DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

Business Continuity and Disaster Recovery Plan

Company Document # GRC-004
Revision: 2.2
Effective Date: 3/10/2020

Updated by: DocuSigned by: Adnan Mahmood 0C7B732D939B4FB...

Approved by: DocuSigned by: Vasanth Madhure 8469C738D9A04F7...

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

Table of Contents.

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

1. Overview

This document describes the Business Continuity and Disaster Recovery Plan for Certent. Certent places a high value on providing continuity of service to its Customers. The ability to restore system data after the interruption of services, corruption of data, or failure of hardware is vital to continue providing services to customers. The processes Certent has implemented to protect data and provide backup access to systems in the case of unplanned events are described below.

1.1 Definitions and Terminology

Disaster	Any loss of utility service, web connection, or a catastrophic event that causes an interruption in Certent operations is considered a disaster
BC	Business Continuity
CDM	Certent Disclosure Management
CRM	Customer Relationship Management
DM	Disclosure Management
DN	Disclosure Research
DR	Disaster Recovery
EM	Equity Management
ISP	Information Security Program
SaaS	Software as a Service

1.2 Related Documents

- Certent Information Security Program

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

1.3 Purpose and Scope

The purpose of this Business Continuity and Disaster Recovery Plan is to describe the preparations Certent has taken to maintain business operations in the event of a disaster such that, impact to Certent operations and customers is minimized and restoration of impacted services is achieved within a defined Service Level Agreement (SLA). This plan addresses key locations, infrastructure, systems, tools and processes related to the continued operation of Certent and customer subscribed services. The locations considered for the scope of this document are:

Corporate Headquarters:

- 1548 Eureka Road
  Roseville, CA 95661
  Site contact: Paul Brigaerts
- Canada Office:
  330 Bay Street, Suite 407
  Toronto, ON M5H 2S8
  Site contact: Mike Kushner
- Romania Office:
  4 Vasile Alecsandri Street
  District 1, Bucharest RO
  Site contact: Adrian Anton
- Ukraine Office:
  9a Borichyv Tik st
  Kyiv 04070
  Site contact: Alex Chernysh

These locations will cover the two pillars of Certent services:

- Equity Management pillar and
- Disclosure Management pillar which includes
  - Disclosure Management (DM),
  - Disclosure Research (DN) and
  - Certent Disclosure Management (CDM).

Certent Data Centers as mentioned in section 7.1 are also in the scope of this document.

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

2. Disaster Declaration

The CEO, CPO or VP of TechOps and InfoSec are responsible for declaring a disaster and initiating the activities as outlined in this plan.

3. Invoking the Plan

This plan becomes effective when a disaster is declared.

3.1 Communication

Communication between company leadership and Certent employees will be via email and phone as required. If company provided phones are unavailable, employees will rely on personal phones to communicate.

The management team, and Tech Ops staff shall keep updated contact information in their personal phones or a printed contact sheet in their homes to assist should an BC/DR event occur.

This contact list is available on Certent SharePoint.

3.2 Assumptions

- Key people will be available following a disaster.
- A national disaster such as nuclear war is beyond the scope of this plan.
- This document and all vital records are stored in a secure off-site location and not only survive the disaster but are accessible immediately following the disaster.

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

4. Certent's Business Continuity Scenarios

This section lists critical areas of Certent's business, considerations and planning of their continuity:

#	Risk	Business Continuity Plan
1	Certent platforms production failure (EM, DM and CDM)	The Certent Platforms are cloud-based systems managed by Certent and hosted with SunGard AS which is a colocation service provider and Microsoft Azure Cloud. In the event of primary location failure for a platform, the DR system at the secondary location is activated if the service cannot be restored within Certent's SLA.
2	Certent offices unavailable	In the event a Certent office is inaccessible to employees, all Certent personnel including all Customer Support and TechOps personnel will work from their homes where they have high speed Internet connection. This enables Certent personnel to access the corporate network remotely using VPN over the internet. In case of a disaster, employees are informed whether to work from home or come into the office via email and/or phone.
3	Certent's CRM (NetSuite) failure	Certent relies on NetSuite CRM to manage support cases which is a cloud-based system. All Certent staff with the need to access the CRM system can access it from anywhere with an internet connection. In the event NetSuite's primary system is not available, the NetSuite DR system will be activated automatically.
4	Telephony (RingCentral) service interruption	Certent has a subscription with RingCentral for telephony and conferencing which is a SaaS offering. All Certent employees have access to telephony via any internet connection. In the event RingCentral's primary system is not available, the DR system will be activated automatically.
5	Microsoft Office 365 service (O365) interruption	Certent's emails are hosted with Microsoft Office 365 which is a SaaS offering. Other services that are also provided part of this offering are SharePoint and Teams. All Certent employees have access to O365 services via any internet connection. In the event Microsoft's primary system is not available, the DR system is activated automatically.

