Internal Business Contingency Planning - 800-53-CP

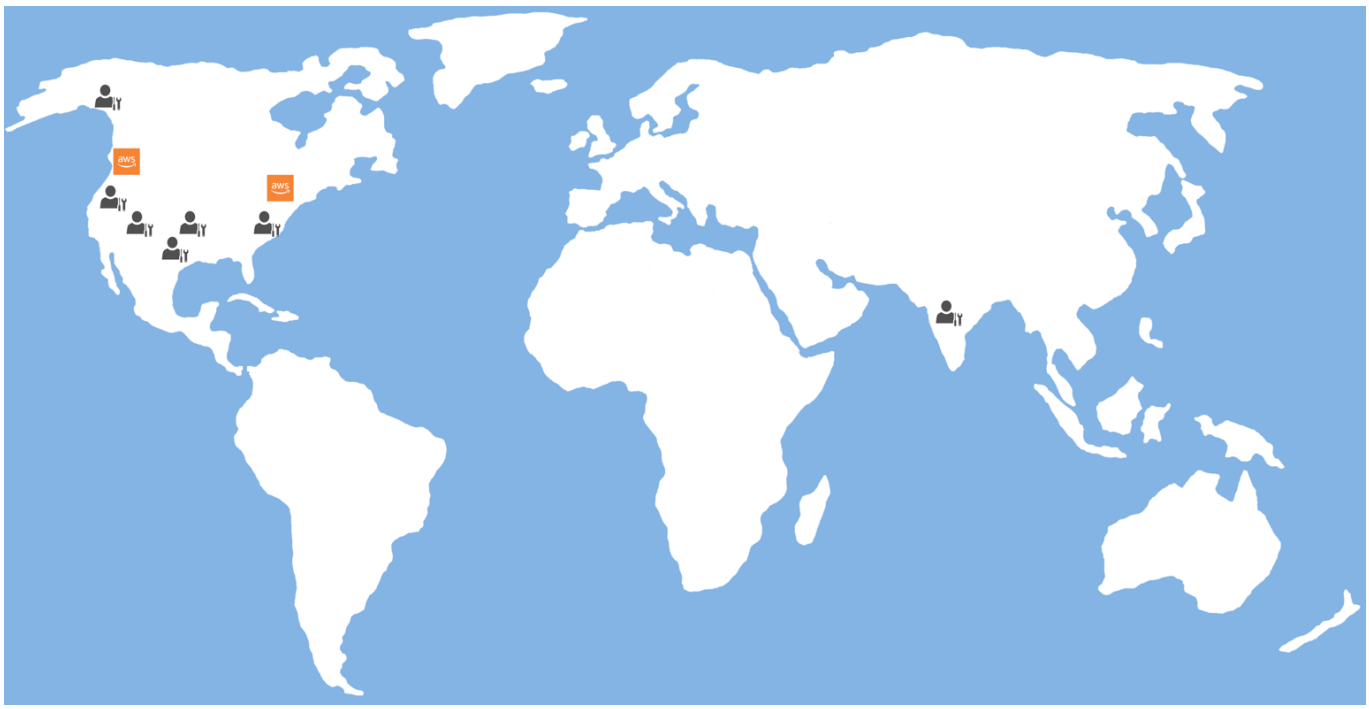
Control Satisfaction Matrix

Standard	NIST Category	Controls Satisfied	800-53r4 Controls Satisfied	ISO/SEC 27001	A-lign Controls
NIST 800-53rev4	Contingency Planning		CP-2a.1,CP-2a.2, CP-2a.3, CP-2a.4, CP-2d, CP-2e, CP-2f, CP-2 (7), CP-2 (8), CP-6 (1), CP-6 (2), CP-8 (4)©, CP-9a, CP-9b,CP-9c,CP-9 (1),CP-9 (5)		

Major Document History

Date	Comment	Editor
5/1/2019	Initial Doc	Tharp
5/7/2019	Update Controls Sat	Tharp
8/13/2019	Satisfaction Matrix	Tharp
8/19/2019	Application Loss Matrix	Tharp
8/29/2019	Copied Content For IS-1 SOC submission	Tharp
12/08/2020	Updated Content Contingency Planning Changes	Tharp
10/6/2021	Policy's Reviewed for Audit	Tharp

Fig 1. - Staffing and Data Processing Geographic Diversity



The DLZP Group mission is supported by 100% Cloud based infrastructure. Our staff is also

geographically dispersed throughout North America and India. At the personnel level each member of the DLZP team needs broadband internet service and their personal computer/laptop and a cell phone to function. This work model eliminates dependence on physical office space as well as fixed or facility based data processing environments that would typically be addressed in a business resumption plan. Our natural geographic diversity also ensures that localized manmade or natural disasters would not overtly impact our prime support mission to our clients, or any of the tools necessary for us to perform those duties. We have enough redundancy in staff roles and responsibilities to overcome any such event.

