Level

{{Organization}} has reviewed the security practices and processes in place for the CI information system and anticipates receiving or maintaining **CMMC Level 3** from an Accredited C3PAO.

System Function

The function and purpose of the CI system is to enable the processing of CUI by persons and processes authorized by {{Organization}}. Primary use-cases include typical productivity applications, such as Microsoft Office, and other applications as may be defined by {{Organization}} to meet contractual requirements.

This function is achieved through the use of Virtual Desktop Infrastructure (VDI) technology as implemented by Azure Virtual Desktop (AVD), formerly known as Windows Virtual Desktop (WVD).

The use of VDI greatly reduces the risks to the system by limiting the extra-cloud data input and output to the Virtual Desktop Client. For example, output is typically limited to the information visible on the VDI host system's screen and system audio. Input is typically limited to subset of the devices connected to the End-user Device (such as a PC or "zero-client") running Virtual Desktop Client software, e.g. keyboard, mouse, security device such as a smartcard reader, microphone, camera.

Implementation details are described in the CMMC Practices section.

System Environments of Operation

The following environments are used to develop, test, or operate the CI system:

System Environments of Operation Diagram

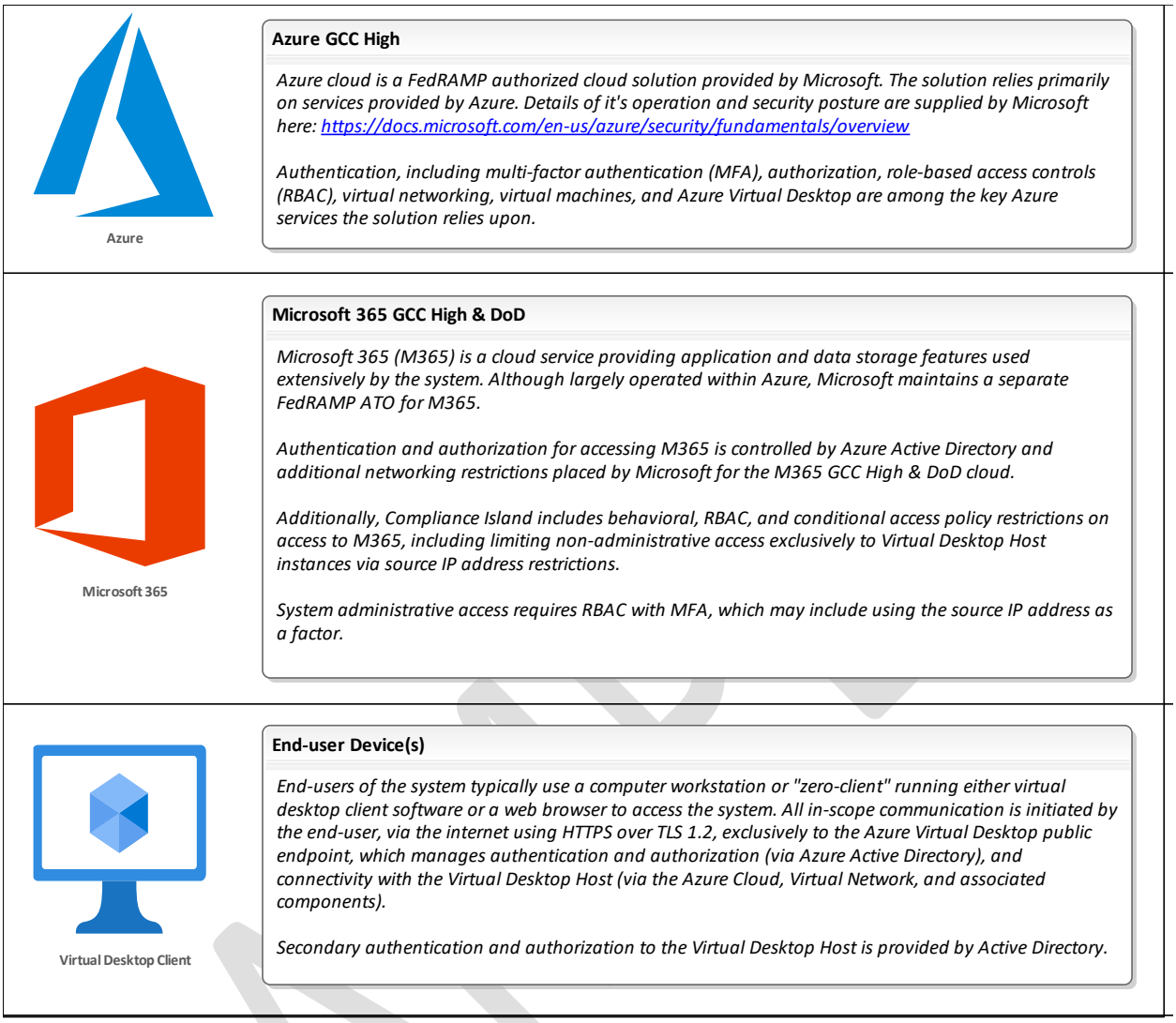

Figure 1. System Environments of Operation

System Interconnections

The CI system is interconnected to the following external systems (blank indicates none):
{{OrganizationInterconnects}}