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

6	Certent's File Server unavailability	The shared drive is where sensitive corporate data used for critical business processes is stored. The shared drive is hosted at the main colocation facility and managed by Certent TechOps. In the event that shared drive is not available from the primary location, the secondary location's shared drive system is activated which includes all data from the main shared drive.
7	Certent VPN service is down	Each site is configured with a VPN gateway that is required for remote access to corporate network or access to Certent's Platforms production networks. In case of a VPN failure at one location, users can connect to another location's VPN gateway and gain access to any network.
8	Pandemic	The impact on Certent operations is minimum based on the fact that Certent employees are geographically distributed. The key groups involved in supporting the Certent Platform are the TechOps, Customer Support, Engineering and Quality Assurance. Table 1 below shows distribution of the Certent personnel from each of those groups.

Table 1: Certent Personnel Distribution

Group	Employees	Location
TechOps	4	Certent Office in Roseville, CA
TechOps	3	Certent Office in Toronto Canada
TechOps	3	Offices in various U.S. locations
Customer Support	12	Certent Office in Roseville, CA
Customer Support	1	Certent Office in Toronto Canada
Customer Support	10	Offices in various U.S. locations
Development	11	Certent Office in Roseville, CA
Development	5	Certent Office in Toronto Canada
Development	5	Offices in various U.S. locations

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

5. Disaster Recovery Procedures:

This section documents specific recovery procedures for different scenarios:

5.1 Certent's RTO and RPO

- Certent's Recovery Time Objective (RTO) is 4 Hours.
- Certent's Recovery Point Objective (RPO) is 1 Hour.

5.2 Full Production Platform Failure

In the event the primary production facility is unavailable, a cut over to DR facility is performed as described below:

- ☐ Maintenance page is displayed on Certent Platform website.
- ☐ The Web Server, Services and the database server at the DR Facility are activated and configured as needed for production operation.
- ☐ Database archive logs are applied.
- ☐ Certent Platform website is made live again.
- ☐ Approximate Elapsed Time: 60 to 120 minutes depending on the nature of failure and Archive log activity at the time of Failure. Overall time is also based on the domain reconfiguration required.

Details regarding the DR capability include:

- ☐ Automation is in place to keep the DR site database and website code current with the production site.
- ☐ All services available on the production site are available on the DR site.
- ☐ Depending on the timing of the outage, maximum data loss is estimated at 60 minutes
- ☐ Estimated downtime to perform the cutover to the DR site is 60 to 120 minutes depending on the nature of the failure and Archive log activity at the time of Failure. Overall time is also based on the domain reconfiguration required.
- ☐ DR testing is performed annually.

5.3 Pandemic

In the event of a Pandemic, Certent will enact the following in offices:

- ☐ Employees from infected regions will not travel to corporate offices.
- ☐ Employees should avoid travel to and from infected zones per travel restrictions and guidelines placed by the World Health Organization (WHO) and Center for Disease Control (CDC).

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

- ☐ Employees are encouraged to get vaccinated.
- ☐ Office Common area and equipment will be disinfected daily.
- ☐ Face masks will be made available in offices.
- ☐ Depending on the gravity of the situation, management will take a call on "work from home" allowance for all staff.

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

6. Production System Failure Cutover

In the event of a Certent platform failure, the process outlined below is followed:

6.1 Disaster Recovery Cutover Decision Makers

- ☐ CEO
- ☐ Chief Product Officer
- ☐ VP of TechOps and InfoSec

6.2 Business Hours Outage

Business hours defined as: Monday – Friday 6:00 a.m. – 6:00 p.m. Pacific Time:

1. Investigate for up to 120 minutes to identify root cause.
2. If root cause is still unknown, perform cutover.
3. If root cause is determined and outage is going to be greater than 4 business hours total from start of outage, perform cutover.
4. If root cause is determined and outage is estimated to be less than business 4 hours, don't cutover. If during the resolution period the outage time is determined to exceed 4 business hours, perform cutover.

