State of California

California Department of Technology

Office of Information Security

Cloud Security Standard

SIMM 5315-B

August 2020

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**August 2020**	**Office of Information Security (OIS)**	**New Standard in support of SAM Sections 4983 - 4983.1, Technological Alternatives – Cloud Computing Policy, and SAM Sections 5315 - 5315.1, Information Security Integration, and System and Services Acquisition.**

TABLE OF CONTENTS

I. INTRODUCTION

Cloud computing is a model for enabling on-demand network access to configurable computing resources. These resources are provided under three service models:

- Infrastructure as a Service (IaaS), the capability to provision processing, storage, networks, and other fundamental computing resources;
- Platform as a Service (PaaS), the capability to deploy applications onto cloud infrastructure using programming languages and tools supported by the provider; and
- Software as a Service (SaaS), the capability to use the provider's applications running on cloud infrastructure.[1]

The responsibility to secure these resources is shared between the customer and the cloud service provider, with varying responsibilities depending on the resource type and service model. Even with this shared responsibility, state entities remain ultimately responsible for selecting and configuring cloud services commensurate with risk tolerance and regulatory requirements.

II. MINIMUM CLOUD SECURITY REQUIREMENTS

To protect information and systems in cloud services, state entities must comply with the Cloud Computing Policy, State Administrative Manual (SAM) Sections 4983-4983.1, and employ the capabilities outlined in this Cloud Security Standard, SIMM 5315-B.

A. Identify

Identification and asset classification enable an entity to focus and prioritize efforts in alignment with its business needs and risk management strategy. To maintain an inventory of cloud information assets in accordance with SAM Section 5305.5, Information Asset Management, state entities shall:

1. Maintain an inventory of accounts with cloud service providers including root email addresses, account IDs, and points of contact.
2. Maintain a method of tracking configuration changes and viewing inventory and configuration history of cloud services.
3. Apply resource tags to data and applications according to their categorization and criticality.

B. Protect

Protective controls are proactive activities and security measures in support of the entity's overall risk mitigation strategy and due diligence.

Identity and Access Management

Security of cloud services stems from managing authentication and fine-grained authorization. To safeguard cloud systems in accordance with SAM Section 5360, Identity and Access Management, state entities shall:

1. Maintain a tiered account management structure and apply restrictions on subordinate accounts (e.g., denying the removal of logging and security features, denying access to services that do not comply with regulatory requirements).

[1] See SAM Section 4819.2 for complete definitions of cloud computing and each service model.

2. Restrict usage of superuser access (i.e., root users) to the creation of less-privileged users for role-based access and administrative actions that can only be performed with superuser access.
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.
4. Configure fine-grained user permissions according to least privilege. Ensure attempts to perform actions not permitted prompt notification of insufficient privilege.
5. Periodically audit access and remove unused credentials and permissions.
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.
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.
8. Provide access to cloud services by federated authentication through a centralized identity management system.
9. Deploy adaptive access control technologies to dynamically adjust authentication requirements based on contextual information (e.g., device content, endpoint security posture, user or entity behavior, location context, network context, targeted application).

Infrastructure Protection

Infrastructure protection controls limit the impact of unintended access or potential vulnerabilities, employing defense in depth. PaaS and SaaS resources may already have these controls implemented by the service provider. SAM Section 5315.6 requires state entities to configure information assets to provide only essential capabilities. In cloud systems, state entities shall:

10. Establish network topologies to limit traffic routing only between resources as necessary.
11. 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.
12. Deploy Web Application Firewalls and/or Distributed Denial of Service protection services to protect public-facing applications.
13. Require authentication and authorization when accessing cloud-based resources even across dedicated network connections, except resources intended to be publicly accessible.
14. Limit virtual machine access to instance metadata services.

Additionally, state entities are encouraged to:

15. Limit deployments and maintenance to automated technologies as much as possible, disabling services used for manual administration.
16. 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.
17. Employ deployment practices which replace running instances with new instances created from an updated configuration, rather than updating running instances.

Data Protection

State entities are entrusted with protecting the integrity and confidentiality of data processed by their information systems. Cloud technologies simplify data protection by providing managed data storage services with native protection and backup features, but these features must be configured and managed appropriately.

State entities shall:

18. 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.
19. Configure fine-grained data access policies.
20. 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.
21. 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).
22. Establish encryption key rotation policies to limit the impact of a single compromised key.
23. 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.
24. Configure data retention policies to automatically destroy data when it is no longer needed, in accordance with SAM Section 5310.6.

Additionally, state entities are encouraged to:

25. Employ techniques for automated discovery and classification of sensitive data.
26. Employ encryption methods to protect data in transit even within trusted network boundaries.

C. Detect

Detective controls identify potential security threats or incidents, supporting timely investigation and response. SAM Section 5345 requires state entities to continuously identify and remediate vulnerabilities. In cloud systems, state entities shall:

1. Log cloud management events to centralized log storage for each cloud service provider, maintaining audit records in accordance with SAM Section 5335.2.
2. Establish threat prevention capabilities to identify weak configurations and notify security personnel. Configure automated remediation where possible.
3. Establish threat detection capabilities informed by threat intelligence and configure alerts to notify security personnel.

Additionally, state entities are encouraged to:

4. Implement tools to detect access credentials being stored in source control repositories.
5. Publish cloud logs to the Security Information and Event Management (SIEM) system operated by the California Department of Technology (CDT) Security Operations Center (SOC).

D. Respond

Respond controls enable timely event and incident response which is essential to reducing the impact if an incident were to occur. State entities shall comply with incident management requirements as outlined in SAM Sections 5340-5340.4, and shall:

1. Ensure incident response plans include procedures for notifying and coordinating with cloud service providers.
2. Ensure incident response procedures include providing access to external incident responders and protecting this access from unintentional use.

Additionally, state entities are encouraged to:

3. Configure automated remediation of weak configurations.
4. Configure automated responses for incident investigation, such as isolating resources from network access but preserving resource state.

E. Recover

Recover controls facilitate longer term recovery activities following events or incidents. With cloud services, primarily SaaS solutions, the service provider hosts the data in its application, and unless properly planned and provisioned for in the contract with the service provider it may be difficult or impossible to obtain the data in a usable format at contract termination. For business continuity, state entities shall:

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.
2. Configure automated data backups and virtual machine snapshots across zones and/or regions, according to recovery time and recovery point objectives.

Additionally, state entities are encouraged to:

3. Define and deploy cloud infrastructure using code-like methods, back up configurations and scripts, and protect them from deletion.

III. QUESTIONS

Questions regarding the implementation of this standard may be sent to:

California Department of Technology
Office of Information Security
Security@state.ca.gov