# Governance and Policy Approach

## Control Satisfaction Matrix

| Standard | Category | Controls Satisfied | 800-53r4 Controls | ISO/SEC 27001 | Audit Controls |
|---|---|---|---|---|---|
| NIST 800-171 | None | None | None | None | None |

### Major Document History

| Date | Comment | Who |
|---|---|---|
| 8/01/2019 | Initial Doc | Tharp |
| 1/04/2021 | Added Evidence File Directory Structure | Tharp |

## Cyber Security Standard

DZP Group elected to adopt the most comprehensive and widely recognized framework NIST 800-53rev4 for both public and private entities along with guidance from other NIST Frameworks in our case 800-171 that was derived from 800-53rev4.

The 800-171 Framework provides guidance on policy creation and implementation for Controlled Unclassified Information (CUI). DLZP determined it was less complicated to adopt a single classification standard and set of controls setting the bar to the highest measure than attempt to take a varied approach to data classification with several layers. Thus, 800-171 adoption provides a single high-hurdle to measure our processes against and maps to both 800-53rev4 and ISO/SEC 27001 Frameworks. These controls are easily achievable within the Amazon Web Service cloud solutions services.

Each Policy Area below shall consist of the Policy its Control Objectives, assertions that define the control objective measures and the relevant test(s) to validate assertion compliance.

```
Policy Area >>> Policy(s) >>> Control Objective(s) >>> Test(s) >>>
Assertion(s)
```

DLZP Group uses 800-171 as our default minimum standards. Where requested by client contract we will match the compliance frameworks that their business or industry is measured by incorporating additional NIST 800-53rev4 measures to satisfy client requirements.

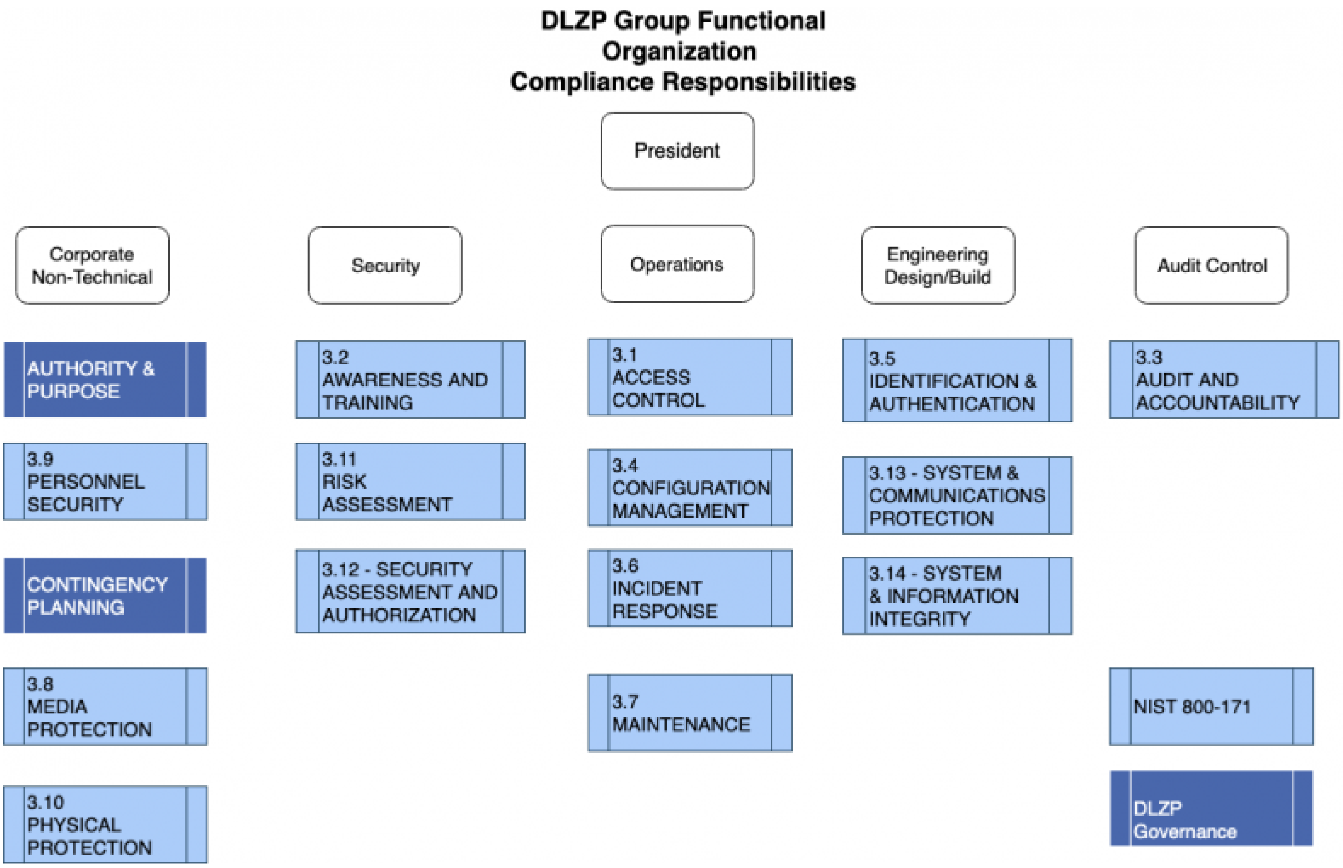
## Organization Responsibility Matrix

| Division | SECURITY REQUIREMENTS | Abbreviation |
|---|---|---|
| Operations | 3.1 ACCESS CONTROL | AC |
| Security | 3.2 AWARENESS AND TRAINING | AT |
| Audit Control | 3.3 AUDIT AND ACCOUNTABILITY | AU |
| Operations | 3.4 CONFIGURATION MANAGEMENT | CM |

