California Department of
PublicHealth

Cloud Service Provider (CSP) Security Standard version 1.3

Contents

Revision History

Date	Author	Version	Change Description
10/19/2022	Cannic Hung – ISO	0.1	Initial Draft
11/29/2022	Cannic Hung – ISO	0.2	- Renamed the “Checklist” document to CSP Security Standard. - Replaced the Roles and Responsibilities section with RACI matrix. - Removed SecOps team under the review and approved responsibilities, as they play a role for onboarding function. - Consolidated Azure Key Vault and Azure IAM Security Requirements to the CSP Security Standard. - Integrated the CSP Security Checklist items and appended to the new CSP Security Standard (ID 6 to 10). - Updated the Security Standard ID 3.4 under the Detect category, to ensure cloud logs are sent to CDPH’s SIEM, not CDT. Also removed the term ‘Desirable’ to make it a mandatory requirement. - Removed the Intro/History section and moved it to Appendix A. - Removed revision dates outlined in the Standard Framework diagram. - Expanded Appendix A’s table with a new column to map other Regulations with the CSP Security Standard. - Added SOC 2, HIPAA, and FedRAMP Requirements (Security Standard ID 11) - Added FIPS-199 and System Security Plan (SSP) requirements (Security Standard ID 8.1 and 8.2)
1/18/2023	Cannic Hung – ISO	0.3	- Added Azure AD is CDPH’s centralized IdP and the CSP must leverage it via SAML/OAuth2 Federation. - Added no creation of local account on systems/services unless they are “break glass” accounts. - Added CSP is fully responsible for FIDO2-certified devices (e.g., Yubikeys) when it comes to hardware cost and inventory management. - Added more context about the requirement 2b.15 - limit VM access to instance metadata services.
1/23/2023	Cannic Hung – ISO	1.0	Reviewed and approved by ISO, Security Architecture and EA teams.
2/27/2023	Cannic Hung – ISO	1.1	- Added a requirement (ID 11.5) - Per SAM 4983.1, physical location of data center must be (1) located within the continental United States, and (2) remote

			access to data from outside the continental United States is prohibited.
5/8/2023	Cannic Hung – ISO	1.2	Created Appendix B to provide a separate area for contractors to fill out and elaborate how their cloud solution complies with our requirements.
5/26/2023	Cannic Hung – ISO	1.3	Updated Appendix B to provide clearer instructions and evaluation criteria.

Overview

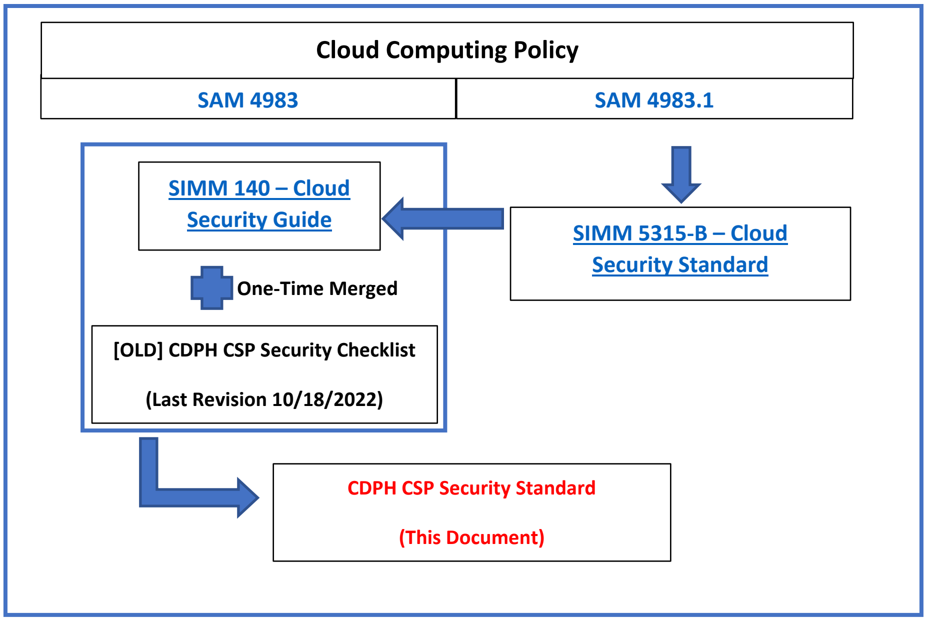
To protect information and systems in cloud services, CDPH must comply with the Cloud Computing Policy, State Administrative Manual (SAM) Sections 4983-4983.1, and employ the capabilities, administrative and technical security requirements outlined in this CSP Security Standard.

In accordance with SIMM 5315-B, the CSP Security Standard is broken down into five capabilities[1], they are Identify, Protect, Detect, Respond, and Recover. Each capability consists of a list of minimum cloud security requirements.

Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

[1] Based on NIST Cybersecurity Framework (CSF)'s core component.

Standard Framework


Cloud Computing Policy
SAM 4983
SAM 4983.1
SIMM 140 – Cloud Security Guide
SIMM 5315-B – Cloud Security Standard
One-Time Merged
[OLD] CDPH CSP Security Checklist
(Last Revision 10/18/2022)
CDPH CSP Security Standard
(This Document)

The diagram shown above illustrates how the **CDPH CSP Security Standard** is derived. By design, the CDPH CSP Security Standard is a living document that contained a set of high-level CSP requirements that are derived from SIMM-140 and other regulations. In addition, the standard contained technical and administrative security requirements based on the CDPH's existing cloud environment, its configurations, and processes.