System Architecture

System Boundary Diagram

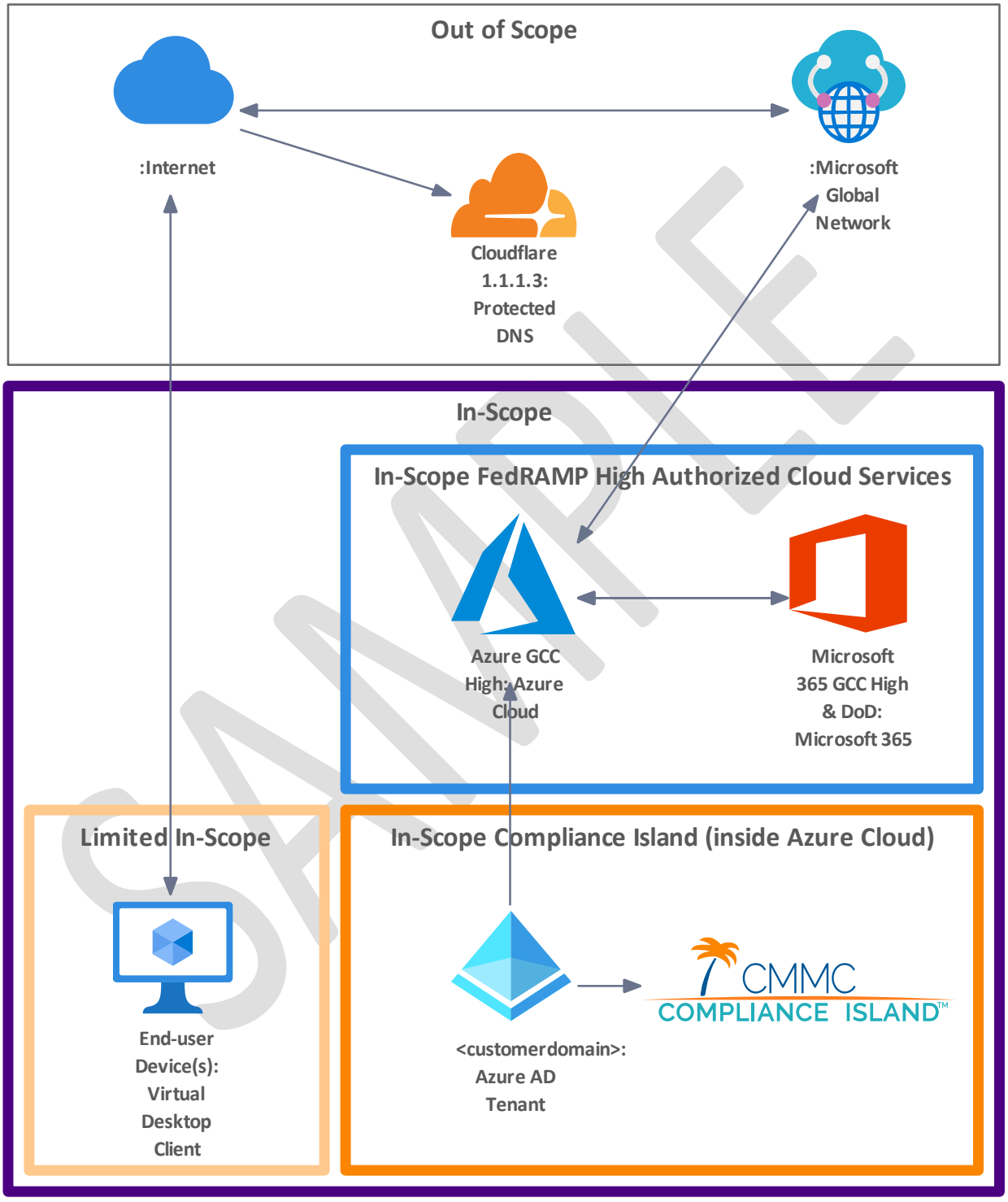

Figure 2. System Boundary

This diagram shows a simplified network architecture and denotes the in-scope vs. out-of-scope high level system components.

The following definitions are used:

- Out of Scope: Systems that are required for system operation but never contain CUI in unencrypted form. CUI may be transmitted over these systems when encrypted by FIPS-certified protocols.
- In-Scope: Systems that process, transmit, and/or store CUI.
- In-Scope FedRAMP High Authorized Cloud Services: Systems that process, transmit, and store CUI within the context of an authorized cloud provider.
- Limited In-Scope: Systems that act as user interface terminals which process and transmit but do not store CUI.
- In-Scope Compliance Island (inside Azure Cloud): System implementations entirely contained within the Azure GCC High cloud that process, transmit, and store CUI.

Azure Logical Structure

Azure Resource Groups (RG) contain various deployed system components, such as virtual network (vNet), virtual machine (VM), disks, network adapters, etc.

Here is a brief description of each Resource Group:

- **Admin Resource Group** - Contains central components of the CI system such as the vNet, Log, Automation Account, and other shared infrastructure. There is only one instance of this RG. Logs may contain CUI.
- **Domain Controller Resource Group** - Contains Active Directory (AD) infrastructure exclusively. There is only one instance of this RG. Does not contain CUI.
- **Compliance Island Resource Group(s)** - Contains the Azure Virtual Desktop infrastructure including the VMs users log into. There may be multiple instances (<XX> represents a sequence number e.g. 01, 02, etc.). Contains CUI.
- **NetworkWatcherRG** - Configuration components for network traffic monitoring. Logs are sent to the Azure Log in the Admin RG. There is only one instance of this RG. Does not contain CUI.

Network Architecture Overview Diagram

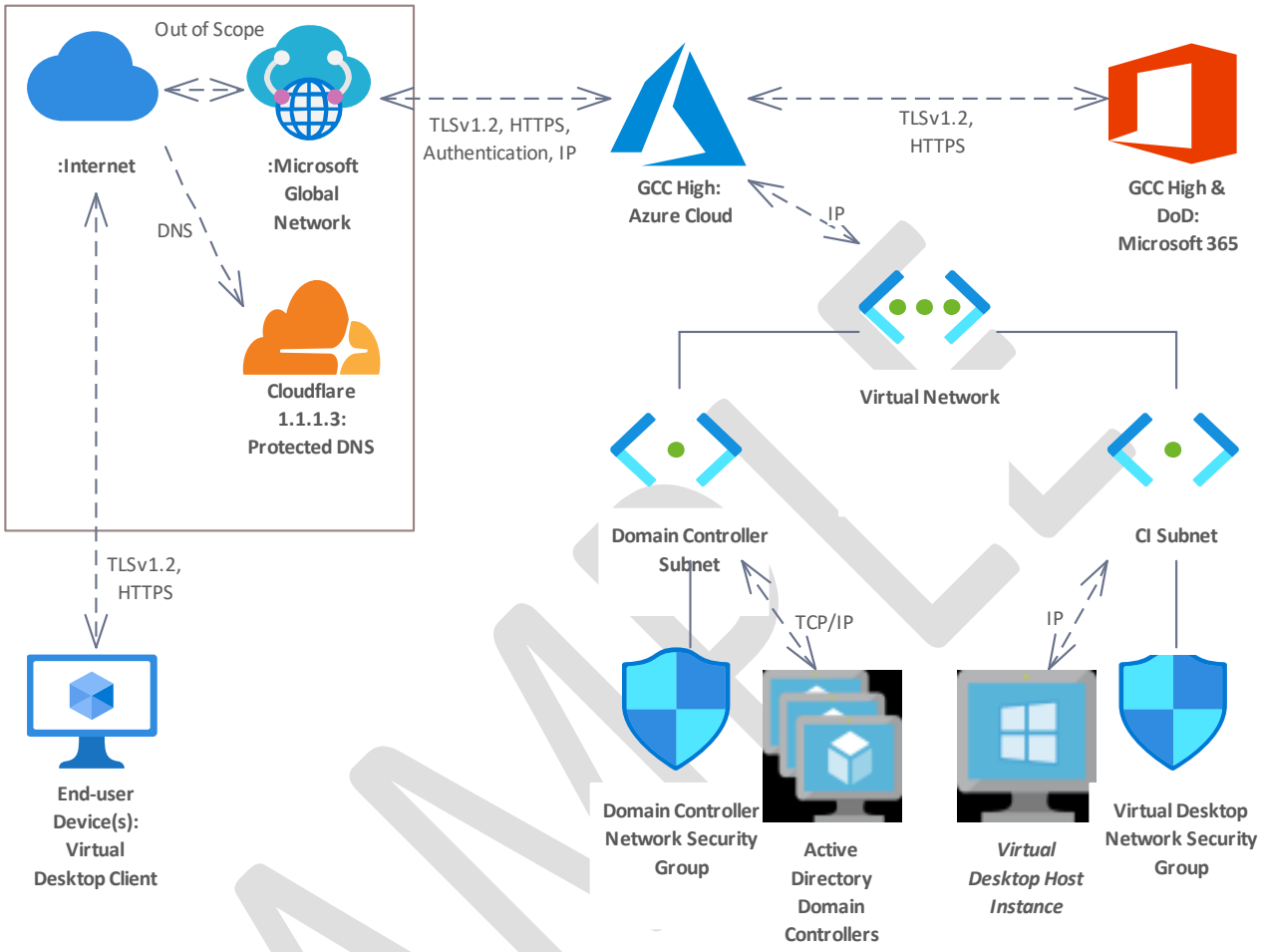

Figure 3. Network Architecture Overview

The Network Architecture Overview diagram presents a simplified version of the key network and architectural components of the system.

