

3.12 - Security Assessment

Control Satisfaction Matrix

Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	Audit Controls
NIST 800-171	Security Assessment	3.12.1 - 3.12.4	CA-2, CA-5, CA-7, PL-2	A.14.2.8, A.18.2.2, A.18.2.3, A.6.1.2	nxxx

Major Document History

Date	Comment	Who
5/14/2019	Initial Doc	Tharp
6/21/2019	CO's & Assertions updated with feedback from B&V CPA's	Tharp
7/30/2019	Strike thru control Objectives	Tharp
8/12/2019	Formatting Updates	Tharp
8/29/2019	Copied Content For IS-1 SOC submission	Tharp
10/6/2021	Policy's Reviewed for Audit	Tharp

Purpose and Scope

The purpose of this policy is to periodically assess the controls in organizational systems to mitigate known and potential security vulnerabilities.

Background

DLZP Group shall review and manage security vulnerabilities to internal systems that we rely on to conduct our business as well as the controls used to support our IT hosted clients.

3.12.1

DLZP Group shall assess security control efficacy on a quarterly basis.

3.12.2

Any deficiencies discovered will be immediately addressed using DLZP incident remediation and project management methodologies depending on scale and scope. Vulnerabilities will be communicated to DLZP Executives within 8 hours of discovery. This is crucial so that DLZP may notify its clients in a timely manner in accordance with contracts and statements of work with those clients.

3.12.3

Security control monitoring shall be instantiated in each environment and should be automated, and technical staff alerted immediately on the discovery of a monitored fault.

3.12.4

DLZP will review and update systems documentation and security plans on a bi-annual basis. This shall include boundary security methods, and interconnections with internal or external systems.

From:
<https://wiki.cloud.dlzpgroup.com/> -

Permanent link:
<https://wiki.cloud.dlzpgroup.com/doku.php?id=corpgov:securityasses>

Last update: **2021/10/06 21:46**