Update Frequency

The CSP Security Standard must be updated, reviewed, and approved when one of the following conditions occur:

- The Office of Information Security (OIS) has published a new version of their Cloud Computing Policies and Standards.
- The CDPH's Security Architecture or Enterprise Architecture has published a new Cloud Computing initiative.
- Microsoft has made updates to their Azure services that could impact the technical security requirements outlined in this CSP Security Standard.

RACI Matrix

Tasks	ISO	Security Architecture	Enterprise Architecture
Owner of the CSP Security Standard, which include tasks such as updating the standard draft, facilitating meetings, managing, and publishing the approved standard in the ISO Intranet site.	R/A	C	C
Conduct a one-time merge analysis: review and merge the CDPH CSP Security Checklist to the new standard.	R/A	R	I
Review SAM 4983 and 4983.1 Policies, SIMM 5315-B and SIMM 140 and future updates	R/A	R	I
Review and approve of the CDPH CSP Security Standard.	R/A	R	R

Code	Stands for	This is the team who is…
R	Responsible	Responsible for performing the task or creating the document
A	Accountable	Accountable for the task or document
C	Consult	Provides consulting or expertise to the team responsible for the task or document
I	Inform	Informed of task progress or results

Approved CSP Security Standard Location

Approved CSP Security Standard is published to the ISO Intranet SharePoint site –

Policies and Procedures (sharepoint.com)

CSP Security Standard

ID	Category	Requirement
1	Identify	
1.1		Maintain an inventory of accounts with CSP including root email addresses, account IDs, and points of contact.
1.2		Maintain a method of tracking configuration changes and viewing inventory and configuration history of cloud services.
1.3		Apply resource tags to data and applications according to their categorization and criticality.
2	Protect	
2a	Identity and Access Management (IAM)	
2a.1		Maintain a tiered account management structure and apply restrictions on subordinate accounts.
2a.2		Restrict usage of superuser access to the creation of less-privileged users for role-based access and administrative actions that can only be performed with superuser access.
2a.3		Require multi-factor authentication for all (1) privileged access, (2) user access to sensitive or confidential data, and (3) accounts representing official communications from state departments.
2a.4		Configure fine-grained user permissions according to least privilege. Ensure attempts to perform actions not permitted prompt notification of insufficient privilege.
2a.5		Perform an annual audit to review access and to remove unused credentials and permissions.
2a.6		Maintain logical perimeters between production and non-production environments (e.g., development, test). Prohibit using the same credentials across environments, except where single sign-on technologies generate unique credentials for federated access.
2a.7		Prohibit embedding credentials directly into code – configure applications to retrieve necessary credentials programmatically. Where feasible, programmatically generate temporary credentials instead of long-term credentials like passwords or access keys. Refer to the Azure Key Vault requirements section for more information.
2a.8		Provide access to cloud services by federated authentication through a centralized identity management system. Azure Active Directory (Azure AD) is the CDPH's centralized cloud identity provider (IdP). CSP must support SAML/OAuth2 federation to CDPH's IdP for user and administrative access. Refer to the Azure IAM Security Requirements section for more information.
2a.9		Deploy adaptive access control technologies to dynamically adjust authentication requirements based on contextual information.
2a.10		Creation of local accounts on systems/services is prohibited unless they are classified as "break glass" accounts.
2b	Infrastructure Protection	
2b.11		Establish network topologies to limit traffic routing only between resources as necessary.

ID	Category	Requirement
2b.12		Limit resource exposure to the public internet to only those resources intended to be publicly accessible and protected accordingly, including deployment of endpoint defense capabilities in accordance with SAM Section 5355.
2b.13		Deploy Web Application Firewalls and/or Distributed Denial of Service protection services to protect public-facing applications.
2b.14		Require authentication and authorization when accessing cloud-based resources even across dedicated network connections, except resources intended to be publicly accessible.
2b.15		Limit virtual machine access to instance metadata services. Reference: Unsecured Credentials: Cloud Instance Metadata API, Sub-technique T1552.005 - Enterprise | MITRE ATT&CK® - Disable the metadata service for any virtual machines which do not require it. - Limit the permissions providing to the virtual machine to least privilege, to limit the impact of compromise. - Utilize local firewall rules to deny sending traffic to the metadata service except from the processes that require it. - Pay particular attention to virtual machines which are widely reachable, for example from the internet.
2b.16		***[Desired, Not Required]*** Limit deployments and maintenance to automated technologies as much as possible, disabling services used for manual administration.
2b.17		***[Desired, Not Required]*** Utilize tools to programmatically scan for weak configurations, including identification and vulnerability assessment of public facing resources. Configure notification and/or automated remediation where possible.
2b.18		***[Desired, Not Required]*** Employ deployment practices which replace running instances with new instances created from an updated configuration, rather than updating running instances.
2c	Data Protection	
2c.19		Select and configure storage services according to data availability (i.e., resilience to system downtime) and durability (i.e., resilience to data loss) requirements, which may include replication across cloud service provider zones and/or regions.
2c.20		Configure fine-grained data access policies.
2c.21		Protect data at rest by employing SAM Section 5350.1 compliant encryption and/or tokenization methods to transform confidential, sensitive, or personal data into a form that is unreadable to unauthorized users.
2c.22		Protect data encryption keys from unauthorized use by defining restrictive policies for key use that enforce the principles of least privilege and separation of duties (e.g., separate users with key administration permissions from users with key use permissions, separate applications that require permission to encrypt data from