Excepting the Internet, each component has additional technical and security components described elsewhere, such as:

- functional relationships between components
- internal Azure networking
- IP protocol routing rules and restrictions
- Network Address Translation (NAT)
- Azure and Microsoft 365 network infrastructure
- firewall and Network Security Group (NSG) settings
- authentication requirements and restrictions
- location-based access controls
- communication protocol specifics
- traffic initiator / responder roles

- multiple Azure regions and virtual network peering
- other network and security component

The network components within Azure can be verified by viewing: https://portal.azure.com/#blade/Microsoft_Azure_Network/NetworkWatcherMenuBlade/topology.

For information about each component, see the Component Details appendix.

CUI Data

CUI Data Flow Diagram Diagram

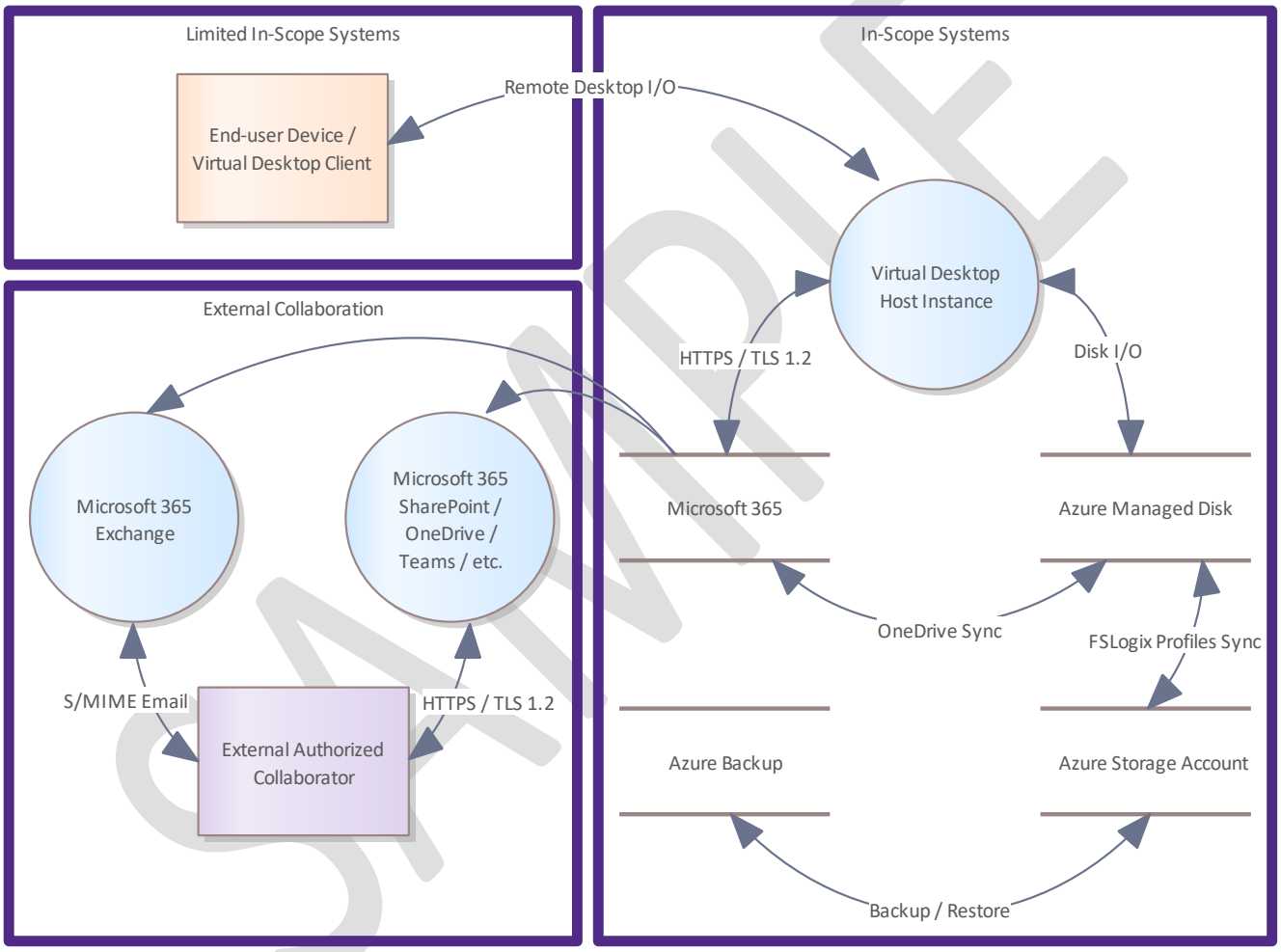

Figure 4. CUI Data Flow Diagram

In-Scope Compliance Requirements

Compliance In-Scope Requirements Overview Diagram

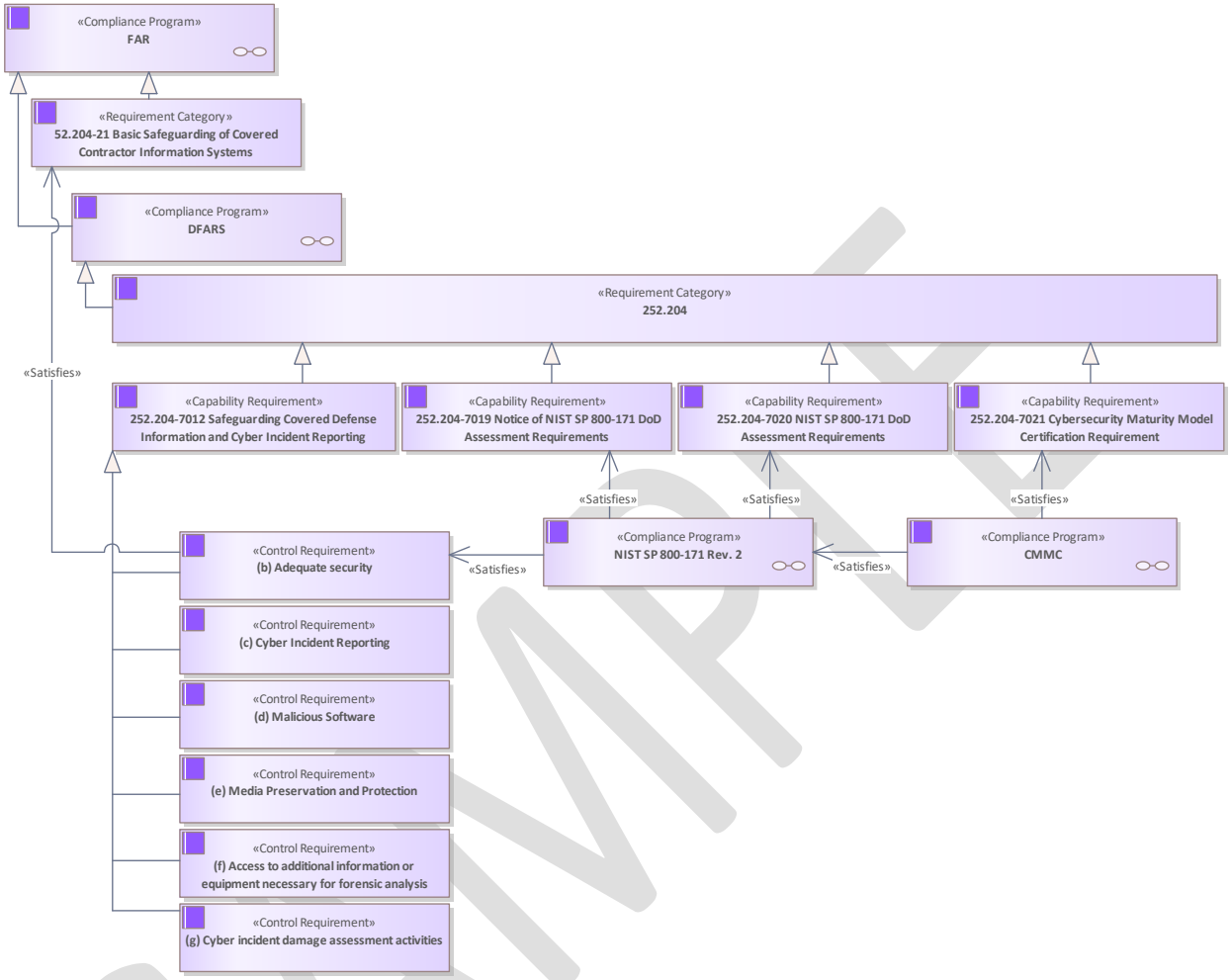

Figure 5. Compliance In-Scope Requirements Overview

This diagram shows the regulatory and compliance requirements that covered within the scope of Compliance Island.

CMMC Overview

CMMC Overview Diagram

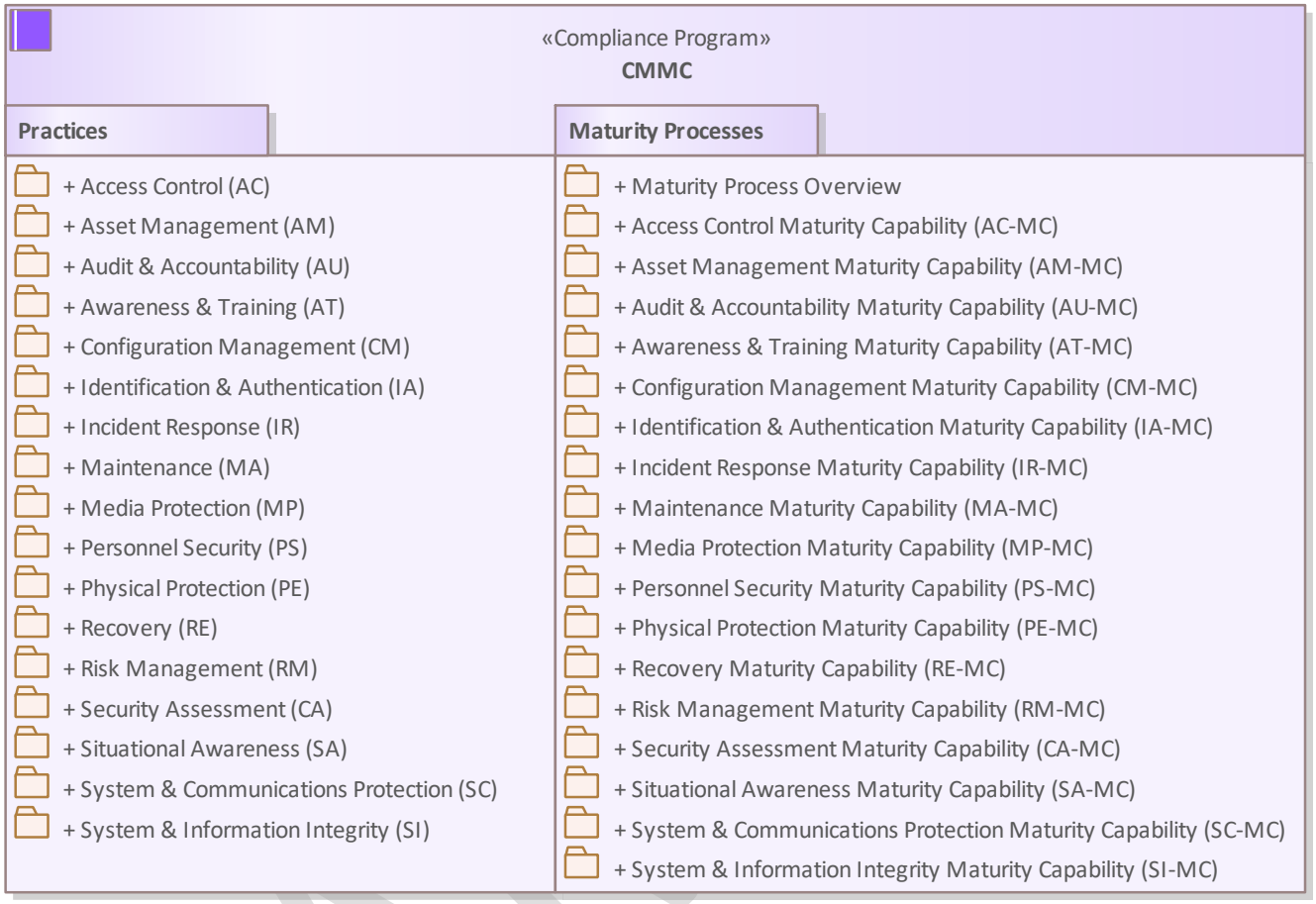

Figure 6. CMMC Overview

Practices

Access Control (AC)