6.3 Non-Business Hours Outage

1. Investigate for up to 120 minutes to identify root cause. Note that depending on system usage (e.g., month end reporting for EM Platform, peak reporting period for DM Platform) and Customer needs, Management reserves the right to extend investigation up to 4:00 AM PT Monday – Friday and for extended periods on Saturday and Sunday to identify root cause.
2. If root cause is still unknown, perform cutover.
3. If root cause is determined and outage is going to be greater than 4 business hours total from start of outage, perform cutover.
4. If root cause is determined and outage is estimated to be less than 4 business hours, don't cutover. If during the resolution period the outage time is determined to exceed 4 business hours, perform cutover.

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

7. Critical Vendors

The following vendors are utilized by Certent for services, hardware, software and systems:

7.1 Services

The contact information for services vendors is provided below:

7.1.1 SunGard Availability Services

SunGard Availability Services provides the Primary (Production) and Secondary (Disaster Recovery) data center facilities for the Certent EM and DM Platforms.

Website: http://www.sungardas.com
Primary Data Center:
Address: 7499 E Paradise Ln Suite 108, Scottsdale, AZ 85260
Phone: (480) 245-5924

Disaster Recover Data Center:
Address: 11085 Sun Center Drive, Rancho Cordova, CA 95670 Phone: 916-877-4005
Contact / Email: Withheld

7.1.2 Equinix Data Centre

Toronto TR1 colocation and Internet exchange service hosts the Disclosure research (DN) platform for Certent.

Website: https://www.equinix.com/locations/canada-colocation/toronto-data-center/tr1/
Address: 151 Front Street West, 3rd, 5th, 6th and 7th floors, Toronto, Ontario M5J 2N1
Phone: +1.866.378.4649

7.1.3 Microsoft Services

Microsoft provides Office 365 services which includes Office applications, email, SharePoint and Teams. It also hosts the production platform for Cognos Disclosure Management (CDM) in Azure.

Website: https://support.office.com/en-us/article/Contact-Office-365-for-business-support-32a17ca7-6fa0-4870-8a8d-e25ba4ccfd4b
https://azure.microsoft.com/en-ca/support/options/
Address: Microsoft, Inc. One Microsoft Way, Redmond, WA 98052-6399
Phone: 800-865-9408
Customer Support is available using the link above

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

7.1.4 RingCentral

RingCentral provides telephony, online conferencing and instant messaging for Certent.

Website: https://www.ringcentral.com/
Address: RingCentral, Inc. 20 Davis Drive, Belmont, CA 94002 - USA
Phone: 1-888-898-4591
Contact / Email: https://success.ringcentral.com/articles/RC_Knowledge_Article/10995-RingCentral-Support-Contact-Us
Account Manager: Laverne Nguyen <laverne.nguyen@ringcentral.com>

7.1.5 NetSuite

NetSuite provides the CRM system for Certent.

Website: https://system.netsuite.com/pages/customerlogin.jsp
Address: NetSuite, Inc. 2955 Campus Drive, Suite 100, San Mateo, CA 94403
Phone: 866-522-1508
Customer Support is available using the link above
Account Manager: Iorga, Flavia <fiorga@netsuite.com>

7.2 Hardware

The contact information for hardware vendors is provided below:

7.2.1 Dell

Dell provides servers and firewalls for the Certent Platform.

Website: http://www.dell.com/support/Contents/us/en/19/article/Product-Support/Self-support-Knowledgebase/hardware-support/hardware, http://support.dell.com/, http://premier.dell.com
Address: One Dell Way, Round Rock, TX 78682
Phone: 800-822-8965, 866-362-5350
Customer Support is available using the link above

7.2.2 Barracuda

Barracuda provides Load Balancers for the Certent Platforms.

Website: http://www.barracudanetworks.com/ns/support/
Address: Barracuda Networks, Inc. 3175 Winchester Blvd, Campbell, CA 95008
Phone: 1.408.342.5400, 888-268-4772
Contact / Email: Customer Support / support@barracuda.com

7.2.3 Cisco

Cisco provides firewalls, switches and routers for Certent.

Website: https://www.cisco.com/c/en/us/support/index.html

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

Address: Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134
Phone: 1-800-553-6387
Customer Support is available using the link above

7.2.4 SonicWall

SonicWall provides firewalls for Certent Platforms.