ID	Category	Requirement
		applications that require permission to decrypt data, require decryption requests to come from a trusted network path).
2c.23		Establish encryption key rotation policies to limit the impact of a single compromised key.
2c.24		Employ SAM Section 5350.1 compliant encryption methods to protect data in transit outside trusted network boundaries, even across dedicated network connections to cloud service providers.
2c.25		Configure data retention policies to automatically destroy data when it is no longer needed, in accordance with SAM Section 5310.6.
2c.26		Employ encryption methods to protect data in transit even within trusted network boundaries.
2c.27		***[Desired, Not Required]*** Employ techniques for automated discovery and classification of sensitive data.
3	Detect	
3.1		Log cloud management events to centralized log storage for each cloud service provider, maintaining audit records in accordance with SAM Section 5335.2.
3.2		Establish threat prevention capabilities to identify weak configurations and notify security personnel. Configure automated remediation where possible.
3.3		Establish threat detection capabilities informed by threat intelligence and configure alerts to notify security personnel.
3.4		Publish cloud/platform security logs to the Security Information and Event Management (SIEM) system operated by CDPH's Security Operations Center (SOC), in accordance with SAM Section 5335.
3.5		***[Desired, Not Required]*** Implement tools to detect access credentials being stored in source control repositories.
4	Respond	
4.1		Ensure incident response plans include procedures for notifying and coordinating with cloud service providers.
4.2		Ensure incident response procedures include providing access to external incident responders and protecting this access from unintentional use.
4.3		***[Desired, Not Required]*** Configure automated remediation of weak configurations.
4.4		***[Desired, Not Required]*** Configure automated responses for incident investigation, such as isolating resources from network access but preserving resource state.
5	Recover	
5.1		Provision for data preservation and retrieval in agreements with cloud service providers, including but not limited to: a) Identification of requisite formats for transfer of data to state entity or subsequent service provider. b) A defined transition period to enable a successful transfer of data from service provider to state entity.

ID	Category	Requirement
5.2		Configure automated data backups and virtual machine snapshots across zones and/or regions, according to recovery time and recovery point objectives.
5.3		***[Desired, Not Required]*** Define and deploy cloud infrastructure using code-like methods, back up configurations and scripts, and protect them from deletion.
6	Security Lifecycle	
6.1		CSP must have controls in place to protect the lifecycle of CDPH information from creation through to deletion.
6.2		CSP must assure CDPH information in digital and physical formats is securely isolated.
7	Personnel Security	
7.1		CSP must have appropriate screening and vetting procedures for internal personnel (besides under CDPH contract terms).
7.2		CSP personnel must be required to undertake mandatory information security awareness (besides under CDPH contract terms).
7.3		CSP must have processes in place to ensure personnel return assets when they leave or change role (MFA devices, mobile devices that have access to CDPH data, etc.).
7.4		CSP must have disciplinary processes for information security and privacy violations (besides under CDPH contract terms).
8	Application and Platform Security	
8.1		CSP must provide documentation that secure system engineering principles are followed within their Software Development Lifecycle (SDLC) processes.
8.2		CSP must provide documentation that host configuration is hardened against vulnerabilities (deploying hardened operating systems, disabling unnecessary services based on secure build images, etc.).
8.3		CSP must have multi-tenancy mechanisms configured and operational to separate CDPH applications from other customers.
8.4		CSP's web applications and APIs must be compliant with security standards, in accordance with OWASP Top 10, OWASP API Top 10, and CWE/SANS Top 25 Most Dangerous Software Errors.
8.5		CSP must have a Change Management Process in place to ensure deployment of validated application patches and updates.
8.6		If using CDPH's namespace for email is a requirement, the CSP's platform must have the capability of sending while meeting DMARC standards for SPF and DKIM, with SPF scoped to CDPH sending hosts only.
9	Network Security	
9.1		CSP's network connectivity must be adequate in terms of availability, traffic throughput, delays, and packet loss.
9.2		CSP must have gateway security measures in place against malware attacks.
9.3		CSP remote administration must be operated via a secure communication channel (SSH, TLS, IPSec, VPN, etc.).

ID	Category	Requirement
9.4		CSP must provide integration with CDPH's Cloud Access Security Broker (CASB) platform for threat monitoring, DLP, anomalous activity or conditional access policies.
9.5		CSP must have the ability to implement source IP restrictions.
10	Portability and Interoperability	
10.1		CSP must agree to provide CDPH information in an agreed upon format when the service arrangement ends.
10.2		CSP must have standardized or open interfaces to mutually exchange information between applications.
11	Regulatory Compliance	
11.1		CSP must be SOC 2 Type II compliance.
11.2		CSP must be NIST SP800-53 revision 5 compliance.
11.3		CSP must be HIPAA / HiTRUST compliance when providing a product or a service involve the creation, storage, or transmission of Protected Health Information (PHI).
11.4		***[Desired, Not Required]*** CSP must be FedRAMP certified.
11.5		The physical location of the CSP's data center, where the data is stored, must be: - Located within the continental United States, and - Remote access to data from outside the continental United States is prohibited unless approved in advance by the State Chief Information Security Officer.

Azure Key Vault Security Requirements

This section describes a set of required security controls for deploying and using Azure Key Vault. The goal of Azure Key Vault is to securely store and tightly control access three types of Key Vault objects:

a. **Secrets** – For example: Token, API key, Password, Connection String
b. **Keys** – For example: Symmetric Keys[2] and Asymmetric Keys
c. **Certificates** – For example: x.509 certificate with Private and Public Keys

Access to Azure Key Vault is controlled by two interfaces (Restful APIs):

- **Management Plane**: For example: Creating and Deleting Key Vaults; Retrieving Key Vault properties
- **Data Plan**e: For example: Add, delete, and modify Key Vault objects

The Key Vault objects could be consumed by cloud applications and services through RESTful APIs using OAuth2. Using Azure Key Vault mitigates the risk of Secrets, Keys and Certificates leakage.