Responsibility Matrix - Access Control (AC) Diagram

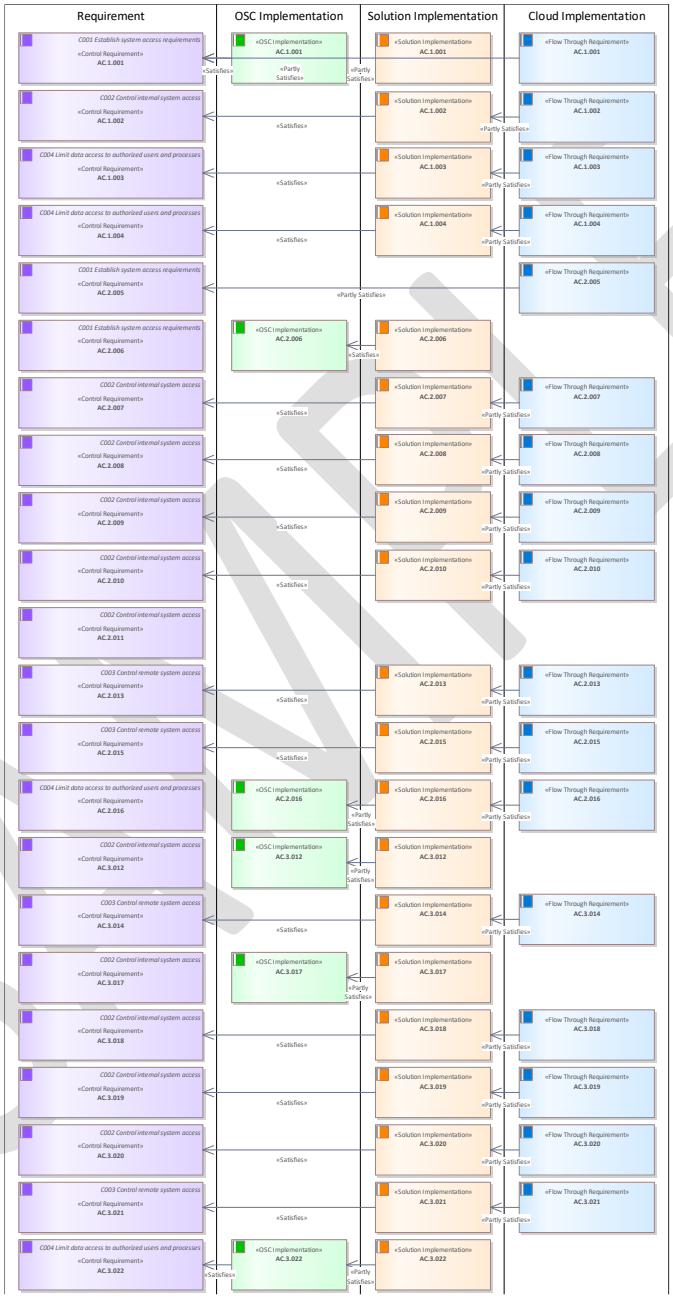

Figure 7. Responsibility Matrix - Access Control (AC)

This diagram shows the relationship between the Access Controls (AC) compliance requirements and implementations.

C001 Establish system access requirements «Capability Requirement»

AC.1.001 «Control Requirement»

Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).

AC.1.001 Diagram

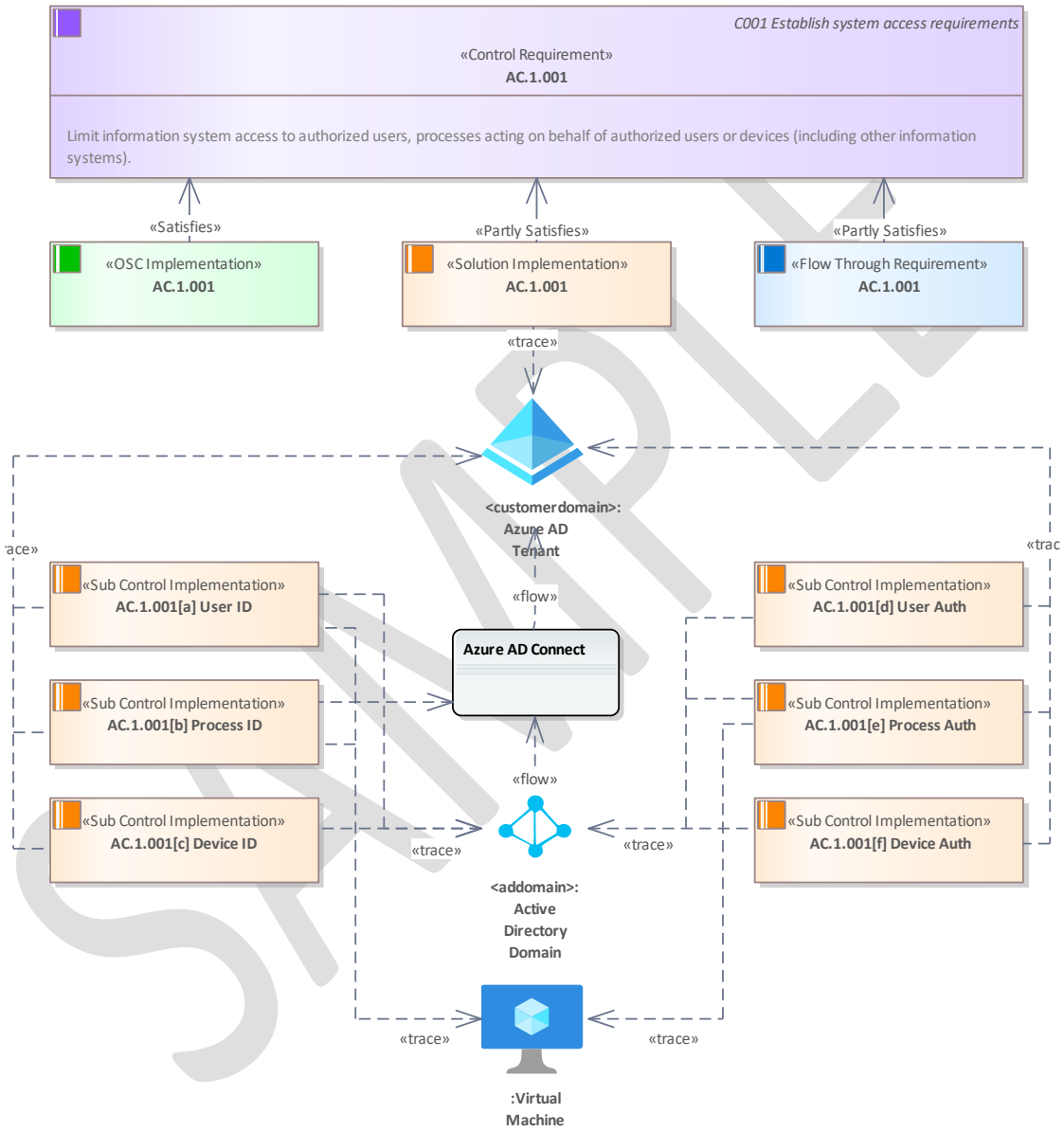

Figure 8. AC.1.001

Access control is implemented by 3 key system components:

1. Azure Active Directory
2. Active Directory
3. Operating Systems

This diagram shows the relationship between those components and the requirement.

