DoControl.

One SaaS to secure all other SaaS

Critical Functions Business Continuity Plan and Strategy
Version 1.1 Sep 21, 2020

Revision History			
Author	**Edition**	**Comments**	**Date**
Ron Peled, Security Consultant	1.0	First draft	Sep 1, 2020
Ron Peled, Security Consultant	1.1	Adjustments to DoControl	Sep 21, 2020

Approval			
Name	Title	Comments	Date
Adam Gavish	CEO	Reviewed and approved	Sep 21, 2020

1. Introduction

Any modern business is dependent on a wide range of computing systems and processes to enable its service delivery. In most cases, organizations are able to operate and keep business as usual, however, there are certain events that may cause business disruption. This includes both technical issues such as local hardware or software failure, power outage or more extreme situations such as fire, flood, natural disasters or pandemic.

2. Why do we need a Business Continuity Plan?

Handling a disruptive event without an advance preparation extends the recovery time and can even lead to a failure to efficiently recover. Many of the potential disruptions and risks can be reduced or eliminated through such proper preparation and implementation of technical, administrative, or operational controls. Such processes are outlined in a Business Continuity Plan.

3. HIgh Level Objectives and Scope

The Business Continuity Plan (BCP) for DoControl has been developed to address what is necessary to (1) reduce the risk of a disruptive event and (2) resume critical assets, services and operations as quickly and as efficiently possible after a disruptive event.

4. High Level Company Overview

DoControl is a fast growing software company that develops an advanced, agentless solution for protecting Cloud and SaaS applications. The company leverages public cloud and software as a service model as its primary infrastructure for service delivery. The company is based in the United States and operates from both the US and Israel.

5. BCP Committee

DoControl established a BCP committee to help plan, prepare, monitor and execute the plan and strategy. Members of the committee include: CEO, CTO and DevOps.

The BCP committee has developed the strategy based on the following stages:

1. Define the business critical assets and units
2. Identify primary risk & business impact for each asset/business function
3. Determine which preemptive controls should be in place to reduce the risk
4. Define recovery plan and process
5. Define roles & responsibilities
7. Define a test plan and frequencies
8. Define the Return Time Objective (RTO) and Return Point Objective (RPO)

6. Critical Assets

Interruptions related to facilities, computing systems, infrastructure, communications, hardware, data, staff and other assets described below might pose a risk to DoControl's services:

1. Production Environment - DoControl Production environment is based and hosted on AWS. The term Production refers to the Virtual Private Cloud based computing assets and infrastructure in use to deliver the service to customers. This includes but not limited to virtual machines, containers, networking devices, databases, hardware and software.

2. Office Operations - refers to the facilities, processes and business units that support the ongoing company operations. For example Finance, HR, DevOps, R&D. Most of the assets within the back office environment do not impact critical customer functions or services.

7. Return Time Objective and Return Point Objective

DoControl's Production Services RTO is up to 12 hours; the RPO is up to 24 hours. DoControl's Office services RTO is up to 48 hours; the RPO is 72 hours.

8. Potential Disruption Analysis

To help address the risks, DoControl performed a Potential Disruption Analysis process and a Business Impact Analysis for each critical function, which are used as the foundation of the plan.

PRODUCTION ENVIRONMENT		
Scenario	Description	Probability
Technical Failure	Service interruptions that might be caused due to software or hardware issue: Connectivity, Disk fault, ISP failure, Public Cloud failure, etc	Medium
Environmental Failures	Service interruptions caused by environmental factors such as fire, water flood / leaks, electricity / power failures, exposure to extreme weather conditions, physical destruction of equipment/hardware.	Low
Human Error	Configuration mistakes, deployment errors and application bugs. Such risks refer to interruptions on both software and hardware level.	Medium
Cyber Attack	Malicious attacks on critical Production assets. Such attacks mainly include distributed denial of service (DDoS), malware/infected assets or other vulnerability exploits on assets within the production environment.	Medium
Data loss or corruption	Loss of information retained in the production environment and required to provide various	Low

	services to customers. Such information include customer related data, configurations, reports and statistics. Loss of data may be caused by both environmental, physical (hardware) and logical (application / software) failures.	
Lack of Physical Access Data Centers (Public Cloud Providers only)	Refer to potential interruptions caused by events preventing physical access to facilities maintaining the production environment and assets. Such eve may include destructive earthquakes, extreme weather conditions, natural disasters, terror attacks / acts of war, large scale accidents, etc.	Low

OFFICE ENVIRONMENT		
Scenario	Description	Probability
Technical Failure	interruptions caused by failures in key network and IT components required to support DoControl’s operations (Office Internet access, VPN connection to Production, email services, Customer Support, CRM and financial systems	Low
Staff shortage	Massive personnel unavailability or shortage of up to 50%, consistent injury or illness (e.g. pandemic), emergency military conflict, etc.	Low
Cyber Attack	Malicious attempts to gain unauthorized access to the company assets by targeting office systems or employees.	Medium
Lack of	Refer to potential interruptions caused by events	Low

Physical Access To facilities	preventing physical access to the office facilities. Such events may include roadblocks, destructive earthquakes, extreme weather conditions, natural disasters, terror attacks / acts of war, large scale accidents, etc.	🟩

9. High Level Business Continuity Strategy

1. Leverage Public Cloud Infrastructure - DoControl's entire Production infrastructure is based on Virtual Private Cloud environment within leading Public Cloud service providers (e.g. Amazon, GCP, Azure). Such providers are subject to strict standards, uptime SLAs and recovery controls.