Website: https://www.sonicwall.com/en-us/support/contact-support
Address: SonicWall, Inc. 2001 Logic Drive. San Jose, CA 95124
Phone: 1.888.793.2830 or 1.408.430.5870
Customer Support is available using the link above

7.2.5 CDW

CDW provides products and services for Certent; specifically switches, firewalls, servers
Website: https://www.cdw.com/content/cdw/en/help-center/contact-us.html
Address: 75 Tri-State International, Lincolnshire, IL 60069
Phone: 847.465.6000
Customer Support is available using the link above

7.3 Software and Systems

The contact information for software and system vendors is provided below:

7.3.1 Oracle

Oracle provides the database software and database operating system for the Certent EM Platform.

Website: https://login.oracle.com/mysso/signon.jsp
Address: Oracle 500 Oracle Parkway, Redwood Shores, CA 94065
Phone: 800-223-1711
Customer Support is available using the link above

7.3.2 Microsoft

Microsoft provides the application, web server and operating system software for the Certent EM and DM pillars and Database software for the DM pillar.

Website: https://support.microsoft.com/en-us
Address: Microsoft, Inc. One Microsoft Way, Redmond, WA 98052
Phone: 800-936-4900 (option 1, then option 2) 800-759-5474 (MSDN), 800-936-4900 (Partner)
Customer Support is available using the link above

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

7.3.3 VMware

VMware provides virtualization software for Certent.

Website: https://www.vmware.com/support.html
Address: VMware, Inc. 3401 Hillview Ave, Palo Alto, CA 94304
Phone: 1-877-486-9273
Customer Support is available using the link above

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

8. BC/DR Plan Execution Items

The items listed below are stored on the shared drive and in print format in the homes of key personnel, so they can be accessed in the event of a BC/DR scenario.

1. BC/DR Plan (this document).
2. Employee contact list including name, phone, personal email.
3. Office machine specifications.
4. Connection instructions for VPN access for all employees.
5. Vendor contact list including name, phone and email.
6. List of all s/w and h/w required for the office to be used to re-order equipment to staff a new facility.
7. List of potential new sites and/or agents to contact to obtain a new corporate facility.
8. Existing corporate office specifications in terms of sq. ft., cubicles, power, conference rooms, amenities, internet access, network, etc.
9. List of all h/w and s/w for the colocations including sq. ft., rack space, power, internet access, network, etc.

9. DR Test Framework

Testing the DR system focuses on verifying the components of the EM and DM pillars function properly. The DR Test Process is a simple 3 step process as listed below:

1. The Certent TechOps Team disables the Certent Platform at the primary production Colocation facility and executes the Cutover to the DR System as described in section “5.2 Full Production Platform Failure”
2. The Certent QA Team performs testing of the various components of the Certent Platform and ensure services are functioning as expected. If critical issues are discovered during DR tests, they are remediated within 45 days and added to lessons learned section of the test report.
3. Once testing is complete, the Certent TechOps team re-enables the Certent Platform at the primary production Colocation facility.

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

10. Compliance

10.1 Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, accessing company devices, and feedback to the policy owner.

10.2 Exceptions

Any exception to the policy must be approved by the InfoSec team in advance.

10.3 Non-Compliance

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

DocuSign Envelope ID: 46B8908A-49B3-4E92-AFCF-30A9195EC9F7

Revision History

Document Version	Revised Date	Revised By	Revision Description
1.0	03/17/2009	Scott Bradley	Draft created.
1.18	6/27/2017	John Underwood	Updated Sec 8.1.1 to reflect Sungard Availability Services information as primary and secondary data center vendor.
1.19	1/19/2018	Praneet Maharaj	General doc review and added new review table to cover sheet. Updated Sec 2 to include General Manager of Disclosure Management Updated sec 6.1 to include General Manager of Disclosure Management Updated Sec 8.1 removed Agility Recovery as a vendor
1.2	3/22/2018	Praneet Maharaj	Updated document format. Replaced Exception section with Compliance.
2.0	12/12/2018	Adnan Mahmood	Major review and update
2.1	7/19/2019	Adnan Mahmood	DR test framework update.
2.2	11/10/2019	Paul Brigaerts	Added additional service provider, CDW, under section 7.25 Hardware
2.2	03/10/2020	Tina Herron	Updated section 5.3