AC.1.001 «Assessment Requirement»

Practice:
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Potential Assessment Methods and Objects:
Determine if: [a] authorized users are identified; [b] processes acting on behalf of authorized users are identified; [c] devices (and other systems) authorized to connect to the system are identified; [d] system access is limited to authorized users; [e] system access is limited to processes acting on behalf of authorized users; and [f] system access is limited to authorized devices (including other systems).

Examine:
SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records

Interview:
SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities

Test:
SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management

Discussion:

AC.1.001 «Flow Through Requirement»

Shared Coverage

Supporting Services:
Azure Active Directory
Intune/Microsoft Endpoint Manager
Conditional Access
Privileged Identity Management
O365 Security and Compliance
Implementation Guidance from Microsoft:
{{Customer}} Responsibility:
{{Customer}} enables relevant Azure policies and leverages Azure automation to implement this control, {{Customer}} is then still responsible for providing the following capabilities:
1) Identification and selection of all {{Customer}} controlled accounts within the system
2) Identification and selection of all {{Customer}} controlled processes acting on behalf of authorized users
3) Identification and selection of all {{Customer}} controlled devices (and other systems) authorized to connect to the system
4) For all of the above, defined system access requirements.
5) Process to define how Authorized users are specified and privilege levels are determined
6) Process to grant {{Customer}} controlled accounts with valid authorizations

AC.1.001 «Solution Implementation»

{[Organization]} responsibility:
1. Identification of authorized users
2. Identification of all End-user Devices
3. Identification of authorized devices connected to End-user Devices, such as printers
4. Identification of all authorized non-AAD associated devices

Primary audit logs for this control can be found here:
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Audit

AC.1.001[a] User ID «Sub Control Implementation»

Authorized users are identified:

A list of authorized users can be found in Azure Active Directory (AAD) at https://portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/MsGraphUsers.

Additionally, the following non-AAD users are identified:
- VM-local operating system root / system / service users (viewable on each VM)
- Active Directory domain administrators (viewable on Domain Controllers)

AC.1.001[b] Process ID «Sub Control Implementation»

Processes acting on behalf of authorized users are identified:

A list of processes can be found here:
https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AllApps/menuId/. For a complete list, including Azure and M365 internal applications, change the Application Type filter to "All Applications".

Additionally, the following processes are identified as acting on behalf of authorized users:
- Virtual Desktop Client processes running on authorized End-user Devices, including the web browser client
- VM operating systems and their components
- Approved applications
- Documented VM extensions and their child processes
- Azure and M365 processes, including documented extensions
- Azure AD Connect, which runs as a Windows service and utilizes the authorized "On-Premises Directory Synchronization Service Account" AAD user account and a local user account on the VM in which it runs (usually DC01)

AC.1.001[c] Device ID «Sub Control Implementation»

Devices (and other systems) authorized to connect to the system are identified.

All In-Scope devices are associated with Azure Active Directory (AAD) and listed here:
https://portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenuBlade/Devices/menuId/

Additionally, Island Systems is authorized for system access from administrative devices that are identified by IP address and listed in the System Admins Azure Named Location. See https://portal.azure.com/#blade/Microsoft_AAD_IAM/SecurityMenuBlade/NamedLocations.

{[Organization]} is responsible for the identification of all Limited In-Scope systems (e.g., End-user Devices).

Devices connected to End-user Devices, such as printers, are disabled by default, however, {[Organization]} may make exceptions and is responsible for identification and authorization of all such devices.

{[Organization is responsible for the identification and tracking of all non-AAD associated devices.

AC.1.001[d] User Auth «Sub Control Implementation»

System access is limited to authorized users.

Access control is performed by Azure Active Directory and additionally, for VDI logins, Active Directory.

No anonymous system access is permitted except for public-facing services such as for login, or terms and conditions pages.

AC.1.001[e] Process Auth «Sub Control Implementation»

System access is limited to processes acting on behalf of authorized users.

Access control is performed by Azure Active Directory, Active Directory, and operating system security.

No processes are allowed by unauthorized users.

AC.1.001[f] Device Auth «Sub Control Implementation»

System access is limited to authorized devices (including other systems).

Access control is performed by Azure Active Directory and Active Directory.

No anonymous system access is permitted except for public-facing services such as for login, or terms and conditions pages.

AC.1.001 «OSC Implementation»

{[Organization]} responsibility implementation:
Identification of authorized users is achieved by following the approved policies and procedures:
{[TODO]}

- Identification of all End-user Devices
- Identification of authorized devices connected to End-user Devices, such as printers
- Identification of all authorized non-AAD associated devices

AC.2.005 «Control Requirement»

Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules.

