3.3 - Audit & Accountability

Control Satisfaction Matrix

Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	Audit Controls
NIST 800-171	Audit & Accountability	3.3.1 - 3.3.9	AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12, AU-2(3), AU-5, AU-6(3), AU-7, AU-8, AU-8(1), AU-9, AU-9(4)	A.12.4.1, A.16.1.2, A.16.1.4, A.12.4.3, A.16.1.7, A.12.4.4, A.12.4.2, A.18.1.3	3.01 - 3.05

Major Document History

Date	Comment	Who
5/13/2019	Initial Doc	Tharp
5/30/2019	Add Control Objectives	Tharp
6/03/2019	Added Control Objectives, Assertions, Actions	Tharp
6/21/2019	CO's & Assertions updated with feedback from B&V CPA's	Tharp
7/30/2019	Remove Control Objectives	Tharp
8/12/2019	Formatting Updates	Tharp
8/29/2019	Copied Content For IS-1 SOC submission	Tharp
3/25/2020	Copied Content For IS-1 SOC evidence 1Q2020	Tharp
6/15/2020	Copied Content For IS-1 SOC evidence 2020Q2	Tharp
10/6/2021	Policy's Reviewed for Audit	Tharp

Purpose and Scope

The purpose of this policy is to establish the organizational requirements for internal monitoring and logging to ensure we operate within a secure infrastructure, using methods that meet or exceed industry best practice as well any governing compliance frameworks necessary to support our customers.

Background

Provide guidance to operation methods and processes that must be maintained to conform with these policies.

Policy

3.3.1

Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

3.3.2

Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

3.3.3

Review and update logged events.

3.3.4

Alert in the event of an audit logging process failure.

3.3.5

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

3.3.6

Provide audit record reduction and report generation to support on- demand analysis and reporting.

3.3.7

Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

3.3.8

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

3.3.9

Limit management of audit logging functionality to a subset of privileged users.

Response Plan

3.3.1r

DLZP Group shall maintain two classes of systems logs via monitoring activities and records that provides analysis, investigation and reporting of unlawful or unauthorized systems activty.

- **The First**, that support internal business, operations, development and support activities. These shall be associated with the systems and applications DLZP Group uses internally to support it business.
- **The Second**, that support hosted systems and the Statement of Work for each individual client.

DLZP shall maintain system logs associated with access to DLZP Group's Internal AWS assets “code”, lab environments and S3 storage, this shall include IAM and API changes. The same minimum standards shall be maintained for each client hosted system, other requirements may be called out in the client's statement of work for inclusion of additional controls.

Log scope including AWS Console and Command Line Activity shall be reviewed monthly, focusing on DLZP or client staff activities appropriate to their job roles as well as insuring no external bad actors have breached this infrastructure. All internal audit logs shall be stored in Dropbox and client logs stored in their respective Dropbox Audit Folder and reviewed monthly.

3.3.2r

Auditing Activities shall ensure that individual users and systems ID's are uniquely traced to hold user and developers accountable for actions and systems code.

DLZP Audit events shall be tracked via a ZOHO Recurring Tasks in the DLZP Internal - Admin Project, Client events shall be tracked in their respective support project.

3.3.3r

Logs must be reviewed at a minimum monthly and shall have alert automation for immediate notification of critical activities. Any audit activities that may be automated shall be accomplished with an appropriate alert.

Audit logs must validate universal clock synchronization amongst DLZP and Client internal AWS assets.

3.3.4r

All systems shall be configured to alert on monitoring and logging failures.

DLZP engineers must not access audit resources with a standard admin ID. Audit ID's must be created for each user requiring access to audit logs.

3.3.5r

Audit events and activities shall be processed by an appropriate parser to identify suspicious, unauthorized or unlawful activity. Events shall be reviewed by security personnel. Audit systems must be configured to alert on failure.

3.3.6r

Audit records shall be stored to support on-demand analysis and reporting.

3.3.7r

Audit activities must validate universal(scoped) clock synchronization.

3.3.8r

Audit tools, and records must be protected from unauthorized access, modification and deletion. Due to DLZP Group size separation of duties is not feasible. To mitigate this DLZP requires technical and audit administrative to be performed with separate and discreet ID's.

3.3.9r

Audit Management will be limited to a subset of privileged users.