3.11 - Risk Assessment

Control Satisfaction Matrix

Standard	Category	Controls Satisfied	800-53r4 Controls	ISO/SEC 27001	Audit Controls
NIST 800-171	Risk Assessment	3.11.1 - 3.11.3	RA-3, RA-5, RA-5(5)	A.12.6.1	23.0

Major Document History

Date	Comment	Who
5/14/2019	Initial Doc	Tharp
6/03/2019	Control Objective, Assertions, Test, Actions	Tharp
6/21/2019	CO's & Assertions updated with feedback from B&V CPA's	Tharp
7/30/2019	Added 23.0	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 organizational risk.

Background

DLZP Group shall review and manage technical vulnerabilities to internal systems that we rely on to conduct our business and the IT processing of our clients. The framework for this undertaking is outlined here: Security Assessment and Authorization - CA

3.11.1

DLZP Group shall review the risk to organizational assets, personnel, operational processes and methods including storage of organizational data on an annual basis. This shall include vulnerabilities from internal and external sources as well as the viability of systems and information (data) due to man made or natural events.

3.11.2

DLZP Group should employ vulnerability scanning tools on those systems where they control the

application or infrastructure e.g. IaaS or PaaS services.

3.11.3

Any vulnerabilities discovered should be tracked and remediated in a timely manner.

Response Plan

23.0 Risk Assessment Plan

23.1 Purpose

To document how the System Administrator performs periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability and initiates appropriate remediation.

23.2 Scope

Risk assessments can be conducted on any entity within DLZP or any outside entity that has signed an Agreement with DLZP. RAs can be conducted on any information system, to include applications, servers, and Systems, and any process or procedure by which these systems are administered and/or maintained.

23.3 Plan

The execution, development and implementation of remediation programs is the joint responsibility of the Project Manager, System Administrator and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the System Administrator in the development of a remediation plan.

23.4 Risk Assessment Process

Describe process to complete risk assessments on a periodic basis, key players involved and tests performed.

23.5 Enforcement

Any employee found to have violated this Plan may be subject to disciplinary action, up to and including termination of employment.

23.6 Definitions

Terms	Definitions
Entity	Any business unit, department, group, or third party, internal or external to DLZP, responsible for maintaining DLZP assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of DLZP's key information assets and systems. The System Administrator is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.