AC.2.005 Diagram

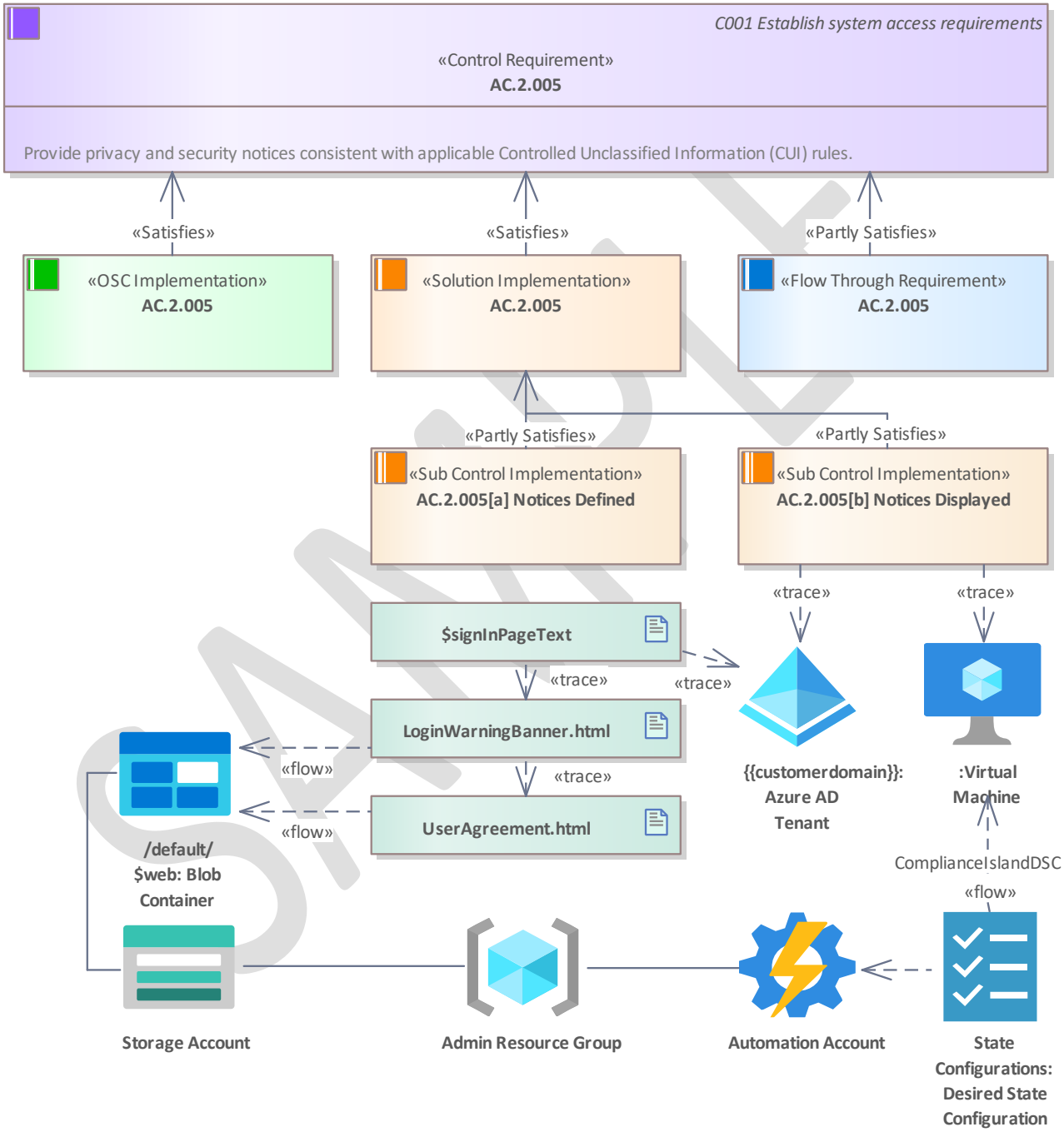

Figure 9. AC.2.005

AC.2.005 «Assessment Requirement»

Practice:
Provide privacy and security notices consistent with applicable CUI rules.

Potential Assessment Methods and Objects:
Determine if: [a] privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category; and [b] privacy and security notices are displayed.

Examine:
SELECT FROM: Privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit logs and records; system design documentation; user acknowledgements of notification message or banner; system security plan; system use notification messages; system configuration settings and associated documentation; other relevant documents or records

Interview:
SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibility for providing legal advice; system developers

Test:
SELECT FROM: Mechanisms implementing system use notification

Discussion:

AC.2.005 «Flow Through Requirement»

Shared Coverage

Supporting Services:
Azure Government Portal
Virtual Machines
Azure Active Directory
Implementation Guidance from Microsoft:
No Statement

AC.2.005 «Solution Implementation»

Solution meets the requirement.

{[Org]} is responsible for reviewing the notices and, if needed, providing Island Systems with any alternate language, including identifying any additional CUI category-specific information.

AC.2.005[a] Notices Defined «Sub Control Implementation»

Privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.

By default, the solution uses the text from the DoD CIO Memo, "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement", dated 9 May 2008.

In accordance with the DoD memo guidance, the AAD login page has limited space for text and therefore presents the following abbreviated message to users prior to login:

Notice and Consent Banner

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the terms in the [User Agreement](hyperlink to UA)

AC.2.005[b] Notices Displayed «Sub Control Implementation»

Privacy and security notices are displayed.

Notices are display in two instances during login:

- During login to AAD prior to authentication
- During login to VMs after authentication

Users login to AAD prior to gaining access to VMs.

AAD configuration can be confirmed here: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/LoginTenantBranding or, more optimally, by logging in.

VMs can be confirmed by checking the Azure Automation Account -> State configuration (DSC) -> Nodes for "Compliant" status.

Checking VMs directly is best achieved by logging into those VMs and observing the notices.

AC.2.005 «OSC Implementation»

{{Org}} has reviewed the notices and has:
[ ] accepted the provided language
[ ] provided Island Systems with alternate language, including identifying any additional CUI category-specific information

(Remaining control implementations have been redacted from this sample document.)

Maturity Processes

Maturity Process Overview

Maturity Process Overview Diagram

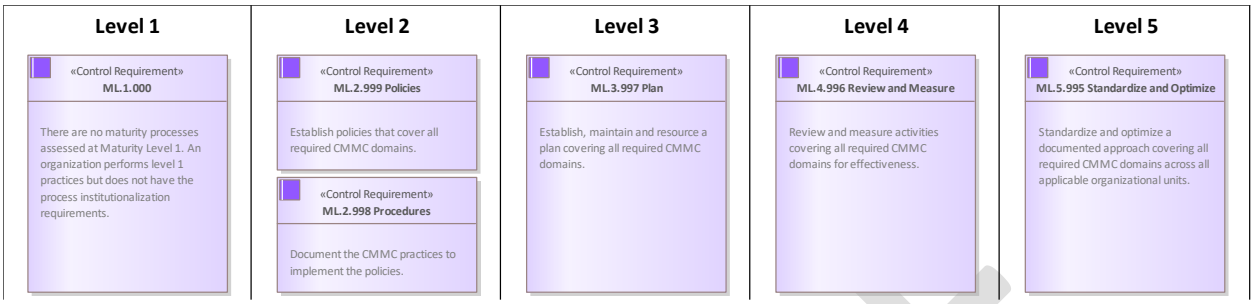

Figure 10. Maturity Process Overview

Maturity Level 1 - Performed «Capability Requirement»

ML.1.000 «Control Requirement»

There are no maturity processes assessed at Maturity Level 1. An organization performs level 1 practices but does not have the process institutionalization requirements.

Maturity Level 2 - Documented «Capability Requirement»

ML.2.999 Policies «Control Requirement»

Establish policies that cover all required CMMC domains.

ML.2.999[a] «Sub Control Implementation»

[a] the purpose of the policy is clearly stated

ML.2.999[b] «Sub Control Implementation»

[b] the scope of the policy is defined (e.g., enterprise-wide, department-wide, or information-system specific)

ML.2.999[c] «Sub Control Implementation»

[c] the roles and responsibilities of the activities covered by this policy are defined; (i.e., the responsibility, authority, and ownership of Access Control activities)

ML.2.999[d] «Sub Control Implementation»

[d] the policy establishes or directs the establishment of procedures to carry out and meet the intent of the policy

ML.2.999[e] «Sub Control Implementation»

[e] any regulatory guidelines that this policy addresses are included

ML.2.999[f] «Sub Control Implementation»

[f] the policy is endorsed by management and disseminated to appropriate stakeholders

ML.2.999[g] «Sub Control Implementation»

[g] the policy is periodically reviewed and updated

ML.2.998 Procedures «Control Requirement»

Document the CMMC practices to implement the policies.