ID	Requirement
1	Cloud applications and services must leverage Azure Key Vault. Never embed Secret, Key, and/or Certificate to an unsecured location like source code or configuration files.
2	Cloud applications and services must leverage the following Azure features for authenticating Azure Key Vault where possible: a. Use Azure Active Directory (AAD) Authentication b. Use Azure Managed Identity. The benefits of using Managed Identity: i. No need to manage credentials. Credentials are not accessible by anyone. ii. Use managed identity to authenticate Azure resources that supports AAD Authentication. iii. Managed Identity can be used at no extra cost.
3	Must disable All Networks access and enable/configure the Azure Key Vault's Firewalls and Virtual Networks settings to limit its access. Optionally a private endpoint[3] can be created in a VNET to connect Azure Key Vault, its traffic is sent privately using Microsoft backbone so it doesn't traverse the internet.
4	Must enable Role-Based Access Control (RBAC) permission model based on the Principle of Least Privilege. The RBAC permission model allows fine-grained access control comparing to Access Policy permission model. For example, RBAC for Key Vault provides the ability to have separate permissions on individual Keys, Secrets, and Certificates.
5	Must define the applicable conditions and criteria for AAD Conditional Access where possible. Consider common use cases such as blocking or granting access from specific locations, blocking risky sign-in behavior, or requiring organization-managed devices for specific applications.
6	Must enable *EnableSoftDelete* and *EnablePurgeProtection.* There could be scenarios where users accidentally run delete/purge commands on Key Vault, or an attacker/malicious user deliberately does so in order to cause disruption. Deleting or purging a Key Vault object leads to immediate data loss, as keys encrypting data and secrets/certificates allowing access/services will become non-accessible. *a. EnableSoftDelete* = True: Key Vault ensures that even if Key Vault is deleted, Key Vault itself or its objects remain recoverable for the next 90 days. Key Vault/objects can

[2] Azure Key Vault provides Standard and Premium SKU, the Standard SKU only support EC and RSA in Key Object
[3] Pricing and Limitation on Private Endpoint

<table>
<tr><th>ID</th><th>Requirement</th></tr>
<tr><td></td><td>either be recovered or purged (permanent deletion) during those 90 days. If no action is taken, key vault and its objects will subsequently be purged.

b. <i>EnablePurgeProtection</i> = True: Key Vault ensures that the Key Vault and its objects cannot be purged until the retention period has passed.</td></tr>
<tr><td>7</td><td>Must set an Expiry Time to each key vault object:
<table>
<tr><th>Key Vault Object Types</th><th>Expiry Time</th></tr>
<tr><td>Secret</td><td>12 months</td></tr>
<tr><td>Certificate</td><td>12 months</td></tr>
<tr><td>Key</td><td>24 months</td></tr>
</table></td></tr>
<tr><td>8</td><td>System Owners must decide the Rotation Policy settings [auto rotation; notification option] for their Cryptographic Key and Certificate objects. The decision on the Rotation Policy could depend on the amount of time they might need to update the system's configuration and to perform testing and validation. In addition, Key Vault auto-rotates certificates only support through established partnerships with Certificate Authorities (CAs), which are DigiCert and GlobalSign. Auto-rotation capability is not supported for certificates created with CAs that are not partnered.</td></tr>
<tr><td>9</td><td>Must enable Diagnostic AuditEvent setting to log the activities performed in Azure Key Vault (e.g., vault management, update/delete/create of objects, etc.).</td></tr>
<tr><td>10</td><td>Must enable Azure Defender for Key Vault to safeguards its objects and to provide an additional layer of security intelligence.</td></tr>
</table>

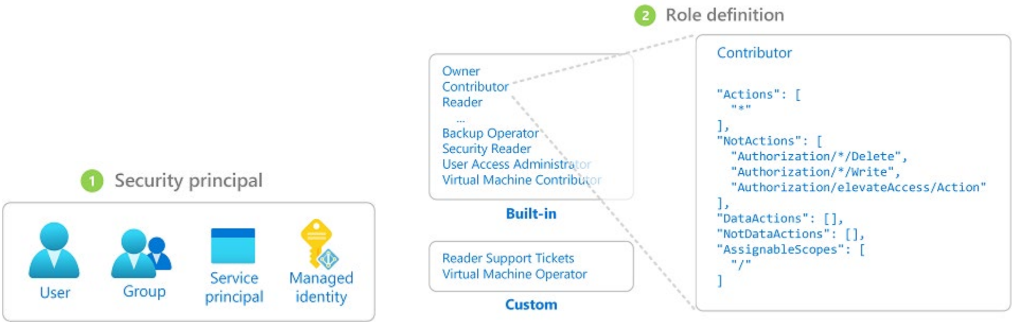
Azure IAM Security Requirements

This section describes a set of security requirements and best practices for protecting cloud resources using Identity and Access Management (IAM) in accordance with SIMM 140.

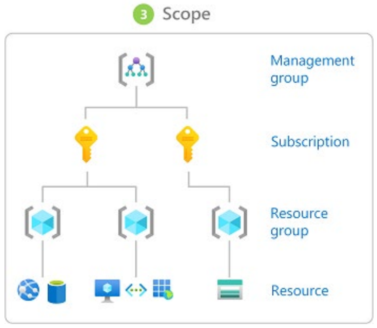
All data sources and computing services are considered resources and all access is granted through an IAM system. These resources rely on policies that define who can execute them and what other resources they have access to.