2. Leverage Software as a Service Model - DoControl uses various Software as a Service solutions for its ongoing operations. Such SaaS providers are subject to strict standards, uptime SLAs and recovery controls. In addition, by leveraging the SaaS model, operating from DoControl offices isn't required for service delivery.

3. Remote operations by default - DoControl designed its operating model to support remote and distributed work. This means that there are no dependencies on specific physical facilities for service delivery, and that DoControl employees are able to continuously work from anywhere in the world.

4. Redundancy and High Availability - DoControl has been architected to provide for high availability for its customers. The infrastructure uses multiple serverless components and step-functions to provide redundancy for any failure. In addition, the data is stored in reliable public cloud based database infrastructure which also has a live replica with automatic failover.

5. Ongoing monitoring - the infrastructure and critical components are monitored on a regular basis. Alerts are sent to the appropriate stakeholders and maintenance staff to help ensure rapid response.

6. Change Management and Rollback procedures - DoControl's software delivery is based on the continuous deployment concept, meaning each change goes through a review and then a set of tests to assure this change didn't break the system. Using this method, the company can conduct a roll forward (for a fix) or roll backward if needed.

7. Backup and recovery - all critical components are backed up on a regular basis, daily snapshots are kept 7 days back, and predeploy backups exist for 6 months. Recovery tests are performed quarterly, with the existing recovery mechanism checked in an automated test daily to make sure it's reliable.

8. Remote work protocols - all critical stakeholders and staff members are provisioned with all necessary equipment and devices to enable extended remote work. Such remote work procedures are tested at least annually.

9. Security program - DoControl has implemented multiple layers of security controls and processes throughout its operations. The solution was designed with senior security architects. In addition, DoControl is in the process of obtaining an ISO 27001 and SOC2 audit report.

10. Environmental controls - all data centers and facilities are subject to the strictest standards and include best of breed environmental controls.

10. Incident Assessment

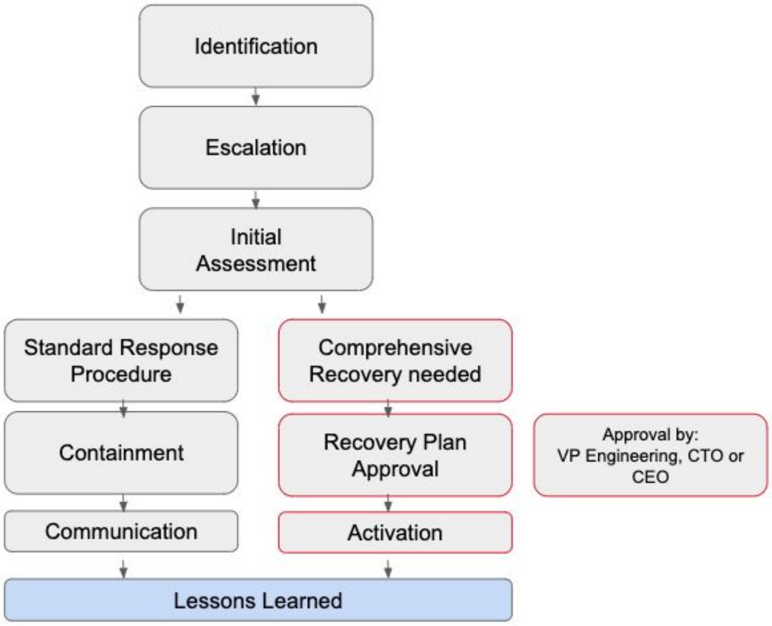
An assessment process will be initiated for unresolved events affecting the availability of service for defined time frames. The affected unit manager will assemble an assessment team that will complete the assessment procedures to determine the extent of interruption, estimated recovery time and whether to classify the event as an emergency that requires the activation of the BCP. The assessment process will address the following concerns at minimum:

- Suspected root cause
- Initial scope of affected services or environments
- Stability of the affected environment

- Estimate recovery time

11. Emergency Event Management

DoControl's emergency event management methodology is based on defined workflow, to help ensure effective response and minimum downtime or service interruptions, as outlined in the diagram below:



12. Notification procedure (to customers, to employees, others)

Where applicable, DoControl maintains a list of emergency contacts for communicating service-related information, such as service interruptions or scheduled maintenance activities that may cause downtime based on SLA and other agreements.

13. Test Plan

In order to measure the effectiveness of the BCP, practice its execution and identify potential failures or gaps, it is essential to test the various components of the plan on a timely basis. Detailed test scenarios with measurable KPIs and frequencies will be defined by managers of critical business units according to the table below.

- Annual Disaster Recovery test
- Annual Data Recovery Test
- Annual Connectivity failure test
- Annual Remote work practice
- Annual Facility evacuation practice
- Annual Security incident (e.g malware found on server)