| Division | SECURITY REQUIREMENTS | Abbreviation |
|---|---|---|
| Engineering | 3.5 IDENTIFICATION AND AUTHENTICATION | IA |
| Operations | 3.6 INCIDENT RESPONSE | IR |
| Operations | 3.7 MAINTENANCE | MA |
| Corporate | 3.8 MEDIA PROTECTION | MP |
| Corporate | 3.9 PERSONNEL SECURITY see HR Policies | PS |
| Corporate | 3.10 PHYSICAL PROTECTION | PE |
| Security | 3.11 RISK ASSESSMENT | RA |
| Security | 3.12 SECURITY ASSESSMENT | SA |
| Engineering | 3.13 SYSTEM AND COMMUNICATIONS PROTECTION | SC |
| Engineering | 3.14 SYSTEM AND INFORMATION INTEGRITY | SI |

## Functional Organization

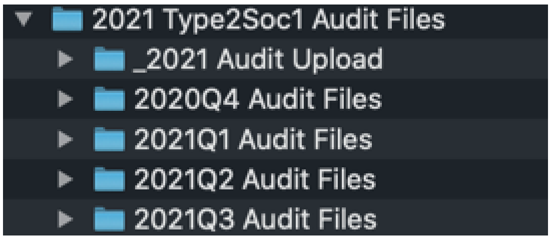
Functional Teams responsible for various Compliance Framework Sections


DLZP Group Functional Organization Compliance Responsibilities
President
Corporate Non-Technical
Security
Operations
Engineering Design/Build
Audit Control
AUTHORITY & PURPOSE
3.9 PERSONNEL SECURITY
CONTINGENCY PLANNING
3.8 MEDIA PROTECTION
3.10 PHYSICAL PROTECTION
3.2 AWARENESS AND TRAINING
3.11 RISK ASSESSMENT
3.12 - SECURITY ASSESSMENT AND AUTHORIZATION
3.1 ACCESS CONTROL
3.4 CONFIGURATION MANAGEMENT
3.6 INCIDENT RESPONSE
3.7 MAINTENANCE
3.5 IDENTIFICATION & AUTHENTICATION
3.13 - SYSTEM & COMMUNICATIONS PROTECTION
3.14 - SYSTEM & INFORMATION INTEGRITY
3.3 AUDIT AND ACCOUNTABILITY
NIST 800-171
DLZP Governance

| 800-171 | NIST 800-171 Naming | A-lign | Security Policy Manual | Asigned |
|---|---|---|---|---|
| 3.1 | Access Control | 3.0 | Access Control Policy | Dave |
| 3.1 | Access Control | 20.0 | Remote Access Policy | Dave |
| 3.1 | Access Control | 28.0 | Third Party Access | Dave |
| 3.2 | Awareness & Training | - | | Brian |
| 3.3 | Audit & Accountability | - | | Brian |
| 3.4 | Configuration Management | 8.0 | Operational and Software Development Change Management Policy | Dave |

| 800-171 | NIST 800-171 Naming | A-lign | Security Policy Manual | Asigned |
|---|---|---|---|---|
| 3.4 | Configuration Management | 12.0 | Encryption Policy | Dave |
| 3.4 | Configuration Management | 24.0 | Server Documentation Policy | Dave |
| 3.4 | Configuration Management | 25.0 | Server Security Policy | Dave |
| 3.4 | Configuration Management | 26.0 | Source Code Control Policy | Dave |
| 3.5 | Identificaion & Authentication | 9.0 | Password Policy | Dave |
| 3.5 | Identificaion & Authentication | 10.0 | Database Password Policy | Dave |
| 3.6 | Incident Response | 14.0 | Incident Handling Policy | Brian |
| 3.6 | Incident Response | 15.0 | Incident Response Guidelines | Brian |
| 3.7 | Maintenance | 19.0 | Patch Management and Systems Update Policy | Brian |
| 3.8 | Media Protection | 17.0 | Media Disposition Policy | Brian |
| 3.8 | Media Protection | 22.0 | Removable Media Policy | Brian |
| 3.9 | HR Policies | 2.0 | Acceptable Use Policy | Kim |
| 3.9 | HR Policies | 6.0 | Automatically Forwarded Email Policy | Kim |
| 3.9 | HR Policies | 11.0 | Email Retention Policy | Kim |
| 3.9 | HR Policies | 16.0 | Information Sensitivity Policy | Kim |
| 3.9 | HR Policies | 27.0 | Wireless Communication Policy | Kim |
| 3.10 | Physical Protection | 4.0 | Physical Security Policy | Brian |
| 3.11 | Risk Assessment | 23.0 | Risk Assessment Policy | Brian |
| 3.13 | Systems & Communications Protection | 13.0 | Extranet Policy | Dave |
| 3.13 | Systems & Communications Protection | 18.0 | Network Documentation Policy | Dave |
| 3.13 | Systems & Communications Protection | 21.0 | Virtual Private Network (VPN) Policy | Dave |
| 3.14 | Systems & Information Integrity | 5.0 | Anti-Virus Software Policy | Dave |
| 3.14 | Systems & Information Integrity | 7.0 | Backup / Restore Policy | Dave |

## Evidence Storage File Structure



- 2021 Type2Soc1 Audit Files
  - _2021 Audit Upload
  - 2020Q4 Audit Files
  - 2021Q1 Audit Files
  - 2021Q2 Audit Files
  - 2021Q3 Audit Files