Azure Active Directory (Azure AD) is the CDPH's centralized cloud identity provider (IdP). It provides single sign-on (SSO), multifactor authentication (MFA), and conditional access policies to safeguard CDPH resources from cybersecurity attacks.

<table>
<tr><th>ID</th><th>Requirement</th></tr>
<tr><td colspan="2">Azure AD Authentication</td></tr>
<tr><td>1</td><td>SSO is required by using SAML 2.0 or OIDC/OAuth2 protocols.</td></tr>
<tr><td>2</td><td>MFA is required for all (a) privileged access, (b) user access to sensitive or confidential data, and (c) accounts representing official communications from state departments.

For implementing FIDO2-certified devices (e.g., YubiKeys), CSP is fully responsible for the associated hardware cost and inventory management.</td></tr>
<tr><td>3</td><td>Azure Conditional Access policy must be enabled and enforced based on contextual information of application users and devices (e.g., user or entity behavior, location context, network context, targeted application).</td></tr>
<tr><td colspan="2">Azure Role-Based Access Control (RBAC)</td></tr>
<tr><td>4</td><td>Azure RBAC must be used to configure fine-grained user permissions based on principal of least privilege.   A role assignment is the way to control access to Azure resources, and it consists of three elements:
<table>
<tr><th>#</th><th>Element</th><th>Description</th></tr>
<tr><td>1</td><td>Security Principal</td><td>An identity that gets the permissions. It could be a user, group, service principal and managed identity.</td></tr>
<tr><td>2</td><td>Role Definition</td><td>A collection of permission, it could be built-in or custom.</td></tr>
<tr><td>3</td><td>Scope</td><td>A way to constrain where those permissions are applicable, it could be management group, subscription, resource group or resource.</td></tr>
</table>

2 Role definition
Owner
Contributor
Reader
...
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor
Built-in
Reader Support Tickets
Virtual Machine Operator
Custom
Contributor
1 Security principal
User
Group
Service principal
Managed identity

"Actions": [
  "*"
],
"NotActions": [
  "Authorization/*/Delete",
  "Authorization/*/Write",
  "Authorization/elevateAccess/Action"
],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
  "/"
]</td></tr>
</table>

ID	Requirement
	 3 Scope Management group Subscription Resource group Resource
5	Maintain a tiered account management structure by organizing Azure subscriptions into management groups and apply restrictions on subordinate accounts. Consider applying the following policies to each subordinate account: ○ Prevent users from disabling service logging ○ Prevent users from disabling or altering alerting ○ Prevent users from deleting network flow logging ○ Prevent users from disabling or altering configuration management controls ○ Prevent users from creating new ways for networks to access the internet ○ Deny access to non-approved regions ○ Require encryption on data storage services ○ Limit compute resources to specific types ○ Require MFA for specific actions like stopping compute instances on production workloads ○ Require tagging upon resource creation
6	Leverage Privileged Identity Management (PIM) to grant just-in-time access. Using PIM, a user can be made an eligible member of an Azure AD role where they can then activate the role for a limited time when needed. Privileged access is automatically removed when the timeframe expires. In addition, configure PIM settings to require approval or receive notification emails when someone activates their role assignment. Notifications provide an alert when new users are added to highly privileged roles.
7	Assign the Azure AD Global Administrator role to limited number of users to reduce the attack surface. Microsoft recommends limiting the number of Global Administrators to less than 5.
8	Avoid assigning roles at broader scopes given those permissions are inherited to lower levels of scope. For example, if you assign the Reader role to an AD group at the subscription scope, all AD users who are member of the AD group can read everything for every resource group and resource in the subscription.
9	Avoid assigning role directly to Azure AD users. Instead, add users to groups and then assign roles to groups.
10	Designated users must perform an access review to privileged Azure resources and Azure AD roles annually to reduce the risk associated with stale role assignments.

<table>
<tr><th>ID</th><th>Requirement</th></tr>
<tr><td colspan="2">Service Principal and Managed Identity</td></tr>
<tr><td>11</td><td>Managed Identity[4] must be used to authenticate Azure resources. A Managed Identity allows an Azure-hosted application to access other Azure AD protected services without having to specify explicit credentials for authentication.</td></tr>
<tr><td>12</td><td>For Azure services don’t yet support Managed Identities, avoid storing credentials or access keys in unsecured locations like source code, configuration files, and environment variables. Instead, store credentials or access keys as secret, key, or certificate object in Azure Key Vault. Secret, key, and certificate objects must be rotated in a set time interval.</td></tr>
<tr><td>13</td><td>Avoid granting roles to the same Service Principal or Managed Identity across environments (non-prod vs prod).</td></tr>
<tr><td colspan="2">Microsoft Authentication Library (MSAL)</td></tr>
<tr><td>14</td><td>MSAL should be used to execute authentication flows for OIDC and OAuth2. If you prefer to use a library other than the MSAL or another Microsoft-supported library, choose one with a certified OpenID Connect implementation. Do not implement or draft your own library or make raw HTTP calls from an application.</td></tr>
<tr><td>15</td><td>An OAuth flow should be chosen based on application type:
<table>
<tr><th>OAuth Flow</th><th>Application Type</th></tr>
<tr><td>Authorization code with PKCE[5]</td><td>Single-page apps (SPA), web, mobile apps, native/desktop apps</td></tr>
<tr><td>Client credential</td><td>Server-side processes, scripts, daemons, server-to-server communication</td></tr>
<tr><td>On-behalf-of (OBO)</td><td>Web APIs that call another web API on a user’s behalf</td></tr>
<tr><td>Implicit grant</td><td>SPA, Web
Not recommended due to 3rd party cookies are being blocked by modern browsers. Instead, use authorization code with PKCE.</td></tr>
<tr><td>Resource Owner Password Credentials</td><td>Not recommended – This flow requires a very high degree of trust in an application and carries risks that are not present in other flows. You should only use this flow when other flows aren’t viable.</td></tr>
<tr><td>Device Code</td><td>Internet of Things (IoT) Devices</td></tr>
</table>
</td></tr>
<tr><td>16</td><td>MSAL is open source. Ensure to obtain MSAL from a reputable project on GitHub. Click here for the Microsoft official supported list based on application type and language/framework.</td></tr>
<tr><td>17</td><td>Always adopt the latest release of MSAL and stay up to date.</td></tr>
</table>

[4] Review the Microsoft documentation for a full and up-to-date list of all the resource type that support managed identities.