ML.2.998[a] «Sub Control Implementation»

[a] the procedures to implement the practices are documented and followed to implement the policy for all required CMMC domains

ML.2.998[b] «Sub Control Implementation»

[b] the procedures specify the activities required to carry out the policies

ML.2.998[c] «Sub Control Implementation»

[c] procedures are reviewed and updated periodically to ensure they meet the policies

Maturity Level 3 - Managed «Capability Requirement»

ML.3.997 Plan «Control Requirement»

Establish, maintain and resource a plan covering all required CMMC domains.

ML.3.997 Plan «Assessment Requirement»

Practice:
Establish, maintain, and resource a plan that includes Asset Management.

Potential Assessment Methods and Objects:
Determine if: [a] the contractor establishes and maintains a plan that provides oversight for implementing the policies required in *.2.999; [b] the plan includes a mission and/or vision statement; [c] the plan includes strategic goals/objectives; [d] the plan includes relevant standards and procedures; [e] the plan documents the activities, due dates, and resources (e.g., funding, people, tools) assigned to implement and manage the policies required in *.2.999; [f] people resources are assigned to support implementing the policies required in *.2.999 and staff members have the appropriate knowledge, skills, and abilities to carry out their duties; [h] funding resources are defined and assigned to fully execute implementing the policies required in *.2.999 to include proper oversight, execution, and maintenance; [i] specific tools required to implement the policies required in *.2.999 are provided and people resources are adequately trained to use these tools; and [j] relevant stakeholders are involved in resourcing activities.

Examine:
SELECT FROM: Information security plans; system security plans; implementation plans; project plans; resourcing plans; organizational charts

Interview:
SELECT FROM: Personnel with security planning and implementation responsibilities; personnel with information security responsibilities

Test:
SELECT FROM: Organizational processes for plan development, review, update, and approval

Discussion:

ML.3.997[a] «Sub Control Implementation»

[a] the contractor establishes and maintains a plan that provides oversight for implementing the policies required in *.2.999

ML.3.997[b] «Sub Control Implementation»

[b] the plan includes a mission and/or vision statement

ML.3.997[c] «Sub Control Implementation»

[c] the plan includes strategic goals/objectives

ML.3.997[d] «Sub Control Implementation»

[d] the plan includes relevant standards and procedures

ML.3.997[e] «Sub Control Implementation»

[e] the plan documents the activities, due dates, and resources (e.g., funding, people, tools) assigned to implement and manage the policies required in *.2.999

ML.3.997[f] «Sub Control Implementation»

[f] people resources are assigned to support implementing the policies required in *.2.999 and staff members have the appropriate knowledge, skills, and abilities to carry out their duties

ML.3.997[g] «Sub Control Implementation»

[intentionally left blank]

ML.3.997[h] «Sub Control Implementation»

[h] funding resources are defined and assigned to fully execute implementing the policies required in *.2.999 to include proper oversight, execution, and maintenance

ML.3.997[i] «Sub Control Implementation»

[i] specific tools required to implement the policies required in *.2.999 are provided and people resources are adequately trained to use these tools

ML.3.997[j] «Sub Control Implementation»

[j] relevant stakeholders are involved in resourcing activities

Maturity Level 4 - Reviewed «Capability Requirement»

ML.4.996 Review and Measure «Control Requirement»

Review and measure activities covering all required CMMC domains for effectiveness.

Maturity Level 5 - Optimizing «Capability Requirement»

ML.5.995 Standardize and Optimize «Control Requirement»

Standardize and optimize a documented approach covering all required CMMC domains across all applicable organizational units.

Access Control Maturity Capability (AC-MC)

MC01-AC Improve Access Control (AC) activities «Capability Requirement»

AC.2.998 «Control Requirement»

Document the CMMC practices to implement the Access Control (AC) policy.

AC.2.998 «Assessment Requirement»

Practice:
Document the CMMC practices to implement the Access Control policy.

Potential Assessment Methods and Objects:
Determine if: [a] the procedures to implement the practices are documented and followed to implement the policy for the Access Control domain; [b] the procedures specify the activities required to carry out the Access Control policy; and [c] procedures are reviewed and updated periodically to ensure they meet Access Control policy.

Examine:
SELECT FROM: Access Control procedures, information security procedures

Interview:
SELECT FROM: Personnel with security planning and implementation responsibilities; personnel with information security responsibilities

Test:
SELECT FROM: Organizational processes for practice development, review, update, and approval

Discussion:

AC.2.999 «Control Requirement»

Establish a policy that includes Access Control (AC).

AC.2.999 «Assessment Requirement»

Practice:
Establish a policy that includes Access Control.

Potential Assessment Methods and Objects:
Determine if: [a] the purpose of the policy is clearly stated; [b] the scope of the policy is defined (e.g., enterprise-wide, department-wide, or information-system specific); [c] the roles and responsibilities of the activities covered by this policy are defined; (i.e., the responsibility, authority, and ownership of Access Control activities); [d] the policy establishes or directs the establishment of procedures to carry out and meet the intent of the policy; [e] any regulatory guidelines that this policy addresses are included; [f] the policy is endorsed by management and disseminated to appropriate stakeholders; and [g] the policy is periodically reviewed and updated.

Examine:
SELECT FROM: Access Control policies; information security policies; information technology policies

Interview:
SELECT FROM: Personnel with security planning and implementation responsibilities; personnel with information security responsibilities

Test:

SELECT FROM: Organizational processes for policy development, review, update, and approval

Discussion:

AC.3.997 «Control Requirement»

Establish, maintain and resource a plan that includes Access Control (AC).

AC.3.997 «Assessment Requirement»

Practice:
Establish, maintain, and resource a plan that includes Access Control.

Potential Assessment Methods and Objects:
Determine if: [a] the contractor establishes and maintains a plan that provides oversight for implementing the policies required in AC.2.999; [b] the plan includes a mission and/or vision statement; [c] the plan includes strategic goals/objectives; [d] the plan includes relevant standards and procedures; [e] the plan documents the activities, due dates, and resources (e.g., funding, people, tools) assigned to implement and manage the policies required in AC.2.999; [f] people resources are assigned to support implementing the policies required in AC.2.999 and staff members have the appropriate knowledge, skills, and abilities to carry out their duties; [h] funding resources are defined and assigned to fully execute implementing the policies required in AC.2.999 to include proper oversight, execution, and maintenance; [i] specific tools required to implement the policies required in AC.2.999 are provided and people resources are adequately trained to use these tools; and [j] relevant stakeholders are involved in resourcing activities.

Examine:
SELECT FROM: Information security plans; system security plans; implementation plans; project plans; resourcing plans; organizational charts

Interview:
SELECT FROM: Personnel with security planning and implementation responsibilities; personnel with information security responsibilities

Test:
SELECT FROM: Organizational processes for plan development, review, update, and approval

Discussion:

AC.4.996 «Control Requirement»

Review and measure Access Control (AC) activities for effectiveness.

AC.5.995 «Control Requirement»

Standardize and optimize a documented approach for Access Control (AC) across all applicable organizational units.

(Remaining maturity processes have been redacted from this sample document. Implementation is outside the scope of this sample document.)

-- End of sample document --