It should be noted that these Contingency Policies address DLZP Group planning only. Hosted Client Contingency planning are addresses within the Infrastructure Design Documents created at the outset of any client hosting engagement.

Essential Missions and Business Functions

DLZP Group provides several essential missions to our clients.

1. Application - design, development, build, hosting and ongoing support.
2. IT Consulting Services
3. Managed Hosting/Application Services

All DLZP Group essential missions and business functions are served entirely by cloud based infrastructure. From a DLZP business resumptions planning perspective all of our cloud based assets can be addressed discreetly in their hosting design plan to ensure the stability we need to support our clients needs.

```
Our standard disaster recovery commitment for client infrastructure is an
RPO of 15 Minutes and an RTO of 2 hours.
```

These client focused recovery objectives are automated within the client's cloud hosted infrastructure and supported by cloud automation without dependency on DLZP team members to take any action to meet the application recovery objectives above.

```
DLZP Group's Standard Service Level commits to a 15 minute response to
Critical Client Incidents.
```

Our staff response to Critical Incident support requires no fixed based infrastructure, client escalations via electronic or voice channels alert staffing groups and not single individuals eliminating the dependence on any single person.

Essential Tools to fulfill DLZP Client Facing Mission

1. AWS Command Line
2. AWS Console
3. AWS S3 - Object Storage
4. DLZP Wiki
5. DropBox - File Sharing - Deprecated March/2020
6. Email - Amazon WorkMail
7. Google Apps

8. Instant Messaging Apps - (Google Hangouts, Teams, Text)
9. PriTunl VPN
10. Trend Micro
11. Voice - Phone - Cellular, VOIP
12. AWS Workdocs migrated from Dropbox March/2020
13. Zoho CRM
14. Zoho Project - Project Management (Project, Change, Issues)
15. Zoom Meetings

Upon careful examination of mission essential tools and their service level commitments to system users we cannot predict any localized system or geographic outage that would prevent us from meeting our service level commitments to DLZP Group clients.

Contingency Roles

DLZP Staff have well defined roles to support day-to-day operations and break-fix activities. Those roles would not differ between client support and DLZP Infrastructure support. See DLZP Escalation and Critical Incident Processes.

Remediation

Any deficient status will be remediated by the Client Services Manager and necessary Functional/Technical team members responsible for that client.

```
A status report will be presented to the President upon successful
remediation
of critical criteria.
```

Contingency Testing

Contingency testing was a typical practice for on-premise IT infrastructure with a one-to-one relationship between production and recover sites and systems. For DLZP internal infrastrcutre dependencies DLZP relies on SaaS based tools and infrastructure having no responsibility for the hosting or care of the SaaS tool. These SaaS systems have 99% or better uptime commitments from their owners. Therefore, our contingency planning becomes a thought experiment to deduce the impact to our organization if a tool(s) becomes unavailable. This exercise is documented in the table below.

Application Loss Resumption or Workaround

SaaS App	Contingency Plan
AWS Command Line	Alternate Region
AWS Console	Alternate Region
AWS Object Storage S3	Alternate Region
DLZP Wiki	Configured to AutoRestore with 15 Min of Data Loss Potential
DropBox	Use Local Copy if DB not Available

SaaS App	Contingency Plan
Email	Use Voice, Web Conferencing or Instant Messaging Apps
Google Apps	Not used for Production Support
Instant Messaging Apps	(Google Hangouts, Slack, Text)
PriTunl	AutoRestore with no Data Loss
TrendMicro	No impact on production workstation
Voice	Land Line, Cellular, VOIP or Web Conferencing Options
Zoho CRM	Not used for production support
Zoho Project	Use Voice or Email, Take Local Notes
Zoom, Hangouts Slack, Other	Multiple Options; Use Alternate Option

Hosting Agreement Language:

Our business contingency plan is already in place. All of our employees are geographically dispersed throughout the world. All key information is stored in the cloud on various servers around the world. In case of an incident related to our force majeure, our contingency plan should stay in effect. All communication is done via the current available methods (telephone, cell phone, and internet) and will be leveraged to their greatest capability during a disaster. In case of a disaster, the DLZP Leadership will ensure the safety of our staff as our first priority, and then begin executing our disaster recovery plan, and those of the affected customers.