[5] Proof Key for Code Exchange

<table>
<tr><th>ID</th><th>Requirement</th></tr>
<tr><td colspan="2">Token Types and Configurations</td></tr>
<tr><td>18</td><td>
<table>
<tr><th>Token Type</th><th>Description</th><th>Default Expiry Time</th></tr>
<tr><td>SAML</td><td>SAML tokens are issued by the Security Token Service. It provides SSO experience for an enterprise SAML application.</td><td>1 hour</td></tr>
<tr><td>Access</td><td>Access tokens are issued by the authorization server to the client application. The client passes access tokens to the resource server. Access tokens contain the permissions the client has been granted by the authorization server. Access Tokens are short-lived.</td><td>Variable between 60 minutes to 90 minutes</td></tr>
<tr><td>Refresh</td><td>The client uses a refresh token, to request new access and ID tokens from the authorization server. Your code should treat refresh tokens and their string content as opaque because they're intended for use only by authorization server. The refresh tokens are long-lived.</td><td>Nonconfigurable: 24 hours for SPA, 90 days for all other scenarios</td></tr>
<tr><td>ID</td><td>ID tokens are issued by the authorization server to the client application. Clients use ID tokens when signing in users and to get basic information about them.</td><td>Bound to a user’s session lifetime</td></tr>
</table>
Token must be configured based on the following requirements:

- Tokens’ claims/assertions must be encrypted to protect the confidentiality of the data.
- Tokens must be digitally signed to protect the integrity of the data.
- The selection of a cryptographic algorithm and its key length must be FIPS 140-2 compliance.
- Tokens must be configured with an expiry time.
- Tokens must be treated like credentials. Do not expose them to users or other services.
</td></tr>
</table>

Appendix A – History and Requirements Mapping

Historically, the Information Security Office (ISO) has maintained a CDPH CSP Security Checklist [*last revised 10-18-2022*] for several years. This CDPH CSP Security standard is to replace the checklist and to achieve the following objectives:

- Compliance with CA Department of Technology (CDT)'s Cloud Computing Policy and Standard, and other regulations
- Compliance with CDPH cloud technical and administrative security controls that define Azure services like Azure Key Vault and Azure Active Directory.
- Define transition strategy to merge security requirements from the CSP Security Checklist to this standard
- Define RACI matrix

To transition from the CSP Security Checklist to the new standard, CDPH's ISO and Security Architecture teams must conduct a one-time analysis task. This is necessary to ensure existing requirements will continue to carry forward to the new standard.

The following table shows the mapping between the SIMM-140 and the CSP Security Checklist. The mapping could be used to analyze:

1. Which out-of-compliance cloud requirements CDPH must enforce, and
2. Which cloud requirements from the CSP Security Checklist need to carry forward to the new CSP Security Standard.

The result of the one-time analysis will augment to the new CSP Security Standard before it can be finalized.

CSP Security Standard		**CSP Security Checklist [Last Revision: 10-18-2022]**	**Regulations**
1 – Identify	1, 2, 3	**None**	
2a - Protect – IAM	1	**None**	
	2	6b	
	3	6e	
	4	6b, 6d	
	5	6c, 6g	
	6	5g	
	7	6f	
	8	6a	
	9	6d, 7h, 7g	
	10	**None**	
2b - Protect – Infrastructure Protection	11	13h	
	12	**None**	SAM Section 5355
	13	5i, 7b, 7c	
	14	6a, 6b	
	15	None	
	16	None	
	17	9a, 9b, 9c, 9d, 9e	

CSP Security Standard		CSP Security Checklist [Last Revision: 10-18-2022]	Regulations
	18	**None**	
2c - Protect – Data Protection	19	11a, 11b, 11c	
	20	6b	
	21	8b, 13a	SAM Section 5350.1; FIPS 140-2
	22	8c	
	23	8d	
	24	8a, 13a	SAM Section 5350.1; FIPS 140-2
	25	2c, 2e, 2f	SAM Section 5310.6
	26	8a	SAM Section 5350.1; FIPS 140-2
3 - Detect	1	5h	SAM Section 5335.2
	2	7b, 7c, 7e, 7g	
	3	5c, 10c, 7b, 7c	
	4	5h	SAM Section 5335
4 - Respond	1	10a, 10b, 10c	
	2	10d	
5 - Recover	1	11a, 11b	
	2	11c, 2d	
8 – Application and Platform Security	1	**None**	SIMM 5305-A; FIPS-199
	2	**None**	NIST SP800-53 Revision 5
	6	5e	OWASP Top 10; OWASP API Top 10; CWE/SANS Top 25 Most Dangerous Software Errors
11 - Regulatory Compliance	1	**None**	SOC 2
	2	1b	NIST SP800-53 Revision 5
	3	**None**	HIPAA
	4	**None**	FedRAMP
	5	**None**	SAM 4983.1

From the mapping shown above, the following items from the CSP Security Checklist may need to carry forward to the new CSP Security Standard:

1. Service Maturity and Capability (1a, 1c, 1d, 1e)
2. Security Lifecycle (2a, 2b)
3. Personnel Security (3a, 3b, 3c, 3d)
4. Data Center Physical Security (4a, 4b)
5. Application and Platform Security (5a, 5b, 5d, 5e, 5f, 5j)
6. Network Security (7a, 7d, 7f)
7. Portability and Interoperability (12a, 12b)
8. Compliance and Transparency (13b, 13c, 13d, 13e, 13f, 13g)

Appendix B – Vendor Responses

Direction: Fill in your responses on how the proposed cloud solution is in compliance with the CDPH CSP Security Standard. Do not answer only with a "Yes", "No" or "Not Applicable" to each requirement, be sure to elaborate on your response. If necessary, use the SIMM-140 Cloud Security Guide to help clarify many of the security requirements.

Evaluation	Description
Does Not Meet	- Inadequate security measures or controls - Weak or improper implementation of security practices - Non-compliance with security regulations or industry standards - Lack of documented security policies, plans, or procedures - Absence of security awareness training or insufficient employee training
Meets	- Basic security measures and controls are in place - Adherence to standard security practices and industry guidelines - Compliance with relevant security regulations and data protection requirements - Existence of documented security policies, plans, or procedures - Regular security awareness training for employees
Exceeds	- Robust and advanced security measures and controls - Implementation of best practices and innovative security solutions - Proactive approach to security, continuous improvement, and staying ahead of emerging threats - Demonstrated compliance with security regulations, industry standards, and certifications - Comprehensive security policies, plans, and procedures, including incident, response, and vulnerability management - Ongoing security awareness training, simulated exercises, and targeted training for specific roles.

ID	Requirement
1.1	Maintain an inventory of accounts with CSP including root email addresses, account IDs, and points of contact.
Response	
1.2	Maintain a method of tracking configuration changes and viewing inventory and configuration history of cloud services.
Response	
1.3	Apply resource tags to data and applications according to their categorization and criticality.
Response	

2a.1	Maintain a tiered account management structure and apply restrictions on subordinate accounts.
Response	
2a.2	Restrict usage of superuser access to the creation of less-privileged users for role-based access and administrative actions that can only be performed with superuser access.
Response	
2a.3	Require multi-factor authentication for all (1) privileged access, (2) user access to sensitive or confidential data, and (3) accounts representing official communications from state departments.
Response	
2a.4	Configure fine-grained user permissions according to least privilege. Ensure attempts to perform actions not permitted prompt notification of insufficient privilege.
Response	
2a.5	Perform an annual audit to review access and to remove unused credentials and permissions.
Response	
2a.6	Maintain logical perimeters between production and non-production environments (e.g., development, test). Prohibit using the same credentials across environments, except where single sign-on technologies generate unique credentials for federated access.
Response	
2a.7	Prohibit embedding credentials directly into code – configure applications to retrieve necessary credentials programmatically. Where feasible, programmatically generate temporary credentials instead of long-term credentials like passwords or access keys. Refer to the Azure Key Vault requirements section for more information.
Response	
2a.8	Provide access to cloud services by federated authentication through a centralized identity management system. Azure Active Directory (Azure AD) is the CDPH's centralized cloud identity provider (IdP). CSP must support SAML/OAuth2 federation to CDPH's IdP for user and administrative access. Refer to the Azure IAM Security Requirements section for more information.
Response	

2a.9	Deploy adaptive access control technologies to dynamically adjust authentication requirements based on contextual information.
Response	
2a.10	Creation of local accounts on systems/services is prohibited unless they are classified as “break glass” accounts.
Response	
2b.11	Establish network topologies to limit traffic routing only between resources as necessary.
Response	
2b.12	Limit resource exposure to the public internet to only those resources intended to be publicly accessible and protected accordingly, including deployment of endpoint defense capabilities in accordance with SAM Section 5355.
Response	
2b.13	Deploy Web Application Firewalls and/or Distributed Denial of Service protection services to protect public-facing applications.
Response	
2b.14	Require authentication and authorization when accessing cloud-based resources even across dedicated network connections, except resources intended to be publicly accessible.
Response	
2b.15	Limit virtual machine access to instance metadata services. Reference: Unsecured Credentials: Cloud Instance Metadata API, Sub-technique T1552.005 - Enterprise | MITRE ATT&CK® - Disable the metadata service for any virtual machines which do not require it. - Limit the permissions providing to the virtual machine to least privilege, to limit the impact of compromise. - Utilize local firewall rules to deny sending traffic to the metadata service except from the processes that require it. - Pay particular attention to virtual machines which are widely reachable, for example from the internet.
Response	
2b.16	***[Desired, Not Required]*** Limit deployments and maintenance to automated technologies as much as possible, disabling services used for manual administration.

Response	
2b.17	***[Desired, Not Required]*** Utilize tools to programmatically scan for weak configurations, including identification and vulnerability assessment of public facing resources. Configure notification and/or automated remediation where possible.
Response	
2b.18	***[Desired, Not Required]*** Employ deployment practices which replace running instances with new instances created from an updated configuration, rather than updating running instances.
Response	
2c.19	Select and configure storage services according to data availability (i.e., resilience to system downtime) and durability (i.e., resilience to data loss) requirements, which may include replication across cloud service provider zones and/or regions.
Response	
2c.20	Configure fine-grained data access policies.
Response	
2c.21	Protect data at rest by employing SAM Section 5350.1 compliant encryption and/or tokenization methods to transform confidential, sensitive, or personal data into a form that is unreadable to unauthorized users.
Response	
2c.22	Protect data encryption keys from unauthorized use by defining restrictive policies for key use that enforce the principles of least privilege and separation of duties (e.g., separate users with key administration permissions from users with key use permissions, separate applications that require permission to encrypt data from applications that require permission to decrypt data, require decryption requests to come from a trusted network path).
Response	
2c.23	Establish encryption key rotation policies to limit the impact of a single compromised key.
Response	
2c.24	Employ SAM Section 5350.1 compliant encryption methods to protect data in transit outside trusted network boundaries, even across dedicated network connections to cloud service providers.

Response	
2c.25	Configure data retention policies to automatically destroy data when it is no longer needed, in accordance with SAM Section 5310.6.
Response	
2c.26	Employ encryption methods to protect data in transit even within trusted network boundaries.
Response	
2c.27	***[Desired, Not Required]*** Employ techniques for automated discovery and classification of sensitive data.
Response	
3.1	Log cloud management events to centralized log storage for each cloud service provider, maintaining audit records in accordance with SAM Section 5335.2.
Response	
3.2	Establish threat prevention capabilities to identify weak configurations and notify security personnel. Configure automated remediation where possible.
Response	
3.3	Establish threat detection capabilities informed by threat intelligence and configure alerts to notify security personnel.
Response	
3.4	Publish cloud/platform security logs to the Security Information and Event Management (SIEM) system operated by CDPH's Security Operations Center (SOC), in accordance with SAM Section 5335.
Response	
3.5	***[Desired, Not Required]*** Implement tools to detect access credentials being stored in source control repositories.
Response	
4.1	Ensure incident response plans include procedures for notifying and coordinating with cloud service providers.
Response	

4.2	Ensure incident response procedures include providing access to external incident responders and protecting this access from unintentional use.
Response	
4.3	***[Desired, Not Required]*** Configure automated remediation of weak configurations.
Response	
4.4	***[Desired, Not Required]*** Configure automated responses for incident investigation, such as isolating resources from network access but preserving resource state.
Response	
5.1	Provision for data preservation and retrieval in agreements with cloud service providers, including but not limited to: a) Identification of requisite formats for transfer of data to state entity or subsequent service provider. b) A defined transition period to enable a successful transfer of data from service provider to state entity.
Response	
5.2	Configure automated data backups and virtual machine snapshots across zones and/or regions, according to recovery time and recovery point objectives.
Response	
5.3	***[Desired, Not Required]*** Define and deploy cloud infrastructure using code-like methods, back up configurations and scripts, and protect them from deletion.
Response	
6.1	CSP must have controls in place to protect the lifecycle of CDPH information from creation through to deletion.
Response	
6.2	CSP must assure CDPH information in digital and physical formats is securely isolated.
Response	
7.1	CSP must have appropriate screening and vetting procedures for internal personnel (besides under CDPH contract terms).
Response	

7.2	CSP personnel must be required to undertake mandatory information security awareness (besides under CDPH contract terms).
Response	
7.3	CSP must have processes in place to ensure personnel return assets when they leave or change role (MFA devices, mobile devices that have access to CDPH data, etc.).
Response	
7.4	CSP must have disciplinary processes for information security and privacy violations (besides under CDPH contract terms).
Response	
8.1	CSP must provide documentation that secure system engineering principles are followed within their Software Development Lifecycle (SDLC) processes.
Response	
8.2	CSP must provide documentation that host configuration is hardened against vulnerabilities (deploying hardened operating systems, disabling unnecessary services based on secure build images, etc.).
Response	
8.3	CSP must have multi-tenancy mechanisms configured and operational to separate CDPH applications from other customers.
Response	
8.4	CSP's web applications and APIs must be compliant with security standards, in accordance with OWASP Top 10, OWASP API Top 10, and CWE/SANS Top 25 Most Dangerous Software Errors.
Response	
8.5	CSP must have a Change Management Process in place to ensure deployment of validated application patches and updates.
Response	
8.6	If using CDPH's namespace for email is a requirement, the CSP's platform must have the capability of sending while meeting DMARC standards for SPF and DKIM, with SPF scoped to CDPH sending hosts only.

Response	
9.1	CSP's network connectivity must be adequate in terms of availability, traffic throughput, delays, and packet loss.
Response	
9.2	CSP must have gateway security measures in place against malware attacks.
Response	
9.3	CSP remote administration must be operated via a secure communication channel (SSH, TLS, IPSec, VPN, etc.).
Response	
9.4	CSP must provide integration with CDPH's Cloud Access Security Broker (CASB) platform for threat monitoring, DLP, anomalous activity or conditional access policies.
Response	
9.5	CSP must have the ability to implement source IP restrictions.
Response	
10.1	CSP must agree to provide CDPH information in an agreed upon format when the service arrangement ends.
Response	
10.2	CSP must have standardized or open interfaces to mutually exchange information between applications.
Response	
11.1	CSP must be SOC 2 Type II compliance.
Response	
11.2	CSP must be NIST SP800-53 revision 5 compliance.
Response	
11.3	CSP must be HIPAA / HiTRUST compliance when providing a product or a service involve the creation, storage, or transmission of Protected Health Information (PHI).

Response	
11.4	***[Desired, Not Required]*** CSP must be FedRAMP certified.
Response	
11.5	The physical location of the CSP's data center, where the data is stored, must be: - Located within the continental United States, and - Remote access to data from outside the continental United States is prohibited unless approved in advance by the State Chief Information Security Officer.
Response	